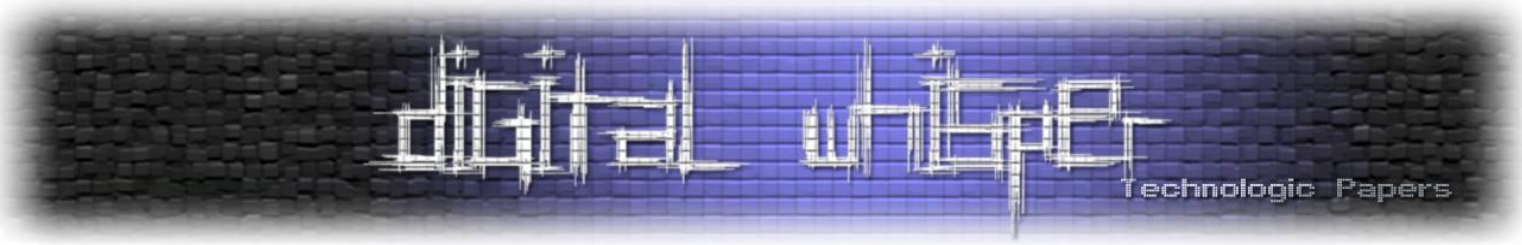


Digital Whisper

גליון 51, יוני 2014

מערכת המגזין:

מייסדים:	אפיק קסטיאל, ניר אדר
מוביל הפרויקט:	אפיק קסטיאל
עורכים:	שילה ספרה מלר, ניר אדר, אפיק קסטיאל
כתבים:	תומי שלו, חץ בן חמו, עמי קאופמן

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

דבר העורכים

חודש יוני הגיע, ואיתו הגיליון ה-51 של Digital Whisper!

האמת היא, שחודש מאי היה יכול להיות "יחסית חודש שקט" (אנחנו לוקחים את זה ש-eBay נפרץ על כל לקוחותיו ומאגריו, ואירועים בסגנון כעניין שבשגרה, כן?). למה "היה יכול להיות?" בגלל שממש לקראת סוף החודש, ב-28/05/2014, החבר'ה שהביאו לנו את TrueCrypt פרסמו את השורה שמופיעה עכשיו כמעט בכל אתר חדשות הקשור לאבטחת מידע:

```
"Using TrueCrypt is not secure as it may contain unfixed security
issues"
```

והעמוד של TrueCrypt ב-SourceForge כעת כולל הוראות כיצד ניתן להגר נתונים שהוצפנו בעזרת התוכנה כך שיהיה ניתן לעבוד איתם תחת BitLocker של Microsoft.

כאן כנראה המקום לציין, שמי שלא אוהב קונספירציות (אז מה לעזאזל הוא עושה בתחום הזה? ☺) יכול לדלג לסוף דבר העורכים.

כל בחור בר-דעת שיכנס לעמוד ישאל את עצמו "מה לעזאזל?", הסיבה שהמפתחים כותבים באתר היא:

```
"The development of TrueCrypt was ended in 5/2014 after Microsoft
terminated support of Windows XP, Windows 8/7/Vista and later
offer integrated support for encrypted disks and virtual disk
images."
```

והטענה היא שכל עוד מיקרוסופט תמכו ב-XP היה היתרון ל-TrueCrypt על פני הצפנות הכוננים מבוססות מערכת ההפעלה, כעת, כשמיקרוסופט כבר לא תומכת ב-XP, יש עדיפות להשתמש באותן מערכות ולא ב-TrueCrypt. לא יודע איך זה נשמע לכם, אבל לי זה נשמע הזוי, ומסתבר, ככה אמרו לי, שכשאנשים עושים דברים שמהצד נראים הזוי - כנראה שיש כאן דברים שלא מספרים לנו.

כבר עלו לא מעט טענות בנוגע ל-TrueCrypt- טענות כגון זה שאף אחד לא פגש אף פעם את המפתחים של התוכנה, וטענות כמו שקשה בצורה מאוד מחשידה להגיע למצב שבו ניתן לקמפל את קוד המקור של התוכנה, או שבפורום של TrueCrypt (שנסגר) יש משטר טרור בנוגע לכל מה שקשור ללדבר על תוכנות אחרות או Fork-ים של אותה התוכנה או זה שבגרסה האחרונה שקוד המקור בגרסה האחרונה שפורסמה (7.2) הורידו הרבה מאוד קוד שנוגע למנגנוני ההצפנה. אני מודה- אני לא כמו הבחור מ-privacylover, שמנהל כבר לא מעט זמן את הפוסט הנ"ל, אבל אני בהחלט מרים גבה.

בעבר פורסם כי גופים שונים כגון ה-FBI לא הצליחו להתמודד עם כוננים שהוצפנו בעזרת TrueCrypt, כמו במקרה עם הבנקאי הברזילאי. מה האינטרס לפרסם אירוע כזה? אני לא באמת יודע, הרי מובן שאם נתון כזה יפורסם - כל עבריין שעיניו בראשו יצפין את הכוננים שלו בעזרת התוכנה, אבל אם תשאלו את הצד הקונספירטיבי שבי, הוא יענה לכם שמדובר כאן בפסיכולוגיה הפוכה - גופים כגון ה-FBI יודעים להתמודד עם TrueCrypt ומעוניינים לפרסם את ההפך (נכון שלא ה-FBI הוא זה שפרסם את האירוע וסיבת הכישלון, אך זה הגיע משם בסופו של דבר) - וכך להגדיל את הסיכוי שבפשע הבא שאותו הם ידרשו לפתור, הם יתקלו בכונן המוצפן באמצעות TrueCrypt.

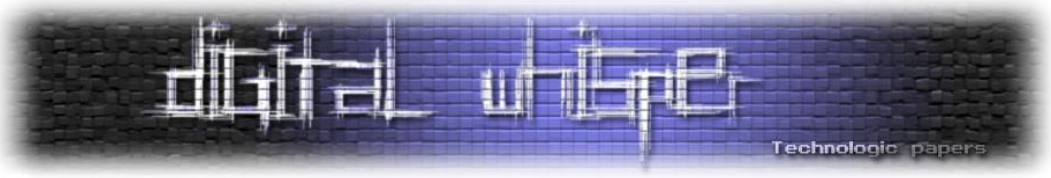
כעת, אם תשאלו את אותו צד קונספירטיבי לגבי האירוע הנ"ל, הוא יענה לכם שה-NSA לא מסתדרים עם הצפנות של TrueCrypt (איך זה הגיוני? פשוט מאוד, באחת הגרסאות הקודמות של TrueCrypt הייתה חולשה / דלת אחורית, וכעת, בגרסאות החדשות - היא הוסרה מהקוד / תוקנה) ולכן הם מנסים לסנדל את הפרויקט ובעזרת דרכים-לא-דרכים מצליחים גם כנראה מצליחים לעשות את זה. אותו צד גם יגיד לכם שאין ל-NSA בעיה להתמודד עם הצפנת הכוננים של BitLocker (בסופו של דבר, Microsoft זאת חברה אמריקאית, שנחשדה לא פעם בביצוע שת"פים עם ה-NSA וכאן גם הקוד של ההצפנה ומימושה הוא קוד סגור...) ולכן לשם הם מפנים את המשתמשים.

זאת המציאות? האם אפשר להמשיך להשתמש ב-TrueCrypt? לכו תדעו, אבל כמו שאמרתי בדיוק לפני חודש, בדברי הפתיחה של הגיליון הקודם, TrueCrypt או BitLocker, כל זה לא משנה, אם אתם לא מעוניינים שהמידע שיש ברשותכם יגיע לידיים הלא נכונות - פשוט אל תשמרו אותו על המחשב שלכם, ולא משנה מה אורך המפתח או אלגוריתם ההצפנה שבה השתמשתם.

וכמובן, לפני שנגש לתכנים, נרצה להגיד תודה לכל מי שהשקיע מזמנו וכתב מאמר לגיליון, תודה רבה ל**תומי שלו**, תודה רבה ל**חץ בן חמו**, תודה רבה ל**עמי קאופמן** ותודה רבה ל**שילה ספרה מלר**.

קריאה מהנה!

ניר אדר ואפיק קסטיאל.



תוכן עניינים

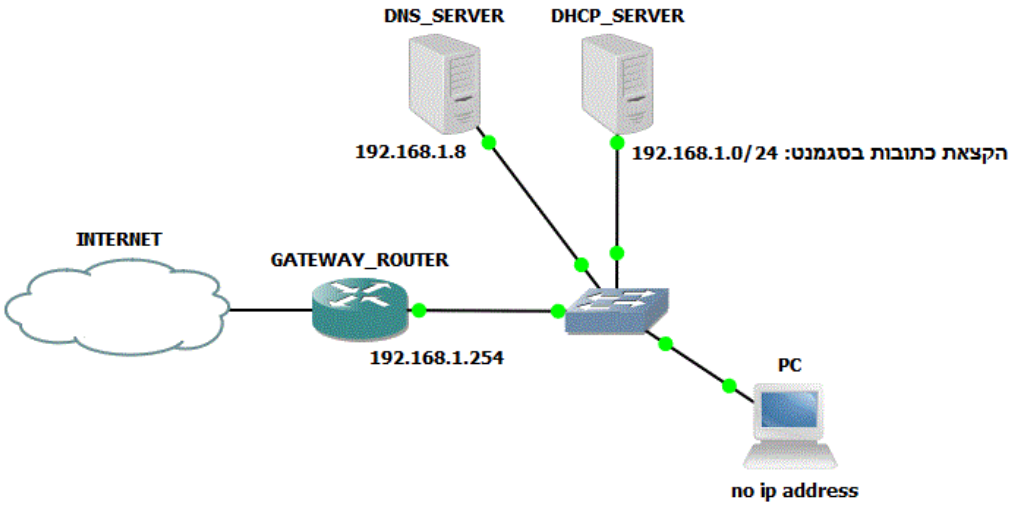
על סוגיות אבטחה ב-DHCP

מאת תומי שלו (פורסם במקור באתר: http://netsystem.org.il)

הקדמה

מנגנון DHCP - Dynamic Host Configuration Protocol הינו מנגנון דינאמי להקצאת פרמטרי רשת שונים בציודי קצה / רשת. פרוטוקול זה מייעל ומפשט תהליכי הקצאת משאבי IP ברשת ונוח מאוד לשימוש והגדרה, יחד עם זאת הוא טומן בחובו פירצות אבטחה ב-L3.

