Official Malware Report

Malware Reverse Engineering part1 of 2. Static analysis

Contact info	
Report:	**Malware reverse engineering part 1. Static analysis**
Author:	*Rick Flores Security Engineer II*
Follow me on twitter:	*https://twitter.com/#!/nanoquetz9l or simply @nanoquetz9l*
Website:	www.nanotechfibers.com
Greetz to:	San Diego eXploit Team, eXploitSD, iqlusion, and isomorphix

Revision Summary				
Rev	**Description of changes**	**Changes by:**	**Review / Approval by:**	**Date**
1.0	Malware reverse engineering part 1. Static analysis	*Flores, Rick*	*N/A*	01/06/2012

Report Details			
Infected user	**Computer Name**	**Malware Analyst**	**Date**
Anonymous	Dumpbin-0425x8F.anonymous.local	*Flores, Rick*	01/06/2012

Table of Contents

1. SCOPE

This malware report is part 1 of 2. Part 2 will focus heavily on dynamic analysis, determining packers/encryption used and finding original entry point (OEP) of the malware sample, and will utilize IDA Pro, and Immunity de-bugger extensively. We will also bypass anti-debugging, and anti-reversing tactics employed by attackers, and malware authors in part 2. Stay tuned!

This report is an effort to track, categorize, contain, understand root cause and infection vector of said user account/s, networked equipment or computer/s. This report pertains to all incidents reported by TIER II help desk, TIER III engineers, customer complaints or random IT Security audit/finding/pen test.

2. INVESTIGATION GOALS

Determine extent of infection, network risk, determine risk of data exposure, figure out infection vector and propogation methods, etc.

3. MALWARE SAMPLES ANALYZED

3.1 Win32 Kryptik.YJA trojan variant *40dbdf4b-7db5306a.exe*

MD5 : f0d0872763058e047922ead2474943ec

SHA1 : 5629f91e72401440024ec170430e60f50d4f4590

SHA256 : b811b4089b36660ae089db8a7c61f2d9dc1ebfeb367ac51e55585ec8eaf1d77a

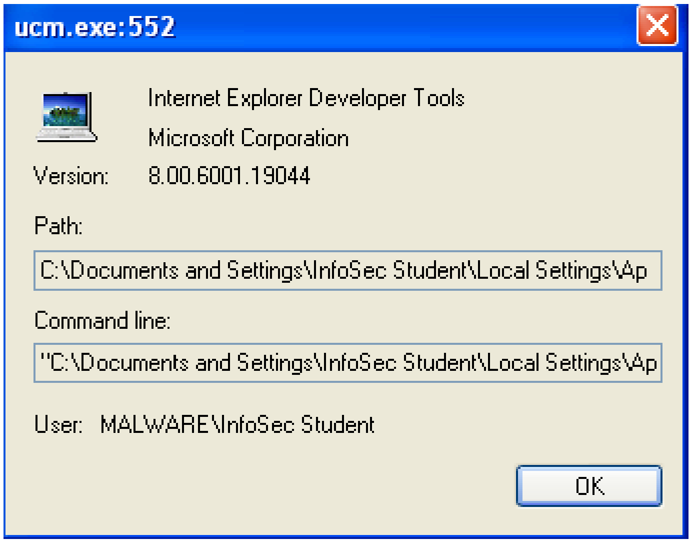
3.2 Location C:\Documents and Settings\anonymousvictim\Local Settings\Temp\40dbdf4b-7db5306a.exe

3.3 Moving forward, and for brevity I will be referring to "40dbdf4b-7db5306a.exe" simply as the malware sample. When you read `malware sample` in the remainder of this report, safely assume I am referring to 40dbdf4b-7db5306a.exe which is the malicious sample used as the basis of this malware report.

3.4 Malware Sample properties. Note the Internet Explorer Developer Tools information recorded, and Original File Name : "iedvtool.dll"

```
"CompanyName", "Microsoft Corporation"
"FileDescription", "Internet Explorer Developer Tools"
"FileVersion", "8.00.6001.19044 (longhorn_ie8_gdr.110211-1700)"
"InternalName", "iedvtool.dll"
"LegalCopyright", "© Microsoft Corporation. All rights reserved."
"OriginalFilename", "iedvtool.dll"
"ProductName", "Windows® Internet Explorer"
```

```
"ProductVersion", "8.00.6001.19044"
```



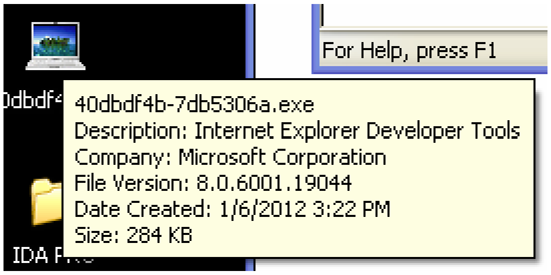
ucm.exe:552

Internet Explorer Developer Tools
Microsoft Corporation
Version: 8.00.6001.19044

Path:
C:\Documents and Settings\InfoSec Student\Local Settings\Ap

Command line:
"C:\Documents and Settings\InfoSec Student\Local Settings\Ap

User: MALWARE\InfoSec Student



40dbdf4b-7db5306a.exe
Description: Internet Explorer Developer Tools
Company: Microsoft Corporation
File Version: 8.0.6001.19044
Date Created: 1/6/2012 3:22 PM
Size: 284 KB