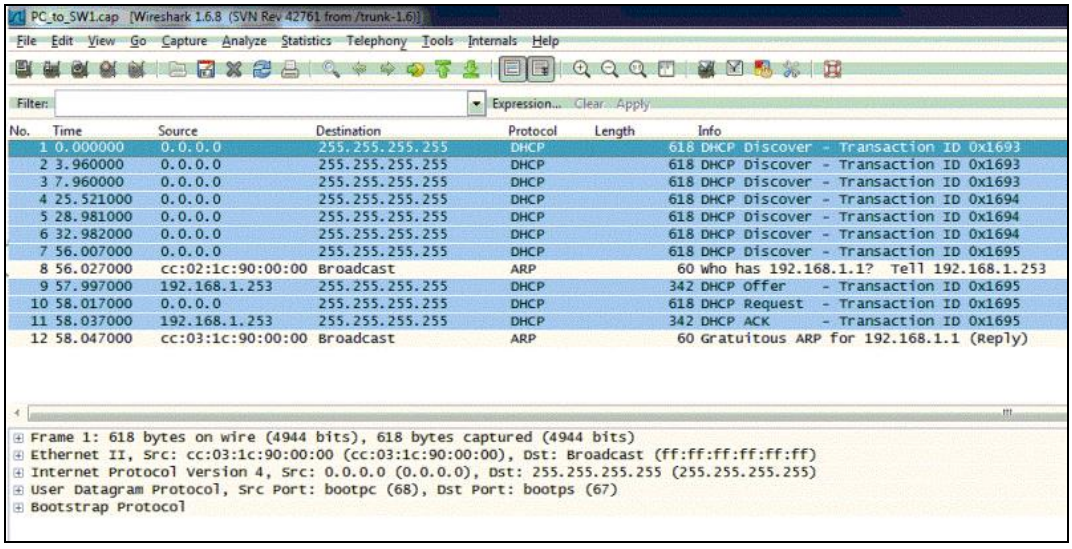
לרוב, שרתים ישמשו כספקי DHCP אך ניתן להגדיר גם ציודי רשת כגון נתבים ומתגים כשרתי DHCP בתהליך הגדרה פשוט. החיסרון העיקרי בהגדרת ציודי רשת כשרתי DHCP הוא חוסר היכולת שלהם להסתנכרן ולעבוד במקביל עם ציוד DHCP נוסף. תצורת רשת פשוטה בה קיימים שרת DHCP, שרת DNS, נתב GW ולקוח DHCP פוטנציאלי תראה כך:



המו"מ שמבצע שרת DHCP אל מול לקוח פוטנציאלי מתרחש ב-4 שלבים עיקריים, כאשר ה"שיחה" בין הלקוח לשרת מתבצעת ב-UDP בפורטים 67 ו-68.

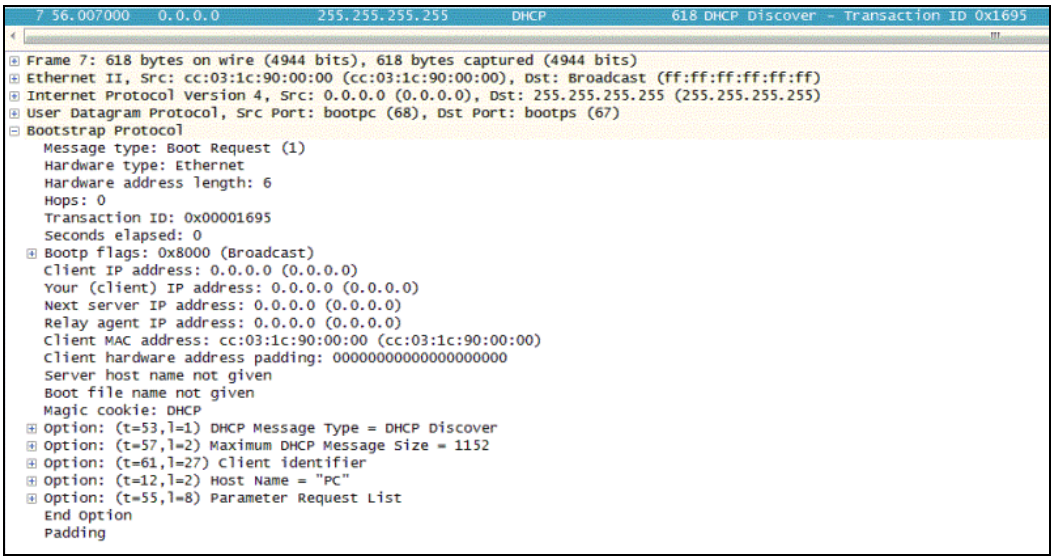
DHCP Handshake

לטובת הבנת תהליך הקצאת הפרמטרים של DHCP נכיר קודם כל את ההודעות הנשלחות במסגרת תהליך ההקצאה, ואלו הן: DHCP DISCOVER, DHCP REQUEST, DHCP OFFER ו-DHCP ACK לדוגמא:



[תהליך המו"מ כפי שנלכד בתוכנת הסניפר WireShark]

שלב 1: לקוח DHCP פוטנציאלי שהוגדר בתצורת DHCP שולח הודעת Discover כהודעת BC(broadcast) בשדות ה-Destination של המסגרת והחבילה (L3+L2). בשדות ה-Source יצויינו כתובת ה-MAC של הלקוח וכתובת IP שהיא 0.0.0.0. כל זאת בתקווה שקיים שרת / ספק DHCP שיאזין להודעתו ויקצה לו את הפרמטרים שביקש.



[בהודעה ניתן לראות את שדה Parameter request list שבו מציין הלקוח את רשימת הפרמטרים שהוא מבקש שהשרת יקצה לו]

שלב 2: שרת DHCP שמקבל את הודעת ה-Discover מלקוח פונטציאלי רוצה כעת "להציע" ללקוח כתובת IP אפשרית, לפני שהוא ישלח לו את ההצעה הוא קודם כל מוודא שב-DB שלו לא קיימת הקצאה של הכתובת, לאחר מכן הוא מבצע בדיקת ARP ע"י שליחה של הודעת ARP request על מנת לוודא כי לא קיים בסגמנט ציוד שהוגדר סטטית עם אותה כתובת ה-IP.

במצב שבו התקבל מענה להודעת ה-request יישלח ICMP echo לווידוא מוחלט - ואם יתקבל מענה גם ל-echo יווצר מצב שנקרא DHCP conflict, כלומר קיימת כתובת מתוך המאגר הפוטנציאלי של השרת שלא הוא הקצה ולא ניתן להקצות אותה זמנית (בתצורות שבהן קיים שרת DHCP מרכזי בליבת הרשת, הוא משתמש ב"סוכנים" שמבצעים עבורו את הבדיקות הללו).

לאחר סט הבדיקות שולח השרת הודעת OFFER כ-BC ב-L2&L3 destination כאשר בשדות ה-SRC הוא מציין את כתובות ה-MAC וה-IP שלו. ההודעה מכילה הצעה עבור כלל הפרמטרים שהלקוח ביקש, בין היתר subnet mask, כתובת IP, כתובת DNS, כתובת GW, זמן השכרה.

```
 9 57.997000   192.168.1.253      255.255.255.255      DHCP          342 DHCP Offer    - Transaction ID 0x1695
⊞ Frame 9: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
⊞ Ethernet II, Src: cc:02:1c:90:00:00 (cc:02:1c:90:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 192.168.1.253 (192.168.1.253), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
⊟ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x00001695
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x8000 (Broadcast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.168.1.1 (192.168.1.1)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: cc:03:1c:90:00:00 (cc:03:1c:90:00:00)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⊞ Option: (t=53,l=1) DHCP Message Type = DHCP Offer
  ⊞ Option: (t=54,l=4) DHCP Server Identifier = 192.168.1.253
  ⊞ Option: (t=51,l=4) IP Address Lease Time = 10 minutes
  ⊞ Option: (t=58,l=4) Renewal Time Value = 5 minutes
  ⊞ Option: (t=59,l=4) Rebinding Time Value = 8 minutes, 45 seconds
  ⊞ Option: (t=1,l=4) Subnet Mask = 255.255.255.0
  ⊞ Option: (t=6,l=4) Domain Name Server = 192.168.1.8
  ⊞ Option: (t=3,l=4) Router = 192.168.1.254
    End Option
    Padding
```