4. MALWARE ANALYSIS METHODOLOGY, SOFTWARE, AND SECURE LAB SETUP

Malware Methodology

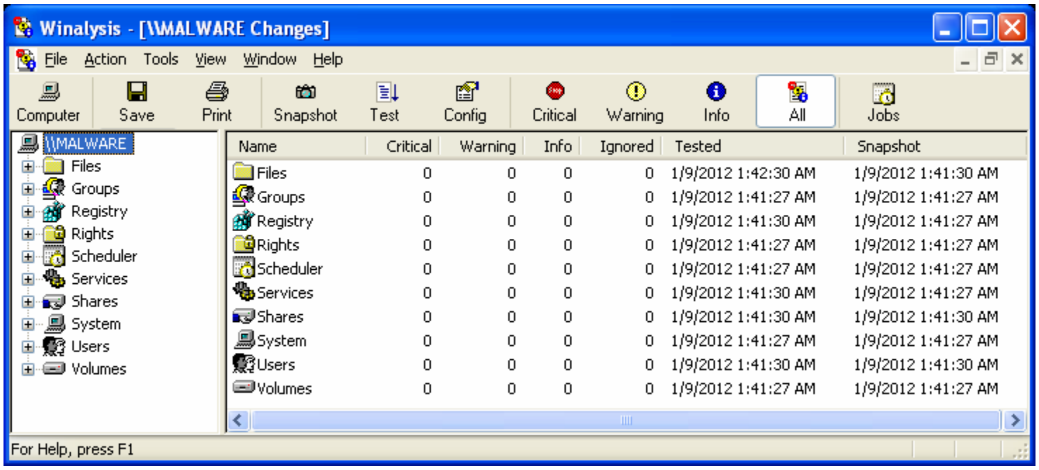
4.1 This malware report focuses on malware static analysis but also lightly introduces dynamic analysis to determine if the malware sample is packed, armored, encrypted, and or obfuscated. There is also a very brief introduction to IDA Pro, and Immunity de-bugger.

4.2 Advanced modern malware applications are either protected, obfuscated, encrypted (armoring) and/or packed (the original code is compressed, encrypted or both). This technique is applied in an attempt to evade signature based malware detection, and to hinder the efforts of static analysis by malware analysts by employing anti-reversing, anti-debugging and self-modifying code tactics. This malware sample is no different. The unpacking or decrypting of the malware layers remains the most complicated & sophisticated task in the overall process of malware analysis and finding the original entry point (OEP). True analysis of packed malicious binary code can only be performed after the payload is unpacked. Dynamic analysis goes beyond the focus of this paper, and will be the focus of part 2 of this malware report. Stay tuned!

Software

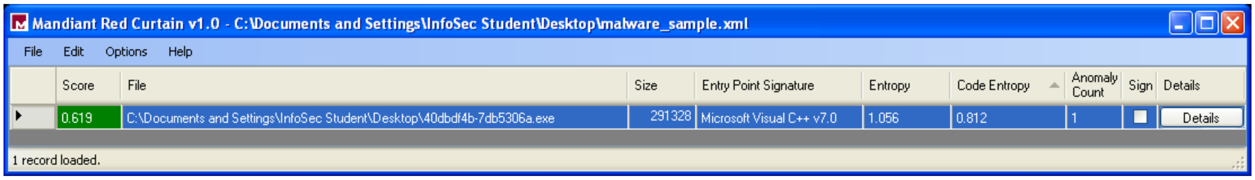
4.3 Software used for the analysis of the malware sample.

1. Winalysis v3.1. Used to snapshot the OS and verify changes to the baseline after the malware sample has been executed.


Winalysis - [\\MALWARE Changes]
File Action Tools View Window Help
Computer Save Print Snapshot Test Config Critical Warning Info All Jobs
\\MALWARE
Files
Groups
Registry
Rights
Scheduler
Services
Shares
System
Users
Volumes
For Help, press F1

Name	Critical	Warning	Info	Ignored	Tested	Snapshot
Files	0	0	0	0	1/9/2012 1:42:30 AM	1/9/2012 1:41:30 AM
Groups	0	0	0	0	1/9/2012 1:41:27 AM	1/9/2012 1:41:27 AM
Registry	0	0	0	0	1/9/2012 1:41:30 AM	1/9/2012 1:41:27 AM
Rights	0	0	0	0	1/9/2012 1:41:27 AM	1/9/2012 1:41:27 AM
Scheduler	0	0	0	0	1/9/2012 1:41:27 AM	1/9/2012 1:41:27 AM
Services	0	0	0	0	1/9/2012 1:41:30 AM	1/9/2012 1:41:27 AM
Shares	0	0	0	0	1/9/2012 1:41:30 AM	1/9/2012 1:41:30 AM
System	0	0	0	0	1/9/2012 1:41:27 AM	1/9/2012 1:41:27 AM
Users	0	0	0	0	1/9/2012 1:41:30 AM	1/9/2012 1:41:30 AM
Volumes	0	0	0	0	1/9/2012 1:41:27 AM	1/9/2012 1:41:27 AM

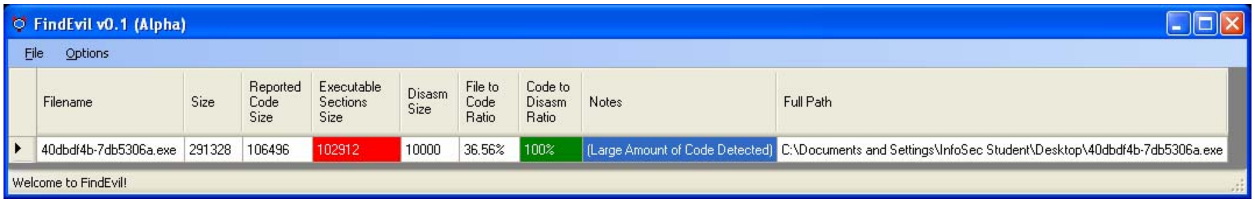
2. Mandiant Red Curtain v1.0. Look for entropy, packing indication, original entry point (OEP), compiler & packing signatures, digital signatures, and it generates a threat score.