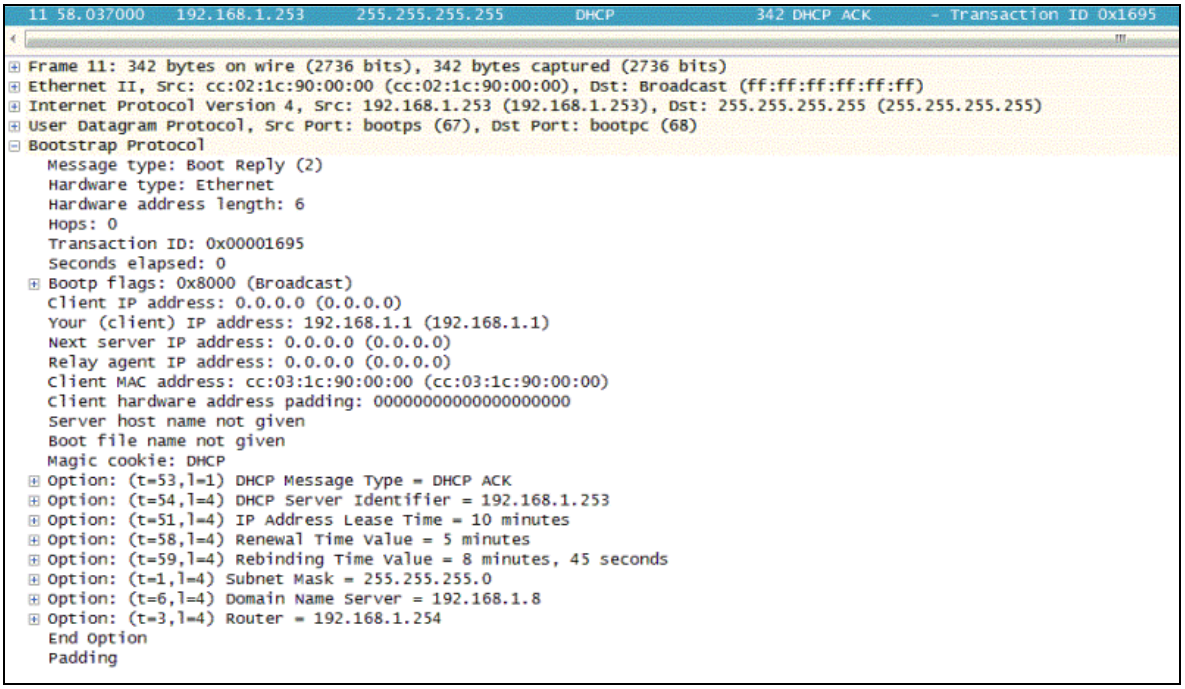
שלב 3: הלקוח שקיבל את הודעת ה-OFFER צריך להגיע כעת להחלטה האם הוא מסכים לקבל את ההצעה מהשרת, אם הוא לא מסכים (למשל מהסיבה שיש לו רשומת ARP שאומרת שכתובת ה-IP שהוצעה לו שייכת בכלל לציוד אחר) הוא ישלח הודעת DECLINE. אם הוא מסכים, הוא ישלח הודעת REQUEST שמהווה בקשה "רשמית" להחיל על עצמו את הפרמטרים שהשרת הציע לו.

הודעה זו מכילה בעצם שדה שמציין מי הוא שרת ה-DHCP, מה הכתובת שהוצעה לו, כתובת ה-MAC של הלקוח (אין קשר ל-MAC במסגרת משום שברשתות גדולות משתמשים בסוכנים המעבירים את ההודעות לשרתי ה-DHCP, לכן מצויין ה-MAC של הלקוח בהודעה עצמה) והזמן לשכירת הפרמטרים (lease time).

```
10 58.017000   0.0.0.0          255.255.255.255      DHCP          618 DHCP Request  - Transaction ID 0x1695
Frame 10: 618 bytes on wire (4944 bits), 618 bytes captured (4944 bits)
Ethernet II, Src: cc:03:1c:90:00:00 (cc:03:1c:90:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Bootstrap Protocol
   Message type: Boot Request (1)
   Hardware type: Ethernet
   Hardware address length: 6
   Hops: 0
   Transaction ID: 0x00001695
   Seconds elapsed: 0
   Bootp flags: 0x8000 (Broadcast)
   Client IP address: 0.0.0.0 (0.0.0.0)
   Your (client) IP address: 0.0.0.0 (0.0.0.0)
   Next server IP address: 0.0.0.0 (0.0.0.0)
   Relay agent IP address: 0.0.0.0 (0.0.0.0)
   Client MAC address: cc:03:1c:90:00:00 (cc:03:1c:90:00:00)
   Client hardware address padding: 00000000000000000000
   Server host name not given
   Boot file name not given
   Magic cookie: DHCP
   Option: (t=53,l=1) DHCP Message Type = DHCP Request
   Option: (t=57,l=2) Maximum DHCP Message Size = 1152
   Option: (t=61,l=27) Client identifier
   Option: (t=54,l=4) DHCP Server Identifier = 192.168.1.253
   Option: (t=50,l=4) Requested IP Address = 192.168.1.1
   Option: (t=51,l=4) IP Address Lease Time = 10 minutes
   Option: (t=12,l=2) Host Name = "PC"
   Option: (t=55,l=8) Parameter Request List
   End Option
   Padding
```

שלב 4: זהו השלב האחרון בתהליך ההקצאה שבו בעצם שרת ה-DHCP משכיר באופן רשמי את הפרמטרים ללקוח. השרת שולח ב-BC הודעת ACKNOWLEDGE שבה מצויינים כלל הפרמטרים הרלוונטיים שמוקצים ללקוח. שימו לב שהודעה זו זהה לחלוטין להודעת ה-OFFER ואפילו גודל המסגרות הוא זהה (במקרה שלנו bytes324). בסוף תהליך זה ולאחר שהלקוח קיבל את הודעת ה-ACK (בעצם החיל על עצמו את הפרמטרים), הוא שולח הודעת Gratuitous ARP שבה הוא מצהיר על עצמו עם כתובת ה-IP החדשה שהוא קיבל.

הערה: לא כל ציוד שולח הודעת ARP בסוף התהליך.



סוכני DHCP

ברוב הרשתות הגדולות מוצבים מס' שרתי DHCP בליבת הרשת, מצב שבעצם מונע גישה מלקוחות פוטנציאליים אל השרתים משום שהודעות ה-BC שהם שולחים מוגבלות ל-BC DOMAIN של הסמגנט שבו הם יושבים (הלקוחות), ידוע שבאופן רגיל ציוד L3 לא מעביר הודעות BC לרגליים אחרות. הפתרון לכך הוא קיום של "סוכני" DHCP שאחראים להעביר הודעות בין לקוח לשרת, לרוב סוכנים אלו יהיו נתבים, מתגי L3 או Firewalls הנמצאים ברשת.

ניתן להשתמש בסוכנים בכמה אופנים כשהעיקרי שבהם הוא שימוש ב-IP HELPER בסגמנט הרלוונטי. הסוכן בעצם לוקח את הודעת ה-BC שאותה הוא "שמע" מהלקוח ושולח אותה ישירות לכתובת שרת ה-DHCP כשהוא משכתב את ההודעות ומציין בשדה ייעודי שהוא (הסוכן) באותו הסמגנט, ע"פ כתובתו של הסוכן יוכל לדעת שרת ה-DHCP אילו פרמטרים להקצות ובאיזה טווח כתובות להשתמש.

לדוגמא: לפי סוכן שכתובתו היא 10.0.0.1/24 יידע שרת ה-DHCP שכתובתו היא 172.16.1.1 להקצות פרמטרים לפי הסגמנט 10.0.0.0/24.

בואו ונחשוב כעת, מה קורה אם גורם עויין מחבר לרשת ספק כתובות IP משלו ("Rogue DHCP") שמקצה ללקוחות את אותם הפרמטרים בדיוק מלבד כתובת ה-GW שתהיה בעצם הממשק שלו בסגמנט, החבילות מאותם הלקוחות יגיעו אליו, הוא ישמור עותק שלהן ויעביר אותן בשלמותן ל-GW האמיתי בסגמנט מבלי שאף אחד ירגיש.

המקרה שתיארתי הוא סוג של מתקפת MAN-IN-THE-MIDDLE שעשויה להתרחש במרחב ה-LAN של כל סגמנט וניתן לממש אותה לדוגמא גם באמצעות התערבות בתהליכי מנגנון ה-ARP. קיימות מספר דרכים אשר נועדו למנוע סוג כזה של מתקפה, אך אני ארחיב על איך ניתן למנוע מתקפה שכזו כמנהלי רשת, במתגי Cisco שאחראיים על תעבורת ה-L2 בעזרת מנגנון בשם DHCP Snooping.

DHCP Snooping הוא מנגנון פשוט שניתן להפעיל בחלק מהמתגים ועיקרו הוא קביעת "אזורים" בטוחים ו"אזורים" שאינם בטוחים במתג. כשאני מדבר על אזור אני מתכוון לפורט/ממשק L2 שעשויות להתקבל בו הודעות DHCP מספק/ספקים הקיימים ברשת.

מה שעושה מנגנון DHCP Snooping הוא בעצם חלוקה של הפורטים במתג ל-2 סוגים: Trusted ports ו-Untrusted ports, כאשר ספקי ה-DHCP יחוברו לפורטים האמינים ושאר העמדות/שרתים ב-LAN יחוברו לפורטים שאינם אמינים.

רק בפורטים אמינים אפשר שיתקבלו הודעות DHCP Reply מהסוגים השונים שמקורן בשרת/ספק DHCP כלשהו. ומה יקרה אם בפורט לא אמין יתקבלו הודעות שכאלו? פשוט מאוד, הפורט ייכנס אוטומטית למצב Error-disable שלא מאפשר שליחה וקבלת מידע נוספת בפורט לאורך זמן מסויים שהוגדר מראש או עד שיבוצע Shut ומיד לאחר מכן No-shut ע"י מנהל הרשת.