Mandiant Red Curtain v1.0 - C:\Documents and Settings\InfoSec Student\Desktop\malware_sample.xml
File Edit Options Help

Score	File	Size	Entry Point Signature	Entropy	Code Entropy	Anomaly Count	Sign	Details
0.619	C:\Documents and Settings\InfoSec Student\Desktop\40dbdf4b-7db5306a.exe	291328	Microsoft Visual C++ v7.0	1.056	0.812	1	□	Details

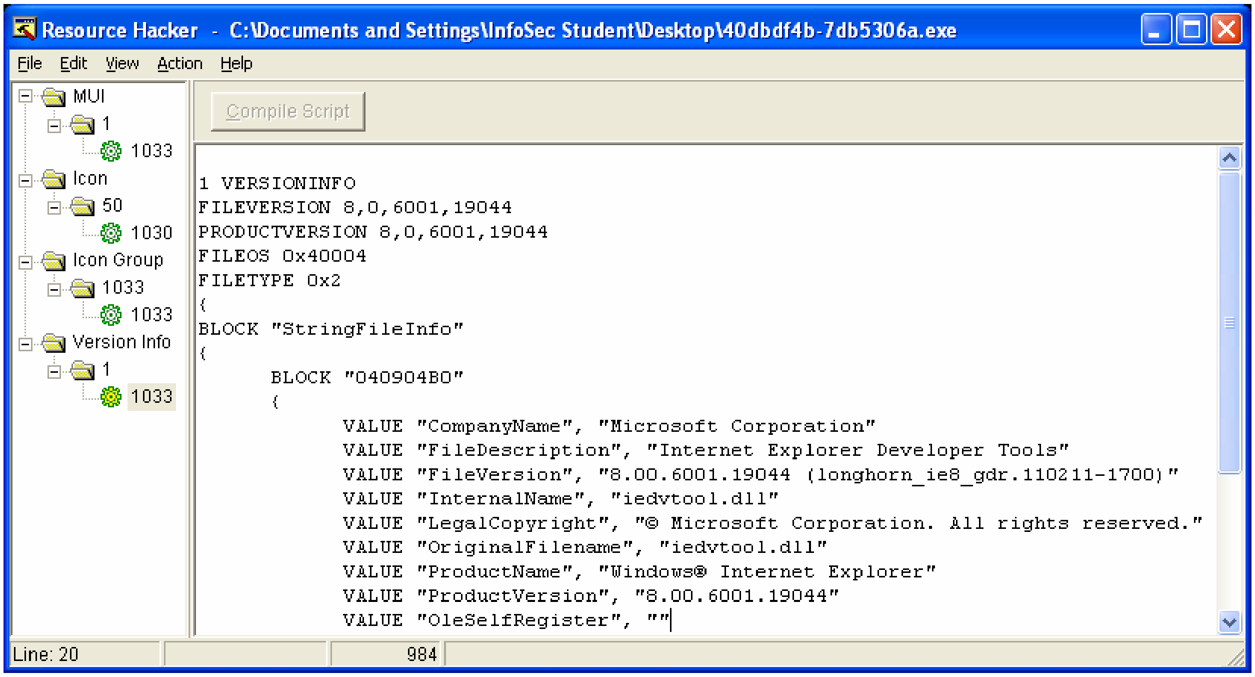
1 record loaded.

3. Mandiant Find Evil v0.1. Malware discovery tool which uses disassembly to detect packed executables.



Filename	Size	Reported Code Size	Executable Sections Size	Disasm Size	File to Code Ratio	Code to Disasm Ratio	Notes	Full Path
40dbdf4b-7db5306a.exe	291328	106496	102912	10000	36.56%	100%	(Large Amount of Code Detected)	C:\Documents and Settings\InfoSec Student\Desktop\40dbdf4b-7db5306a.exe

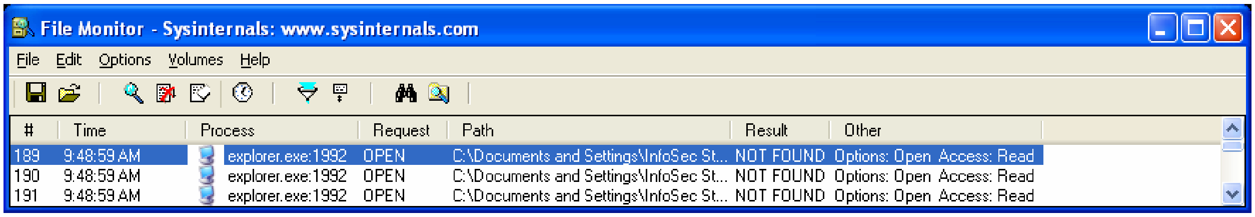
4. Resource Hacker v3.4.0.79. To view/modify Windows executable resources.



```
1 VERSIONINFO
FILEVERSION 8,0,6001,19044
PRODUCTVERSION 8,0,6001,19044
FILEOS 0x40004
FILETYPE 0x2
{
BLOCK "StringFileInfo"
{
	BLOCK "040904B0"
	{
		VALUE "CompanyName", "Microsoft Corporation"
		VALUE "FileDescription", "Internet Explorer Developer Tools"
		VALUE "FileVersion", "8.00.6001.19044 (longhorn_ie8_gdr.110211-1700)"
		VALUE "InternalName", "iedvtool.dll"
		VALUE "LegalCopyright", "© Microsoft Corporation. All rights reserved."
		VALUE "OriginalFilename", "iedvtool.dll"
		VALUE "ProductName", "Windows® Internet Explorer"
		VALUE "ProductVersion", "8.00.6001.19044"
		VALUE "OleSelfRegister", ""
```

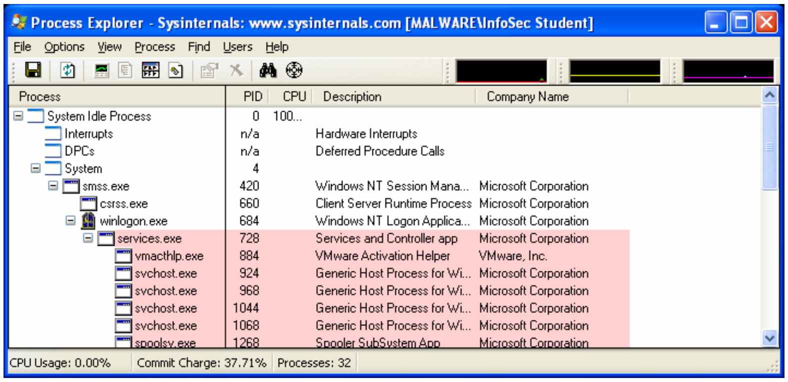
5. Sysinternals Suite. All sorts of goodness!

File Monitor.



#	Time	Process	Request	Path	Result	Other
189	9:48:59 AM	explorer.exe:1992	OPEN	C:\Documents and Settings\InfoSec St...	NOT FOUND	Options: Open Access: Read
190	9:48:59 AM	explorer.exe:1992	OPEN	C:\Documents and Settings\InfoSec St...	NOT FOUND	Options: Open Access: Read
191	9:48:59 AM	explorer.exe:1992	OPEN	C:\Documents and Settings\InfoSec St...	NOT FOUND	Options: Open Access: Read

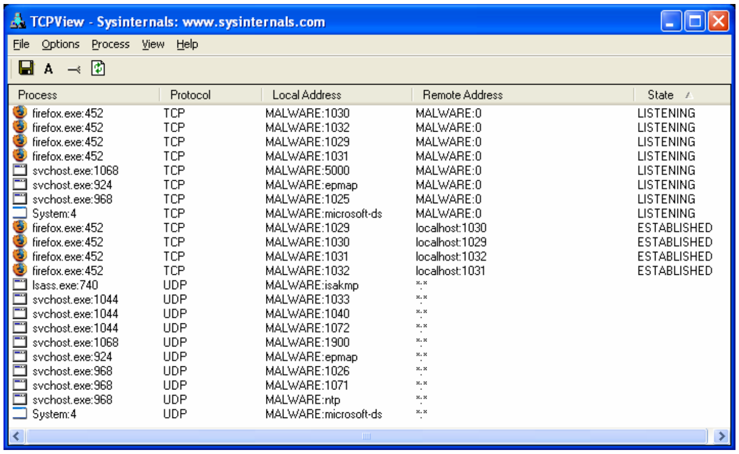
Process Explorer.


Process Explorer - Sysinternals: www.sysinternals.com [MALWARE\InfoSec Student]
File
Options
View
Process
Find
Users
Help

Process	PID	CPU	Description	Company Name
System Idle Process	0	100...		
Interrupts	n/a		Hardware Interrupts	
DPCs	n/a		Deferred Procedure Calls	
System	4			
smss.exe	420		Windows NT Session Mana...	Microsoft Corporation
csrss.exe	660		Client Server Runtime Process	Microsoft Corporation
winlogon.exe	684		Windows NT Logon Applica...	Microsoft Corporation
services.exe	728		Services and Controller app	Microsoft Corporation
vmacthlp.exe	884		VMware Activation Helper	VMware, Inc.
svchost.exe	924		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	968		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1044		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1068		Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe	1268		Spooler SubSystem App	Microsoft Corporation

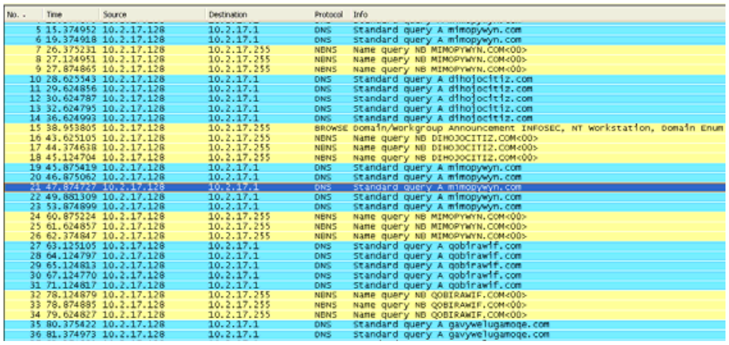
CPU Usage: 0.00% Commit Charge: 37.71% Processes: 32

TCP view.



Process	Protocol	Local Address	Remote Address	State
firefox.exe:452	TCP	MALWARE:1030	MALWARE:0	LISTENING
firefox.exe:452	TCP	MALWARE:1032	MALWARE:0	LISTENING
firefox.exe:452	TCP	MALWARE:1029	MALWARE:0	LISTENING
firefox.exe:452	TCP	MALWARE:1031	MALWARE:0	LISTENING
svchost.exe:1068	TCP	MALWARE:5000	MALWARE:0	LISTENING
svchost.exe:924	TCP	MALWARE:epmap	MALWARE:0	LISTENING
svchost.exe:968	TCP	MALWARE:1025	MALWARE:0	LISTENING
System:4	TCP	MALWARE:microsoft-ds	MALWARE:0	LISTENING
firefox.exe:452	TCP	MALWARE:1029	localhost:1030	ESTABLISHED
firefox.exe:452	TCP	MALWARE:1030	localhost:1029	ESTABLISHED
firefox.exe:452	TCP	MALWARE:1031	localhost:1032	ESTABLISHED
firefox.exe:452	TCP	MALWARE:1032	localhost:1031	ESTABLISHED
lsass.exe:740	UDP	MALWARE:isakmp	*:*	
svchost.exe:1044	UDP	MALWARE:1033	*:*	
svchost.exe:1044	UDP	MALWARE:1040	*:*	
svchost.exe:1044	UDP	MALWARE:1072	*:*	
svchost.exe:1068	UDP	MALWARE:1900	*:*	
svchost.exe:924	UDP	MALWARE:epmap	*:*	
svchost.exe:968	UDP	MALWARE:1026	*:*	
svchost.exe:968	UDP	MALWARE:1071	*:*	
svchost.exe:968	UDP	MALWARE:ntp	*:*	
System:4	UDP	MALWARE:microsoft-ds	*:*	