התגובה של המנגנון מונעת מגורם זדוני להתחזות לספק ה-DHCP ברשת ה-LAN ובעצם מדליקה נורה אדומה עבור מנהל הרשת על מנת שיתבצע תחקור לאירוע.

ומה קורה אם השרת נמצא הרחק מהמתג? פשוט וקל! נצטרך להפעיל קצת את הראש ולחזות מהיכן עשויות להגיע הודעות התגובה משרת ה-DHCP שלנו, אם המתג מחובר בתצורה שרידה או מקושר לאזור ה-L3 אז אפשרי שההודעות יגיעו מכל פורט שמקשר אותנו לציוד אחר (נתב, מתג, FW) ולכן את הפורטים הללו נגדיר כ-Trusted ואת השאר כ-Untrusted.

ואם למתג מתחבר מתג נוסף בתצורת זנב (כלומר אנחנו הגישה של המתג הנוסף אל הרשת) אז כמובן שלא נצפה לקבל בממשק שבינינו הודעות שמקורן בספק DHCP ולכן נגדיר את הממשק כ-Untrusted במתג המקומי וכ-Trusted במתג הזנב.

בנוסף לחלוקת המתג לאזורים, מנגון זה משתמש באמצעי אבטחה נוסף שנקרא "DHCP OPTION 82", כדי לוודא שהודעות ה-DHCP שמתקבלות מהשרת אכן עברו לפני כן דרך המתג כבקשות סטנדרטיות.

איך זה פועל? להודעות DHCP שמתקבלות מלקוח (כלומר מפורטים שהוגדרו כ-Untrusted), מוסיף המתג מידע כמו כתובת ה-MAC של הממשק וערך PORT-ID של הממשק וכאשר שרת ישיב להודעות אלו הוא יציין בהן את הערכים המקוריים, כך שהמתג יוכל לדעת שהודעות התשובה שהתקבלו הן עבור בקשות שאכן עברו במתג (לשם כך צריך שהשרת יתמוך ביישום).

> לידע כללי, OPTION 82 קיים לשימושים נוספים מלבד זה שציינתי, לדוגמא ניתן להשתמש בשדה זה יחד עם הגדרות נוספות בסוכן ובספק (כאשר עובדים בתצורה כזו) כדי שהסוכן יבקש מהשרת להקצות כתובות בטווח מסויים מה-POOL הכללי. מי שיתעניין בכך יהנה מכמה שזה מגניב למרות שמדובר בחקירה עד רמת הביט ומימוש מעט מסובך, כמו גם שיש שוני במימוש בין חברות התקשורת השונות.

ונעבור לפקודות:

- אפשור כללי של המנגנון במתג:

```
config-if# ip dhcp Snooping
```

- אפשור המנגנון ב-Vlan-ים מסוימים:

```
config-if#ip dhcp Snooping vlan [1,2,3]
```

(הערה: ברגע שמגדירים את אחת מהפקודות הללו, אוטומטית כל הממשקים הרלוונטיים יתפקדו כ"בלתי אמינים".)

- הגדרת ממשק כ"אמין":

```
config-if#ip dhcp Snooping trust
```

לקוח עויין

עד כה דיברנו על סוגיה שבה מתחברת לרשת, "שרת DHCP עויין", כעת נעבור לסוגיה נוספת (ואחרונה) שאדבר עליה, שנקראת "לקוח עויין".

מהו לקוח עויין? לקוח עויין יכול להיות כל ציוד שברגע שמקושר לרשת שלנו יוכל בעצם לגשת למירב המשאבים בדרך כזו או אחרת, או שיכול להפיץ וירוס או תוכנה זדונית אחרת שתטייל לנו ברחבי הרשת ותגיע לכל חלקיה. ל"לקוח" שכזה שמקבל אוטומטית וללא כל מאמץ גישה לרשת בעזרתו של שרת ה-DHCP האדיב יש פוטנציאל נפיץ ביותר, לכן מומלץ לתכנן מראש את הרשת כך שאם כבר נשתמש בשרת / ספק DHCP, נוודא שרק מורשי גישה יוכלו להתחבר לרשת ואם כבר התחברו מן הסתם שיכולותיהם

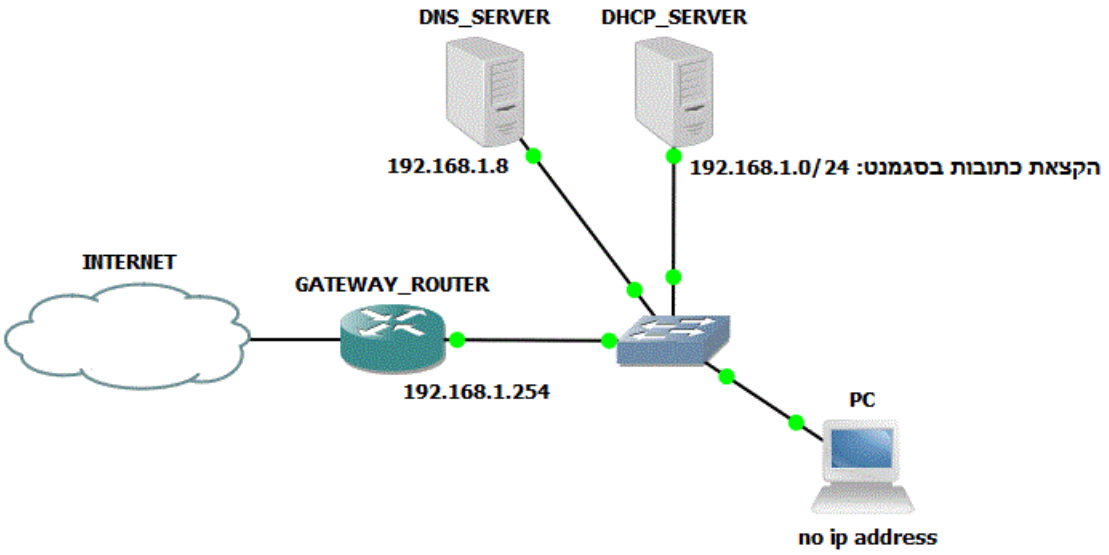
יוגבלו.

איך נממש פתרון הגנה תקשורתי?

- נשתמש בהקצאות סטטיות בספק ה-DHCP.
- לא נאפשר במתגים ממשקים שלא מחובר אליהם כלום, נגדיר ממשקים כאלו על VLAN מדומה כלשהו.
- נשתמש ב-Port-Security.
- נשתמש ב-Dot1X אם יש אפשרות ורצון לנהל את המנגנון הזה.

לכל אלו נוסיף כמובן אפיון חוקה מדוייקת ב-FW לסוגי התעבורה המאופשרים ברשת. בקיצור, לא חסרות לנו אפשרויות מימוש, רק לבחור ולהתחיל לעבוד.

סיימנו לדבר ועכשיו נחזור קצת לתכלס: אחרי שמימשנו והגדרנו את תצורת ה-DHCP שלנו, נתחיל להבין איך בעצם לנתח את הפלטים מפקודות ה-Show של DHCP. בואו ונזכר קודם כל איך נראית הרשת החביבה שלנו:



הפקודה הראשונה שלנו היא:

```
show ip dhcp server statistics
```

```
R1#sh ip dhcp server statistics
Memory usage         24504
Address pools        2
Database agents      0
Automatic bindings   1
Manual bindings      1
Expired bindings     0
Malformed messages   0
Secure arp entries   0

Message              Received
BOOTREQUEST          0
DHCPDISCOVER         6
DHCPREQUEST          6
DHCPDECLINE          0
DHCPRELEASE          8
DHCPINFORM           0

Message              Sent
BOOTREPLY            0
DHCPOFFER            6
DHCPACK              6
DHCPNAK              0
R1#
```

פקודה זו תציג לנו נתונים כלליים הקשורים לתפקידו של הציוד כספק DHCP, נוכל לראות מידע לגבי כמות הודעות שנשלחו/התקבלו ע"פ סוגן, כמות הקצאות, זיכרון בשימוש ועוד.

הפקודה השנייה שלנו היא:

```
show ip dhcp binding
```

```
R1#sh ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.1.5         0063.6973.636f.2d63.    May 06 2014 05:45 PM    Automatic
                    6330.342e.3131.3730.
                    2e30.3030.302d.4661.
                    302f.30
192.168.1.240       0063.6973.636f.2d63.    Infinite                Manual
                    6330.312e.3131.3730.
                    2e30.3030.302d.4661.
                    302f.30
R1#sh clo
R1#sh clock
17:35:17.087 UTC Tue May 6 2014
R1#
```

פקודה זו בעצם מציגה לנו את כל הקצאות ה-DHCP הקיימות שהנתב/מתג L3 מכיר בהן והקצה הוא בעצמו. בפלט שאני מציג לכם ניתן לראות 2 הקצאות לשני לקוחות, הקצאה אחת סטטית כפי שלימדתי במאמר הקודם, והקצאה אחת דינאמית שנבחרה מתוך POOL הכתובות.

העמודה הראשונה כמובן מציינת את כתובת ההקצאה, העמודה השניה מציינת את ערך ה-Client-ID של הלקוח שמצויין בהודעות ה-DHCP שהוא שולח (לפי ערך זה לימדתי שניתן לבצע הקצאה סטטית בציוד מבוסס IOS), העמודה השלישית מציינת את התאריך והשעה המדוייקים שבהם יפוג תוקף ההקצאה - שימו לב שעבור ההקצאה הסטטית מצויין ערך Infinite שמשמעותו היא שאין תוקף להקצאה ושהיא בעצם אינסופית. העמודה הרביעית Type שמה, מציינת את השיטה שבה בוצעה ההקצאה: אוטומטית או ידנית.

אם נרצה מכל סיבה שהיא לנקות את הטבלה הזו ובעצם לגרום לנתב/מתג L3 "לשכוח" את ההקצאות שביצע, נשתמש בפקודת:

```
Clear ip dhcp binding
```

שבהמשכה נציין את ההקצאה שברצוננו למחוק (אם נרצה למחוק את כל הטבלה, נציין כוכבית (*) בסוף הפקודה).

כמובן שלא מומלץ לבצע ניקוי סתם כך, אלא רק להקצאות שאנו יודעים בוודאות שכרגע אינן בשימוש ונשארו בטבלה כשתוקפן עדיין לא פג, משום שהלקוחות לא דיווחו על הויתור עליהן באמצעות הודעת RELEASE. הנתב/מתג L3 מבצע כל כמה זמן בדיקה של הקצאות שתם זמנן ומוחק אוטומטית במקרה הצורך. אציין גם שלא ניתן לנקות הקצאות סטטיות מהטבלה מן הסתם.

הפקודה השלישית שלנו היא:

```
show ip dhcp pool
```

```
R1#sh ip dhcp pool

Pool LAB :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 192.168.1.6          192.168.1.1      - 192.168.1.254     1

Pool client :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 1
 Leased addresses               : 1
 Pending event                  : none
 0 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 192.168.1.240        192.168.1.240    - 192.168.1.240     1
R1#
```

פקודה זו מציגה לנו את כל המידע הרלוונטי על ה-POOL-ים שהגדרנו בנתב/מתג L3.

הפקודה תציג לנו בין היתר: נצילות ה-POOL באחוזים, כמות כוללת של כתובות בטווח המוגדר, כמות הכתובות שכרגע מוקצות, טווח הכתובות ב-POOL, ומבחינתי הפלט הכי חשוב שמוצג כ-Current index ואומר לנו על איזו כתובת IP עומד כרגע האינדקס, כלומר מה כתובת ה-IP הבאה שתוקצה מתוך ה-POOL.

בנתב/מתג L3 אין בחירה אקראית של כתובות מתוך הטווח אלא הקצאה בסדר קבוע שמתחיל בתחילת הטווח, נגמר בסופו ומתקדם בקפיצות של 1. ברגע שהנתב/מתג L3 מגיע לסוף הטווח, האינדקס יקפוץ לכתובת הבאה הפנויה החל מתחילת הטווח.

סיכום

מנגנון DHCP הינו כלי מרכזי במימוש רשת גדולה ויעילה, יחד עם זאת הוא טומן בחובו לא מעט פירצות, שיש לקחת בחשבון ולדעת להתגונן מפניהן. השילוב של DHCP יחד עם רשת מאובטחת יתן לנו יתרונות גדולים מאוד אם נדע לנהל נכון את העניינים.

על המחבר

הנדסאי חשמל ואלקטרוניקה, בן 25 מאשדוד, בעל הסמכת CCNP, עוסק מזה 5 שנים בעיקר בתחום תקשורת הנתונים בשירות המדינה ויכול להגיד מניסיון שהתחום הזה לא מפסיק לגדול ולהתפתח וטוב שכך, זה משאיר אותנו (מי שאוהב את התחום) תמיד צמאים לעוד, ובידיעה שאף פעם לא חסרים דברים חדשים ללמוד עליהם.

לשאלות, טענות, עזרה, ייעוץ, תלונות וכו' - Tomy Shalev בפייסבוק.

על אבטחת מידע, עבר, הווה ועתיד

מאת חץ בן חמו (hetz@hetz.biz)

הקדמה

בין קוראי המגזין Digital Whisper ישנם רבים שמבינים באבטחת מידע, יש המבינים ברמה של Overview ויש מומחים המבינים עד רמת ה-packet בתקשורת ועד ה-Buffer overflow באפליקציות ובקוד. במאמר זה אנסה להתייחס ברמה שדי כללית, אולם אנסה "לנגוע" קצת יותר לעומק (עם הסברים) היכן שניתן.

תחום אבטחת המידע עובר טלטלה בשנים האחרונות, ומנהלים רבים עדיין לא מבינים זאת. תחושת ה"יש לנו חומת אש יקרה ומעולה" אופפת אותם, בו בזמן שחומת אש, כמה שתהיה משוכללת **אינה רלוונטית** במקרי פריצה רבים.

בשנים האחרונות מעבר לרמת ה-Firewall הבסיסי שנתן לנו הגנה ברמה של חסימת/פתיחת פורטים בצורה זו או אחרת, נכנסו חומות אש מסוג שונה, הלו הם ה-WAF (ר"ת Web Application Firewall) שחלקם הוטמעו במוצרי Firewall כמו Checkpoint, Fortinet ואחרים, ואילו חברות אחרות בנו WAF שיושב "מאחורי" ה-Firewall של החברה וכל מטרתו היא לנתח את התעבורה ולמצוא נסיונות פירצה, החל מ-SQL Injection, נסיונות כניסה מרובים מכתובת IP אחת ועד נסיונות התקפת DDoS (כאן המקום להזכיר שעם כל הכבוד לכל פתרון שנקנה ספציפית נגד DDoS, הפתרון לא יספק מכיוון שהתקשורת אל האתר כבר תהיה פקוקה ויש לפתור זאת ברמת ה-ISP). פתרונות ה-WAF עושים את עבודתם בצורה לא רעה וחוסמים חלק ניכר מה"האקרים" שברובם הם מה שנקרא "Script Kiddies" (אגב, בניגוד למה שרבים חושבים, Script Kiddies אינם ילדים שכותבים סקריפטים, רובם פשוט מורידים סקריפטים מוכנים ומשתמשים בהם, ותעיד העובדה שבפורומים רבים שאותם סקריפטים ניתנים להורדה, ישנם הרבה תלונות של אותם Kiddies על כך שזה "לא עובד" - מה שמראה שאותו Kiddie אפילו לא יודע את שפת הסקריפט).

כל הדברים שציינתי אינם חדשים לא לקוראים ולא למנהלי אבטחה. הבעיות מתחילות ברמה מעבר, ברמה ששום Firewall **לא עוזר**. ברמה של פריצה למחשב בודד אחד.

תכירו את שוקי

לשם המאמר, נכיר את שוקי, אדם שנשכר כדי לפרוץ לארגונים ולדלות מידע. שוקי הוא דמות פיקטיבית שמומצאת לצורך מאמר זה, ואני אציין ברמה עקרונית כיצד שוקי פורץ ובהמשך המאמר אסביר מה מחלקת האבטחת מידע צריכה לעשות כדי להתגונן נגד שוקי. (אגב, אני איננו שוקי, ואיננו פורץ, גם לא בתשלום או בחינם).

הלקוחות של שוקי הם בד"כ ארגונים שפונים דרך צד שלישי כדי להסתיר עקבות. נניח שחברת התוכנה (הפיקטיבית) Micro Code 2000 נמצאת בקשיים ואילו המתחרה שלה Server Code מציגה בדוח"ות הרבעוניים רווחים נאים ועליה של עשרות אחוזים במכירות מדי רבעון. ב-Micro Code ניסו הכל, החל בהעתקת המוצר של המתחרה, שיווק אגרסיבי, הנחות ענק לעוברים מהמוצר המתחרה ועוד, אולם בינתיים רווחים גדולים עדיין לא הגיעו ל-Micro Code ובהנהלה החליטו שהם מעוניינים במידע "מבפנים" מה קורה אצל המתחרים. הם ניסו לעבוד בשיטה הידועה של "חטיפת" עובדים בכירים מהמתחרים, אולם הנסיונות כשלו ואותם אלו שקיבלו פניה מ-Micro Code "לערוק" - סירבו בנימוס.

מישהו מההנהלה מחליט לפנות לבחור שהוא מכיר (נקרא לו יקי) כדי שימצא מישהו ש"יציץ" ויעביר מידע רגיש של המתחרים ל-Micro Code. סוג המידע? פרטים על לקוחות של Server Code, מחירים לא רשמיים, תוכניות עתידיות של החברה, אסטרטגיות שיווקיות. קוד מקור של Server Code אינו כל כך חשוב אבל אם גם זה יגיע לידי Micro Code הם לא יתלוננו על כך. יקי שומע, ומבקש סכום התחלתי כדי למצוא מישהו ולשלם לו. מתבצעת העברה כספית בצינורות אחוריים של כמה עשרות אלפי דולרים. יקי גוזר קופון שמן ופונה לשוקי עם ההוראות.

עתה נמנה אותך, קורא יקר, למנהל האבטחת מידע של Server Code. שוקי **הולך לפרוץ ולגנוב מידע ממך**. איך הוא הולך לעשות זאת? או, טוב ששאלת. ישנם מספר דרכים.

הדבר הראשון ששוקי יעשה הוא מחקר מקיף לגבי מי האנשים שנמצאים בחברה, מה תפקידם ומה כתובת המייל שלהם. לשם כך הוא ישתמש בגוגל, יוטיוב, לינקדין ואתרים אחרים - הכל על מנת לדלות את המידע ולבנות לעצמו מעין עץ של בעלי תפקיד ב-Server Code. לאחר שהוא בנה, הוא ישיג את כתובות המייל שלהם.