6. Wireshark. Used to capture all network packets, DNS requests, HTTP get requests… etc generated by the malware sample.



No.	Time	Source	Destination	Protocol	Info
5	15.374952	10.2.17.128	10.2.17.1	DNS	Standard query A mimopywyn.com
6	19.374918	10.2.17.128	10.2.17.1	DNS	Standard query A mimopywyn.com
7	26.375231	10.2.17.128	10.2.17.255	NBNS	Name query NB MIMOPYWYN.COM<00>
8	27.124951	10.2.17.128	10.2.17.255	NBNS	Name query NB MIMOPYWYN.COM<00>
9	27.874865	10.2.17.128	10.2.17.255	NBNS	Name query NB MIMOPYWYN.COM<00>
10	28.625543	10.2.17.128	10.2.17.1	DNS	Standard query A dihojocitiz.com
11	29.624856	10.2.17.128	10.2.17.1	DNS	Standard query A dihojocitiz.com
12	30.624787	10.2.17.128	10.2.17.1	DNS	Standard query A dihojocitiz.com
13	32.624795	10.2.17.128	10.2.17.1	DNS	Standard query A dihojocitiz.com
14	36.624993	10.2.17.128	10.2.17.1	DNS	Standard query A dihojocitiz.com
15	38.953805	10.2.17.128	10.2.17.255	BROWSE	Domain/Workgroup Announcement INFOSEC, NT Workstation, Domain Enum
16	43.625105	10.2.17.128	10.2.17.255	NBNS	Name query NB DIHOJOCITIZ.COM<00>
17	44.374638	10.2.17.128	10.2.17.255	NBNS	Name query NB DIHOJOCITIZ.COM<00>
18	45.124704	10.2.17.128	10.2.17.255	NBNS	Name query NB DIHOJOCITIZ.COM<00>
19	45.875419	10.2.17.128	10.2.17.1	DNS	Standard query A mimopywyn.com
20	46.875062	10.2.17.128	10.2.17.1	DNS	Standard query A mimopywyn.com
21	47.874727	10.2.17.128	10.2.17.1	DNS	Standard query A mimopywyn.com
22	49.881309	10.2.17.128	10.2.17.1	DNS	Standard query A mimopywyn.com
23	53.874899	10.2.17.128	10.2.17.1	DNS	Standard query A mimopywyn.com
24	60.875224	10.2.17.128	10.2.17.255	NBNS	Name query NB MIMOPYWYN.COM<00>
25	61.624857	10.2.17.128	10.2.17.255	NBNS	Name query NB MIMOPYWYN.COM<00>
26	62.374847	10.2.17.128	10.2.17.255	NBNS	Name query NB MIMOPYWYN.COM<00>
27	63.125105	10.2.17.128	10.2.17.1	DNS	Standard query A qobirawif.com
28	64.124797	10.2.17.128	10.2.17.1	DNS	Standard query A qobirawif.com
29	65.124813	10.2.17.128	10.2.17.1	DNS	Standard query A qobirawif.com
30	67.124770	10.2.17.128	10.2.17.1	DNS	Standard query A qobirawif.com
31	71.124817	10.2.17.128	10.2.17.1	DNS	Standard query A qobirawif.com
32	78.124879	10.2.17.128	10.2.17.255	NBNS	Name query NB QOBIRAWIF.COM<00>
33	78.874885	10.2.17.128	10.2.17.255	NBNS	Name query NB QOBIRAWIF.COM<00>
34	79.624827	10.2.17.128	10.2.17.255	NBNS	Name query NB QOBIRAWIF.COM<00>
35	80.375422	10.2.17.128	10.2.17.1	DNS	Standard query A gavywelugamoge.com
36	81.374973	10.2.17.128	10.2.17.1	DNS	Standard query A gavywelugamoge.com

7. Malicious domain research & staying anonymous during investigation.

I primarily use a mixture of the following. Tor/TorSOCKS, Privoxy, anonymous.org, hidemyass.com, and/or a VPN connection.

8. Researching malicious Domains, and IP's.

Query whois records. www.networktools.nl/whois

How many malicious domains are hosted on an IP? www.networktools.nl/reverseip

Is IP listed in SPAM blacklists? www.networktools.nl/rblcheck

GeoIP location search/trace. www.ip-adress.com/ip_tracer/

9. IDA Pro v6.1

10. Immunity De-bugger v1.83

Secure Lab setup.

4.4 VMware workstation v8.0.1 build-528992. Under the guest VM I like to disable drag/drop, and copy/paste. I also set my host firewall to a default DROP/LOG ALL stance for the duration of the malware analysis, and you can also run snort on the host just for paranoia. I like to perform two different analysis. The same malware sample on a physical machine, and one on a virtual machine. I then compare the results and verify if the malware detected or changed its payload if under a VM (red pill) or tried to escape the VM sandbox (which is very possible). That is the reason you should have a dedicated malware machine for these purposes, and never be connected to the internet while analysis is underway. Your host machine can still be infected even if you run your guest machines under NAT/Bridged or host only networking modes. Being paranoid is the only way to survive!

5. GENERAL FUNCTION AND FUNCTIONALITY OF THE MALWARE

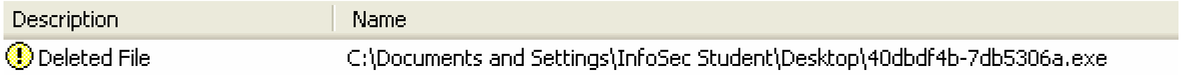
5.1 This malware sample installs fake antivirus software on the victim machine. It attempts to trick the user with several popups that resemble valid applications warning that the user is infected and that he/she needs to buy the full version of the software in order to be fully protected.

The malware sample's main purpose is to steal credit card information from the victim. It has very extensive networking capabilities which are detailed in the Network Behavior section 7 of this report.

6. BEHAVIORAL PATTERNS OF THE MALWARE AND LOCAL SYSTEM INTERACTION

6.1 As soon as I executed the malware sample it immediately deleted itself.

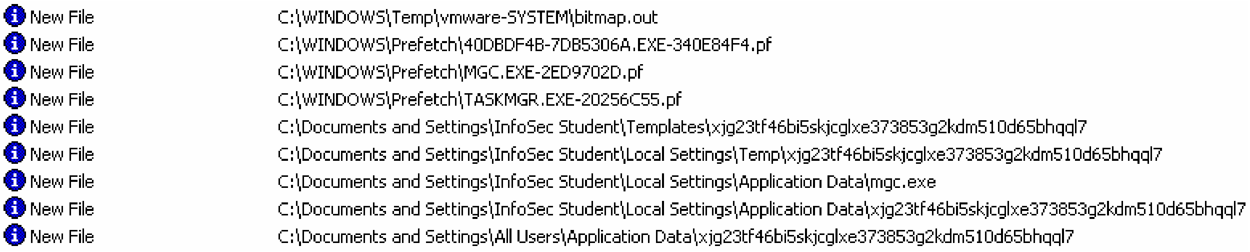
Meaning that the malware sample disappeared right after I double clicked/executed it.



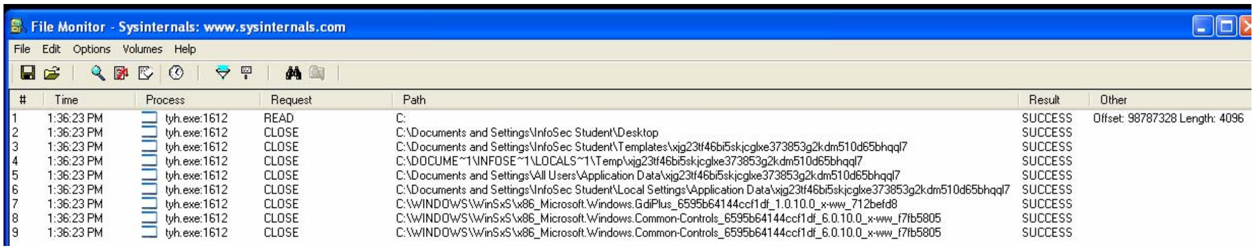
Description	Name
⚠ Deleted File	C:\Documents and Settings\InfoSec Student\Desktop\40dbdf4b-7db5306a.exe

7. FILES AND REGISTRY KEYS CREATED, MODIFIED AND ACCESSED

7.1 The malware sample installed/dropped the following new malicious files, and executables on the victim machine.

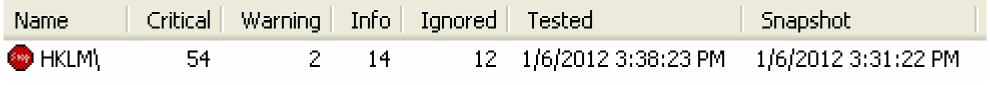


ℹ New File	C:\WINDOWS\Temp\vmware-SYSTEM\bitmap.out
ℹ New File	C:\WINDOWS\Prefetch\40DBDF4B-7DB5306A.EXE-340E84F4.pf
ℹ New File	C:\WINDOWS\Prefetch\MGC.EXE-2ED9702D.pf
ℹ New File	C:\WINDOWS\Prefetch\TASKMGR.EXE-20256C55.pf
ℹ New File	C:\Documents and Settings\InfoSec Student\Templates\xjg23tf46bi5skjcglxe373853g2kdm510d65bhqql7
ℹ New File	C:\Documents and Settings\InfoSec Student\Local Settings\Temp\xjg23tf46bi5skjcglxe373853g2kdm510d65bhqql7
ℹ New File	C:\Documents and Settings\InfoSec Student\Local Settings\Application Data\mgc.exe
ℹ New File	C:\Documents and Settings\InfoSec Student\Local Settings\Application Data\xjg23tf46bi5skjcglxe373853g2kdm510d65bhqql7
ℹ New File	C:\Documents and Settings\All Users\Application Data\xjg23tf46bi5skjcglxe373853g2kdm510d65bhqql7