מכיוון ששוקי קיבל כמות כספים רצינית, הוא יכול לפנות לכל מיני אתרים ב"שוק שחור" (רבים חושבים שמדובר ב-Dark Web אבל במקרים רבים באתרי אבטחה רבים ניתן ליצור קשר פרטי ו"חברי" עם כל מיני פורצים כדי לרכוש מהם פריצות למוצרים שונים, כל עוד הפריצות לא דווחו ואינם מפורסמים בשום מקום. ביטקוין היא צורת התשלום הרצויה. מה לעשות, יש עדיין כאלו שחושבים שביטקוין הוא אנונימי) כדי לרכוש פירצה. הוא יוצא מתוך הנחה שבחברה מותקן אצל אותם מנהלים ה-Adobe Reader והוא יוצר

קובץ PDF מיוחד שמשתמש באותה פירצה לא ידועה כדי לשתול Loader קטנטן במחשבו של אותו מנהל. אותו Loader מהרגע שהוא יופעל (בכך שאותו מנהל יפתח את קובץ ה-PDF הנגוע) יטען כבר את החלקים האחרים של האפליקציה ששוקי כתב/גנב/השאיל/שינה כדי להקים מעין Shell קטנטן בתוך אותו מחשב.

מהרגע שאותו Shell רץ, לשוקי יש גישה למחשבו של אותו מנהל. מה עם ה-Firewall של החברה או כל משהו באמצע? הם **לא רלוונטיים** כי שוקי משתמש באותם הגדרות שאותו מנהל גולש (לדוגמא - אם יש Proxy באמצע, גם ה-Shell של שוקי ישאב מידע דרך הפרוקסי). שוקי מספיק חכם כדי למצוא מה הפורטים הפתוחים וכיצד הוא יכול לבנות Tunnel בינו לבין מחשבו של המנהל (סביר להניח שיהיה מעורב שרת באמצע שנמצא באמזון או אצל כל ספק שרותי VPS/ענן כלשהו כדי לטשטש עקבות).

מכיוון ששוקי פרץ למחשבו של המנהל, יש לו מיידית גישה לקבצים שיווקיים, כך שאסטרטגיות שיווקיות, מבצעים ומידע על מוצרים עתידיים זמין לו כבר עכשיו והוא יכול בשמחה להוריד אותם ולמסור אותם ליקי, אבל שוקי לא עוצר כאן, הוא רוצה להיות "מגובה" כך שאם המחשב שהוא פרץ אליו הוא Laptop שהמנהל לוקח הביתה ומנותק מה-LAN של החברה, שוקי יוכל לגשת גם ממחשב אחר בחברה. לשם כך הוא רוכש עוד פרצה שעדיין לא פורסמה ל-Windows והוא פורץ לעוד 3-4 מחשבים ומתקין גם שם את אותו Shell. שוקי עכשיו לא צריך לשבור את הראש על ה-Firewall הארגוני או כל כלי הגנה אחר שמגן על התנועה מבחוץ. **הוא כבר בפנים** וכל מה שהוא צריך לעשות הוא להעביר את המידע בצורה שלא תגרום לאחת ממערכות ה-IPS/IDS לחשוד. איך עושים זאת? די פשוט: שותלים Header ("ראשן") כאילו מדובר בקובץ וידאו קובץ של תמונה גדולה ובמשכו ה-DATA בצורה מוצפנת (ה-Shell יכול להצפין). מבחינת מערכות ה-IPS/IDS, המנהל שולח תמונות שהוא צילם או מעלה וידאו. הן **לא תתרענה** על בעיות.

שוקי לא עוצר כאן, שוקי **רוצה לראות קוד**, אבל איך הוא יוריד קוד? למנהלי שיווק והנהלה בכירה בד"כ אין שום נגיעה לקוד, בוודאי שלא ל-Source Repository כלשהו (Source Safe, SVN, GIT וכו'). אז מה הוא יעשה?

הוא יתחיל לסרוק את מחשבי החברה. הוא לא יעשה זאת בצורה גורפת (שוב, הוא לא מחפש "להעיר" את שרת ה-IPS/IDS), אלא לאט לאט. אם לדוגמא מוצר החברה רץ על לינוקס, הוא יחפש מכונות שיש להן Port-22 פתוח. המוצר מבוסס על Windows? הוא ינסה לפרוץ למכונות Windows אחרות תוך חיפוש קוד בהן ואם מנהל הרשת היה עצלן ולא הגדיר הרשאות מוגבלות למחלקות שונות, אז הוא בכלל "יחגוג" על ה-File Servers השונים ויוריד כמה שיותר.

וכאן נמצאת חולשה שקיימת **בחברות רבות** אך לא תמיד זוכה ליחס מצד אבטחת המידע (שוב, אשליית ה-Firewall "החזק" שמגן): במחלקות R&D רבות שמשתמשות לדוגמא בלינוקס, המפתחים מבטלים מנגנוני אבטחה כמו חומת אש פנימית (iptables) או מנגנוני אבטחה מבוססי Kernel (כדוגמת SELinux),

מה שאומר שכל מה ששוקי צריך לעשות זה לפרוץ למכונת Windows אחת שרץ עליה Putty עם מפתחות או SecureCRT, להעתיק את הפרופיל **ובמכה אחת יש לו גישה להרבה מכונות לינוקס בלי לשבור את הראש על סיסמא**. לפעמים הוא כלל לא יצטרך זאת אם המשתמש שומר קבצי מקור בכונן C מקומי ואז לשוקי יש בכלל חיים קלים.

זו היתה השיטה הראשונה. נעבור לאופציה אחרת ששוקי לא מצליח לפרוץ למחשב דרך שליחת קובץ PDF נגוע (מה לעשות, המנהל שהוא שלח אליו את המייל כבר לא נמצא ב-Server Code או שאשכרה מישהו עושה צעדי מנע כדי לתקוף את הבעיה של חולשות בקבצי PDF). איך שוקי יצליח לחדור?

כאן אנחנו מגיעים ל"מימד האנושי". שוקי יתחיל לחפש עבודות באותה חברה. לא משנה מה העובדה, העיקר שהוא יוזמן לראיון עבודה. לא, בזמן הראיון הוא לא יגע במחשב. כל מה שהוא עושה הוא שולח קורות חיים (מפוברקים כמובן) למנהלת כח האדם בחברה (לא קובץ נגוע).

סביר להניח ששוקי יזומן לראיון. הוא יגיע לחברה, ישב וישוחח עם החברה ובמהלך השיחה הוא יזכיר בהתלהבות אתר חדש שהוא "שמע" עליו. אתר מ-ה-מ-ם שהיא ח-י-י-ב-ת לראות אותו! מנהלת כח האדם סקרנית והיא פותחת דפדפן. שוקי מכתיב לה את שם הדומיין ואכן יש אתר. מהמם? שאלה טובה, אבל אם נסתכל על שוקי, נראה שהוא מחייך. מדוע שוקי מחייך?

כי את אותו אתר "מהמם" בנה שוקי. כשמנהלת כח האדם נכנסה אליו, היא נכנסה לאתר שסורק בעצם את הדפדפן ומנסה עליו פריצות שונות, הכל לפי הידע והפריצות ששוקי קנה. השרת של שוקי לא מצליח לפרוץ? אז הוא יתן למנהלת כח האדם הודעה שנגן ה-Flash שלה ישן ויש להתקין את הקובץ הבא. מה לכל הרוחות מבינה מנהלת כח אדם בגרסאות Flash? כלום, אבל שוקי כבר יעודד אותה להוריד ולהריץ. תודות לתמימותה של המנהלת, לשוקי יש עכשיו גישה מרחוק.

הדבר הראשון ששוקי יעשה לאחר שיגיע לביתו ויתחבר מרחוק (דרך אותה אפליקציה שהמנהלת התקינה) הוא לשאוב את ה-Contact List כדי שידע בדיוק למי לגשת. אם הוא רוצה לפרוץ לשאר המחשבים, הוא יכול לשלוח דרך כתובת המייל שלה **בשימוש בשרת הפנימי** אימייל עם אותו פריצת PDF שאינה ידועה עדיין ובכך להשיג השתלטות על מחשבים אחרים וכך הוא יוכל לגנוב מידע וקוד.

נעזוב עתה את שוקי ונחזור למציאות שלנו. אומר לכם משהו פשוט: **רוב החברות עדיין לא יודעות להתמודד מול שוקי**. אנשי אבטחת מידע רבים, לצערי, מנסים לחשוב על אבטחת מידע באופן סיסטמתי בשעה שמחשבה נכונה על אבטחת מידע צריכה להיות **הכל חוץ מסיסטמתי**. שוקי נשכר לפרוץ אליכם והוא מעוניין להרוויח כסף, לא להחזיר אותו. Micro Code תשכור דרך יקי מישהו אחר אם שוקי לא יצליח כי הם רוצים בכל דרך לעקוף את Server Code.

עניין ה-R&D שהזכרתי לעיל, לדוגמא, הוא עניין שאישית ראיתי בחברות קטנות וגדולות כאחד. מפתחים רוצים לנסות משהו ומעיפים כל הגנה בסיסית. קבצים נכתבים עם מקסימום הרשאות (כי ה-Apache לא נותן כתיבה אז פותחים הכל ל-777!), אין הפרדת משתמשים והסיסמאות הן מגוכחות בפשטותן ואינן מוחלפות. עדכוני אבטחה שאמנם מיושמים על שרתי פרודקשן **במקרים רבים כלל לא מיושמים** על מכונות D&R וכך לאותו שוקי תהיה עבודה מאוד קלה בשאיבת הקוד ואם הוא ירצה - בגרימת נזק.

איך מתגוננים? נתחיל בעניין חולשות ה-PDF וחולשות קבצים אחרים. רובם בד"כ מגיעים דרך האימייל.

אז מה ניתן לעשות?

איך מטפלים בכך? אם לדוגמא יש לכם שרת Exchange אז כדאי שתשתמשו במוצר כזה או כזה שמתחבר ל-Exchange ושומר את ה-Attachments בתיקיה נפרדת כך שהמייל מגיע למשתמש ללא ה-Attachment, רק HTML של המייל.