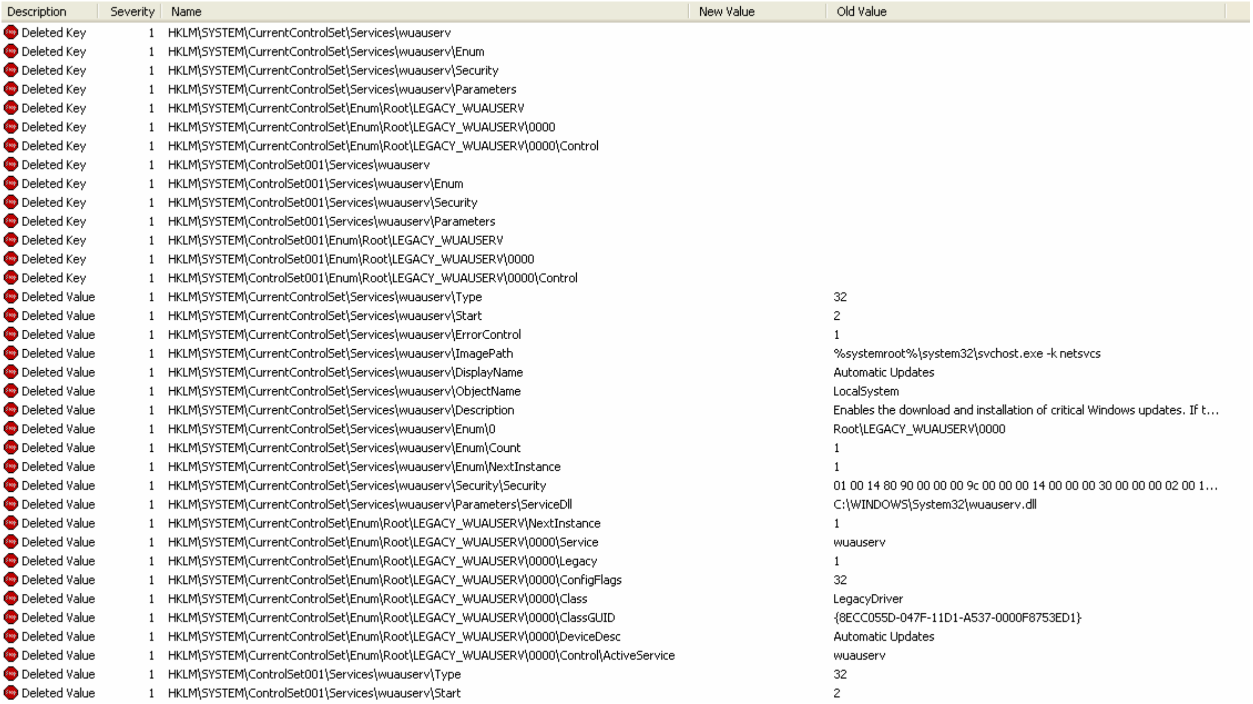
#	Time	Process	Request	Path	Result	Other
1	1:36:23 PM	tyh.exe:1612	READ	C:	SUCCESS	Offset: 98787328 Length: 4096
2	1:36:23 PM	tyh.exe:1612	CLOSE	C:\Documents and Settings\InfoSec Student\Desktop	SUCCESS	
3	1:36:23 PM	tyh.exe:1612	CLOSE	C:\Documents and Settings\InfoSec Student\Templates\xjg23tf46bi5skjcglxe373853g2kdm510d65bhqql7	SUCCESS	
4	1:36:23 PM	tyh.exe:1612	CLOSE	C:\DOCUME~1\INFOSE~1\LOCALS~1\Temp\xjg23tf46bi5skjcglxe373853g2kdm510d65bhqql7	SUCCESS	
5	1:36:23 PM	tyh.exe:1612	CLOSE	C:\Documents and Settings\All Users\Application Data\xjg23tf46bi5skjcglxe373853g2kdm510d65bhqql7	SUCCESS	
6	1:36:23 PM	tyh.exe:1612	CLOSE	C:\Documents and Settings\InfoSec Student\Local Settings\Application Data\xjg23tf46bi5skjcglxe373853g2kdm510d65bhqql7	SUCCESS	
7	1:36:23 PM	tyh.exe:1612	CLOSE	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.10.0_x-ww_712befd8	SUCCESS	
8	1:36:23 PM	tyh.exe:1612	CLOSE	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.10.0_x-ww_f7fb5805	SUCCESS	
9	1:36:23 PM	tyh.exe:1612	CLOSE	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.10.0_x-ww_f7fb5805	SUCCESS	

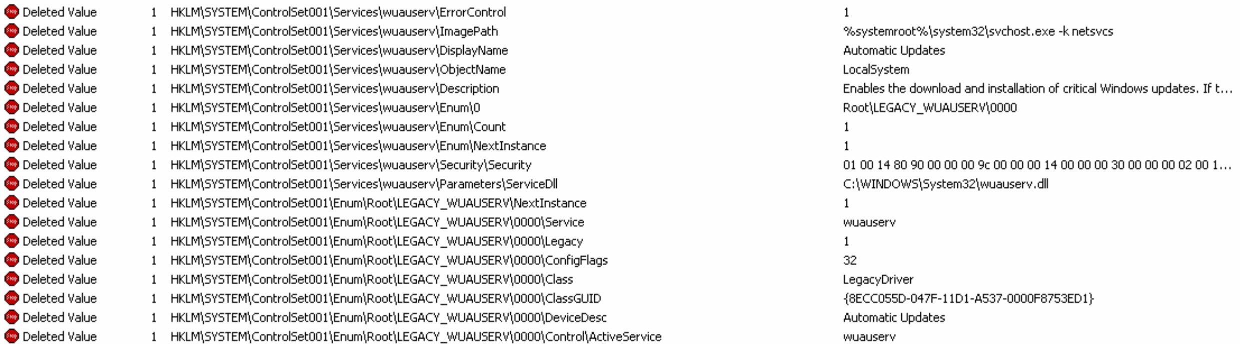
7.2 The malware sample made 54 critical changes to the registry.



Name	Critical	Warning	Info	Ignored	Tested	Snapshot
HKLM\	54	2	14	12	1/6/2012 3:38:23 PM	1/6/2012 3:31:22 PM

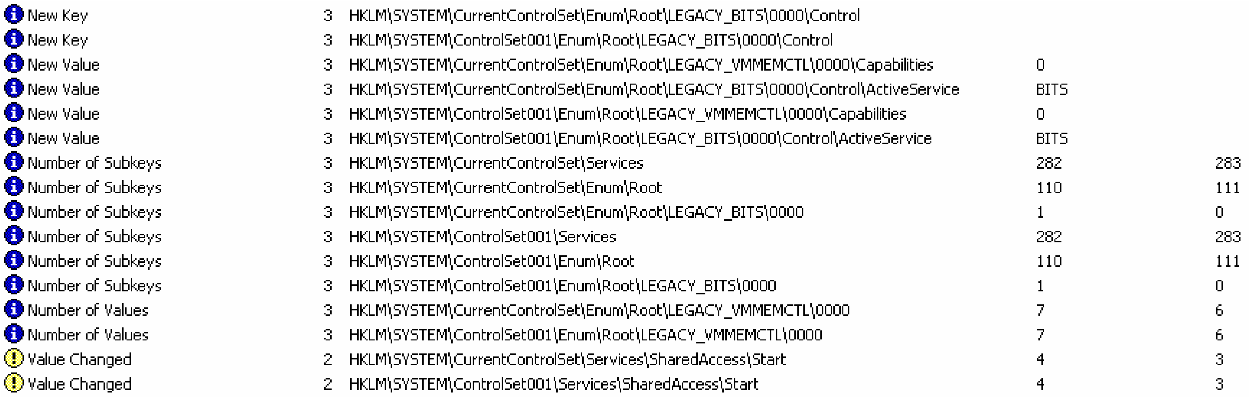
7.3 It deleted the following registry keys from the registry.