כאן אני ממליץ להרים שרת לינוקס פשוט ולהתקין עליו ImageMagick ולבצע "חיבור" בין אותה תיקיית Attachment לבין הלינוקס, ובעזרת סקריפט פשוט להריץ Convert **לכל קובץ** שמגיע והוא ברמת סיכון שהוא כולל פירצה. כך לדוגמא קובץ PDF אפשר לבצע לו convert ל-PNG או לבצע המרה לאותו פורמט ומכיוון שהלינוקס יוצר את הקובץ, הוא אינו כולל קוד זדוני (קבצי אופיס ניתן להמיר עם ooo-thumbnail של Open Office או Libre Office), ולאכסן את הקובץ שנוצר במקום הקובץ המקור. את הקובץ המקורי נעביר לתיקיה אחרת כך שאם המשתמש ירצה, הוא יוכל בעזרת קישור במערכת להגיע אליו. בעזרת מערכת פשוטה כזו גם אם שוקי ישלח קובץ PDF (או קובץ וורד/אקסל/פאואר-פוינט) נגוע, המשתמש יראה במייל טקסט כלשהו כתמונת PNG או כקובץ PDF רגיל. אם שוקי שלח שטויות ב-PDF, אז אותו מנהל יגחך ויזרוק את המייל, לא בוצעה חדירה. את הקבצים המקוריים ניתן יהיה להשמיד לאחר מספר ימים או לפי הנוהלים של החברה. מבחינת אחסון ושרת, אין צורך במשהו עוצמתי, תספיק מכונת לינוקס פשוטה ו-RAID של מספר דיסקים גדולים עם חיבור SATA הואיל ואין צורך כאן בכתיבה/קריאה מהירה.

מבחינת הורדת קבצים ע"י המשתמשים, כדאי לארגן את התצורה כך שהם ירדו לתיקיית רשת עם עדיפות שיראו ב-Viewer פנימי. לכרום ופיירפוקס ישנו Viewer של PDF כך שהם אינם צריכים את התוסף של אדובי מותקן בדפדפן (אפשר, שוב, לחבר את אותו שרת לינוקס לעיל כדי שימיר אוטומטית קבצים שיורדים בפורמטים פופולריים לתמונות או שיצור אותם מחדש - ויתן למשתמש את הגירסה המומרת ורק אם צריך - את קבצי המקור). קבצי EXE או כל קובץ שהוא מסוג Executable שיורדו ע"י משתמש יעברו אישור של אבטחת מידע או כל גורם מוסמך אחר בחברה.

בשיטות אלו אנו מונעים משוקי גישה. השיטה היא כמובן אינה Bullet Proof (שוקי עדיין יכול לקבוע פגישה ולתת Disk On Key לאחד המנהלים ולהדביק את מחשבו של המנהל לדוגמא), אבל היא חוסכת למנהלי המערכת הרבה כאב ראש.

ועכשיו אשאל אותך קורא יקר שאלה: כיצד הינך יודע ששוקי (או דומים לשוקי) לא קיימים אצלך במערכת? כל מנגנוני האנטי וירוס למינהם עובדים בתצורה של חתימות או זיהוי סוגים שונים של תולעים ונוזקות אחרות, אך הם אינם יודעים להתמודד עם פריצות שלא פורסמו, שבוודאי עדיין לא ננעלו ע"י יצרן התוכנה.

הטריק שאני משתמש הוא טריק פשוט: קח סופ"ש או חג וקבע אותו כיום שהמשתמשים **לא מכבים** את המחשבים שלהם. הם עושים Logout וזהו ואם אפשר, אנשים שמשתמשים במחשבים ניידים, שישאירו אותם בחברה במצב **פעיל**. למשך החג או לילה או סופ"ש שמור את הטראפיק שיוצא ונכנס (או לפחות את הלוגים שלו) וכשתחזרו לעבודה, עברו על הלוגים, תראו מי נכנס ומי יצא ובמיוחד מאלו מחשבים/שרתים. חלק מהתעבורה הוא "כשר" (כמו עדכונים שיורדים) אולם יכול להיות שחלק מהתעבורה מגיע למקומות שאתה לא בטוח שהם "כשרים". לכתובות האלו תבצע בדיקת PTR (כדי להמיר כתובת IP לכתובת DNS שמית) ואז יהיה יותר קל לבדוק זאת. פורצים רבים מנצלים את סופ"ש/חג/לילה כדי לבצע העברות, וכך תוכל לדעת אם יש דברים לחקור.

והנה נקודה שאני חוזר ואומר שוב ושוב: מצאת טראפיק חשוד? **אל תתקוף את הפורץ בחזרה**. לפעמים אותו שוקי נעקב בעצמו ע"י גורמי בטחון שונים מהארץ ו/או מחו"ל ותקיפה שלך רק תדפוק עבודות מעקב שונות. אם אתם ארגון גדול, פנה למחלקת הבטחון ושהם יפנו למז"פ/עבירות מחשב במשטרה. אם אתם ארגון קטן, פנו ישירות למשטרה. חשוב שתשמור כל לוג או כל טראפיק שיש לך ואם אתה יודע מהו המחשב הנגוע, שמור את הטראפיק ממנו/אליו. אני יודע שרבים צוחקים על מחלקת פשעי המחשב של המשטרה (ללא הצדקה, אגב, המצב שהיה בעבר הרחוק השתנה לגמרי כיום, ואני מדבר ספציפית על המחלקה הזו ולא על פדיחות שנעשים ע"י מחלקות אחרות בתביעות של פורצים) אבל בכל זאת - לכו by the book.

העתיד בכל הקשור לפריצות אינו מביא בשורות טובות. אדרבא, הוא מביא כאב ראש לא קטן למחלקות הסיסטם ואבטחת המידע יחד. בסוף מאי eBay, חברה שיש לה נסיון גדול מאוד באבטחת מידע - הודיעה שפרצו לבסיסי הנתונים שלה. אמנם הפורץ לא הצליח להשיג את המפתחות לפתיחת ההצפנה וקיבל ג'יבריש בתור dump, אבל עדיין - פורצים מצליחים להגיע למקומות רבים באותם שיטות ששוקי לעיל השתמש.

"הדור הבא" של פריצות, לדעתי, יהיה יותר מוטה חומרה. כיום ישנן מערכות לינוקס משובצות בגודל של קופסת סיגריות (כולל סוללה) עם חיבורי RJ45 פנימה והחוצה, כך שניתן לחבר אותן מתחת לשולחן לכניסת הרשת של PC, אותו ציוד יתחזה מבחינת MAC Address כ-PC (כך שלא תוכלו לדעת דרך ה-Switch בדיוק מה קורה אלא אם תבצעו Sniffing) כך שהפריצה מרחוק תהיה יותר קלה לפורצים. כל מה שצריך זה לתפוס עמדת מידע כלשהי שמחוברת ל-LAN, להתקין את הקופסא ולחבר לחשמל (ולהטעיה יש כאלו שאפילו ישימו מדבקה עם לוגו של החברה הנפרצת על מנת להטעות עובדים שאינם מבינים בנושא). חושבים ש-Offline מוגנים? תחשבו שוב: ישנן קופסאות לינוקס (עדיין לא יצאו רשמית, אגב) שלא רק מציעות 2 חיבורי רשת אלא גם חיבור WIFI בתדר 2.4 או 5 ג'יגהרץ, השידור יקלט ע"י מודם סלולרי שמוחבא מחוץ לדלת החברה (ה-SSID חבוי והתקשורת מוצפנת) והמודם הסלולרי מחובר ל-G3 כך שכל מה שהפורץ צריך לעשות זה להתחבר למודם הסלולרי שמתחבר לקופסא - ומשם לעשות כרצונו.

מי המטרה של פריצות עתידיות כאלו? כל חברה גדולה שיש לה מתחרים מאוד שאפתניים **וגם חברות ביטוח ובנקים**. המחיר של הציוד זול, זול מאוד אפילו: קופסא כזו יחד עם מודם סלולרי לא יעלו יותר מאלפי שקלים בודדים והפיתוי לפורצים הוא גדול, מה שיצריך מחשבה מחדש מבחינת מחלקות אבטחת מידע כיצד ניתן להגן על התשתית והמידע, ואם מישהו חושב שהוא מוכן, שיזכר בבקשה מתי הוא עבר על שקעי ה-RJ45 וראה מה מחובר למה ומתי הוא עשה סריקה של תדרים 2.4 ו-5 ג'יגהרץ לאחרונה.

לסיכום

עולם ה-Cyber Crack **רק גודל**. זה מגיע אלינו מאוחר, אבל הגיע. שום ארגון שהכניס לתוכו כל מיני "קופסאות פלא" **אינו מוגן** כפי שהוא חושב, ועם מזעור חומרות פריצה ומערכות משובצות, גילוי הפרצות יהיה יותר מורכב ויצריך מחשבה מחוץ לקופסא. לא חסרים גורמים שירצו את המידע שיש ברשותכם, החל ממתחרים מקומיים ועד חברות ענק בינלאומיות וכלה במדינות שבהן ה"ספורט הלאומי" הוא פריצות כדי להשיג מידע (סין, NSA בארה"ב וכו'), ואם אתם רוצים להגן, תחשבו בצורה יצירתית.

על המחבר

שמי חץ בן חמו, אני פרילאנסר ואני עוסק בתחומי לינוקס, וירטואליזציה ואבטחת מידע. ניתן ליצור איתי קשר במייל hetz@hetz.biz ובטלפון: 054-5297156. בנוסף, אני כותב בבלוג "כמה מילים, ברשותכם".

iBanking מבצרת עמדות

מאת עמי קאופמן, מנתח מודיעין איומי ב-RSA

הקדמה

בעולם פשעי הסייבר צריך תמיד להזהר. הגנבים עושים מאמצים כבירים כדי לחמוק מעיניהם הבוחנות של אנליסטים ורשויות החוק, זאת כדי למנוע את סגירת המיזם שלהם או גרוע יותר - מעצר. המפתחים של הסוס הטרויאני iBanking - אפליקציה זדונית הפוגעת במכשירי אנדרואיד - אינם יוצאים מן הכלל. בדומה לתוכנות דומות הפוגעות במחשבים האישיים ומיישמות מנגנוני הגנה כגון ערפול קוד (Obfuscation) ושימוש בהצפנה חזקה, גם בגרסאות האחרונות של iBanking נלקחו צעדים להקשחת התשתית של התוכנה הזדונית והפעלתה.

למרות שקוד המקור של התוכנה הודלף לפני מספר חודשים, האפליקציה עדיין נמצאת תחת פיתוח מתמשך וכיום מציגה יכולות חדשות, כגון מעקב אחר כל האפליקציות המותקנות על המכשיר הנגוע, איסוף תמונות ומידע על מיקום גיאוגרפי מדויק. כדאי לציין גם את התמיכה הגדלה המאפשרת תקיפת יעדים נוספים: הניתוח האחרון שלנו זיהה כ-30 שבלונות "גרפיות" ל-iBanking הדומים לאפליקציות או אתרים של גופים פיננסיים שונים. אך החידוש המעניין ביותר הוא ללא ספק השימוש במנגנון הגנה העצמית כגון קידוד AES, בערפול קוד ובאנטי-SDK/VM.

מנגנוני הגנה עצמית

הניסיונות הגוברים של מפתחים להמנע מגילוי הם חלק טבעי באבולוציה של תוכנות זדוניות. ככל שמנתחי האבטחה מפתחים את שיטות הניתוח וגילוי שלהם, מפתחי התוכנות הזדוניות ממהרים להפעיל צעדי מנע להגנה על פעילותם ושמירה על חשאיותם. בדומה לקידוד FUD בסוסים הטרויאנים הפוגעים במחשבים אישיים, iBanking כיום משתמש בשיטות הצפנה חזקות יותר כדי להגן על קוד המקור שלו מניסיונות הינדוס חוזר וגילוי על ידי אנטי-וירוס. האפליקציה גם מיישמת הגנת אנטי SDK כדי להתחמק מסביבת הניתוח בארגזי חול. כמו בכל דבר הקשור למובייל, התפתחויות אלו התרחשו מהר מן הצפוי.

קידוד AES

הניסיון הראשון של iBanking בהגנה עצמית הופיע כקידוד AES. כדי להסתיר את המקורות השונים שלו, iBanking השתמשה במפתח פרטי בקידוד קשיח (בתוך האפליקציה) שקידד את התוכן של קבצי XML ושל מקורות התקשורת. קבצי XML מכילים מידע הקשור למקורות חיצוניים כגון תמונות, אך גם מידע הקשור להגדרות האפליקציה. כפי שנאמר, האפליקציה גם עשתה שימוש בהצפנה עבור מקורות התקשורת שלה, כולל כתובות URL ומספרי טלפון לשליטה.

```
<resources>
    <string-array name="adm_domens">
        <item>4338aa1dc5facbdd4ec0b8be27e4ccb4</item>
        <item>6388995b4c309de03aa68ac12c9b4ff5</item>
        <item>942a7d4f210ad5e1db0c015a4726771e</item>
        <item>11412065eb093a3ade1c4825b64e6d16</item>
        <item>22a5ed85e999ace9c23a870822fda2a3</item>
        <item>9e2d6f1bd13eec8af0c19ef85e16ae55</item>
        <item>0d4a2ebf7fd4b5659a83e951d1aea77b</item>
        <item>4af46d70be43642f4a2bb74c44913ae2</item>
        <item>30679f21a7676ec32650a119b8bb5180</item>
    </string-array>
</resources>
```

[מקורות תקשורות בקידוד AES, מקור: https://blogs.rsa.com/ibanking-mobile-bot-raising-shields/untitled-37]

ערפול קוד האפליקציה

השלב הבא בניסיונות ההתחמקות היה ערפול הקוד. לאחר שעקבנו מקרוב אחד הודעות המפתח בפורומים מחתרתיים, גילינו גרסה חדשה של iBanking שבמבט ראשון נראה כמלא שגיאות שגרמו לקריסתה. הניתוח שביצענו הראה בסיס-קוד ותשתית חדשים לגמרי.

לאחר שבוצע הינדוס-לאחור (Reverse Engineering) של האפליקציה, גילינו הפתעה לא נעימה. במאמץ לבצר עוד יותר את האפליקציה מההינדוס החוזר, המפתח השתמש בערפול קוד כדי להקשות על ניתוח הקוד. לאחר היישום, ערפול הקוד הגדיל את מספר קבצי ה-JAVA מ-23 ל-245 והקצה שמות אקראיים לקבצים החדשים. יתרה מכך, הערפול החליף את שמות המשתנים הסטטיים למחרוזות חסרי משמעות ולערכי מחרוזת מקודדים. כפי שניתן לראות בתמונה מטה, המערפל חכם מספיק דיו להמנע מהצפנה/ערפול משתני מערכת, כגון "app_name". הצפנת המחרוזות נעשתה באמצעות פונקציה בקידוד קשיח ופשוטה יחסית.

[משתנים שעברו ערפול והערכים המקודדים החדשים, מקור: https://blogs.rsa.com/ibanking-mobile-bot-raising-shields/untitled-38/]

מנגנון אנטי-SDK

למרות זאת, אותו ערפול מדובר לא סיפק הסבר המניח את הדעת להימצאות השגיאות באפליקציה ולקריסה. תהליך דה-באגינג רחב של האפליקציה חשף מנגנון הגנה אנטי- SDK מחוכם, שניתן להשוות למנגנון הקיים נגד ארגזי חול בתוכנות הזדוניות הפוגעות במחשבים אישיים.

הניתוח שלנו חשף כי בשלבים המוקדמים של הפעלת האפליקציה היא מריצה פונקציה המשווה מזהים ייחודיים שנאספו מהמכשיר הנגוע עם ערכים בקידוד קשיח. התאמה עם אחד מערכים אלו "יגלה" לאפליקציה שהיא מופעלת בתוך מכשיר וירטואלי ותגרום להפסקה מיידית של פעילותה. אנו זיהינו את ארבעת הערכים הבאים:

1. האם EMEI המכשיר שווה "000000000000000"?
2. האם מספר הטלפון מתחיל ב-"1555521"?
3. האם המפעיל הוא "Android"?
4. האם המספר הסידורי של ה-SIM שווה ל-"89014103211118510720"?

אם התשובה לאחת משאלות אלה היא "כן", האפליקציה מפסיקה את פעילותה באופן מיידי ומדמה קריסה. הערכים בקידוד קשיח מתכתבים לערכי ברירת המחדל המסופקים בדרך כלל על ידי SDK של אנדרואיד ומיושמים באופן שכיח בסביבות לניתוח אפליקציות.

```
SharedPreferences var3 = PreferenceManager.getDefaultSharedPreferences(this.getApplicationContext());
String var4 = ((TelephonyManager)this.getSystemService("phone")).getDeviceId();
if(this.getResources().getString(2131034115).equals("1")) {
   label141:  {
      if(!var4.equals("000000000000000")) {
         TelephonyManager var77 = (TelephonyManager)this.getSystemService("phone");
         String var78 = var77.getLine1Number();
         String var79;
         if(var78 != null && !var78.toString().trim().isEmpty()) {
            var79 = var78;
         } else {
            var79 = var77.getSubscriberId();
         }

         if(!var79.startsWith("1555521") && !this.c().equals("Android") &&
            !((TelephonyManager)this.getSystemService("phone")).getSimSerialNumber().equals("89014103211118510720")) {
            break label141;
         }
      }

      Process.killProcess(Process.myPid());
   }
}
```

[פונקציית השוואת אנטי SDK - ניסיון למנוע ניתוח דינאמי, מקור: https://blogs.rsa.com/ibanking-mobile-bot-raising-shields/untitled-39]

סיכום

מפתחי התוכנות הזדוניות למחשבים אישיים, בהיותם ערים לנוכחות גוברת של מנתחי אבטחה, מיישמים מזה זמן מנגנונים שונים נגד גילוי וניתוח התוכנות שלהם. אך שיטת פעולה זו לא הייתה ההנורמה עד היום בתוכנות זדוניות לנייד. תוכנת iBanking מראה כי מפתחי התוכנות הזדוניות נהיו ערים גם לצורך להגן על המכשירים הניידים הנגועים שלהם. ייתכן כי תופעה זו מסמנת טרנד חדש בזירה המתפתחת של תוכנות זדוניות לנייד.

הניתוח המתמשך שלנו ל-iBanking חושף תוכנה זדונית מפותחת ובוגרת הפוגעת במכשירי אנדרואיד. אנו עדים לכך כי Botnets רבים החלו להשתמש בה על מנת להשתלט על סמארטפונים, וזוהי מגמה שאנו ממשיכים לעקוב אחריה.

דברי סיכום

בזאת אנחנו סוגרים את הגליון ה-51 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 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"

אם הכל יעבור כשורה, הגליון הבא ייצא ביום האחרון של חודש יוני.

אפיק קסטיאל,

ניר אדר,

31.05.2014