Description	Severity	Name	New Value	Old Value
Deleted Key	1	HKLM\SYSTEM\CurrentControlSet\Services\wuauserv		
Deleted Key	1	HKLM\SYSTEM\CurrentControlSet\Services\wuauserv\Enum		
Deleted Key	1	HKLM\SYSTEM\CurrentControlSet\Services\wuauserv\Security		
Deleted Key	1	HKLM\SYSTEM\CurrentControlSet\Services\wuauserv\Parameters		
Deleted Key	1	HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_WUAUSERV		
Deleted Key	1	HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_WUAUSERV\0000		
Deleted Key	1	HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_WUAUSERV\0000\Control		
Deleted Key	1	HKLM\SYSTEM\ControlSet001\Services\wuauserv		
Deleted Key	1	HKLM\SYSTEM\ControlSet001\Services\wuauserv\Enum		
Deleted Key	1	HKLM\SYSTEM\ControlSet001\Services\wuauserv\Security		
Deleted Key	1	HKLM\SYSTEM\ControlSet001\Services\wuauserv\Parameters		
Deleted Key	1	HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_WUAUSERV		
Deleted Key	1	HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_WUAUSERV\0000		
Deleted Key	1	HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_WUAUSERV\0000\Control		
Deleted Value	1	HKLM\SYSTEM\CurrentControlSet\Services\wuauserv\Type		32
Deleted Value	1	HKLM\SYSTEM\CurrentControlSet\Services\wuauserv\Start		2
Deleted Value	1	HKLM\SYSTEM\CurrentControlSet\Services\wuauserv\ErrorControl		1
Deleted Value	1	HKLM\SYSTEM\CurrentControlSet\Services\wuauserv\ImagePath		%systemroot%\system32\svchost.exe -k netsvcs
Deleted Value	1	HKLM\SYSTEM\CurrentControlSet\Services\wuauserv\DisplayName		Automatic Updates
Deleted Value	1	HKLM\SYSTEM\CurrentControlSet\Services\wuauserv\ObjectName		LocalSystem
Deleted Value	1	HKLM\SYSTEM\CurrentControlSet\Services\wuauserv\Description		Enables the download and installation of critical Windows updates. If t...
Deleted Value	1	HKLM\SYSTEM\CurrentControlSet\Services\wuauserv\Enum\0		Root\LEGACY_WUAUSERV\0000
Deleted Value	1	HKLM\SYSTEM\CurrentControlSet\Services\wuauserv\Enum\Count		1
Deleted Value	1	HKLM\SYSTEM\CurrentControlSet\Services\wuauserv\Enum\NextInstance		1
Deleted Value	1	HKLM\SYSTEM\CurrentControlSet\Services\wuauserv\Security\Security		01 00 14 80 90 00 00 00 9c 00 00 00 14 00 00 00 30 00 00 00 02 00 1...
Deleted Value	1	HKLM\SYSTEM\CurrentControlSet\Services\wuauserv\Parameters\ServiceDll		C:\WINDOWS\System32\wuauserv.dll
Deleted Value	1	HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_WUAUSERV\NextInstance		1
Deleted Value	1	HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_WUAUSERV\0000\Service		wuauserv
Deleted Value	1	HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_WUAUSERV\0000\Legacy		1
Deleted Value	1	HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_WUAUSERV\0000\ConfigFlags		32
Deleted Value	1	HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_WUAUSERV\0000\Class		LegacyDriver
Deleted Value	1	HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_WUAUSERV\0000\ClassGUID		{8ECC055D-047F-11D1-A537-0000F8753ED1}
Deleted Value	1	HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_WUAUSERV\0000\DeviceDesc		Automatic Updates
Deleted Value	1	HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_WUAUSERV\0000\Control\ActiveService		wuauserv
Deleted Value	1	HKLM\SYSTEM\ControlSet001\Services\wuauserv\Type		32
Deleted Value	1	HKLM\SYSTEM\ControlSet001\Services\wuauserv\Start		2
Deleted Value	1	HKLM\SYSTEM\ControlSet001\Services\wuauserv\ErrorControl		1
Deleted Value	1	HKLM\SYSTEM\ControlSet001\Services\wuauserv\ImagePath		%systemroot%\system32\svchost.exe -k netsvcs
Deleted Value	1	HKLM\SYSTEM\ControlSet001\Services\wuauserv\DisplayName		Automatic Updates
Deleted Value	1	HKLM\SYSTEM\ControlSet001\Services\wuauserv\ObjectName		LocalSystem
Deleted Value	1	HKLM\SYSTEM\ControlSet001\Services\wuauserv\Description		Enables the download and installation of critical Windows updates. If t...
Deleted Value	1	HKLM\SYSTEM\ControlSet001\Services\wuauserv\Enum\0		Root\LEGACY_WUAUSERV\0000
Deleted Value	1	HKLM\SYSTEM\ControlSet001\Services\wuauserv\Enum\Count		1
Deleted Value	1	HKLM\SYSTEM\ControlSet001\Services\wuauserv\Enum\NextInstance		1
Deleted Value	1	HKLM\SYSTEM\ControlSet001\Services\wuauserv\Security\Security		01 00 14 80 90 00 00 00 9c 00 00 00 14 00 00 00 30 00 00 00 02 00 1...
Deleted Value	1	HKLM\SYSTEM\ControlSet001\Services\wuauserv\Parameters\ServiceDll		C:\WINDOWS\System32\wuauserv.dll
Deleted Value	1	HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_WUAUSERV\NextInstance		1
Deleted Value	1	HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_WUAUSERV\0000\Service		wuauserv
Deleted Value	1	HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_WUAUSERV\0000\Legacy		1
Deleted Value	1	HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_WUAUSERV\0000\ConfigFlags		32
Deleted Value	1	HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_WUAUSERV\0000\Class		LegacyDriver
Deleted Value	1	HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_WUAUSERV\0000\ClassGUID		{8ECC055D-047F-11D1-A537-0000F8753ED1}
Deleted Value	1	HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_WUAUSERV\0000\DeviceDesc		Automatic Updates
Deleted Value	1	HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_WUAUSERV\0000\Control\ActiveService		wuauserv

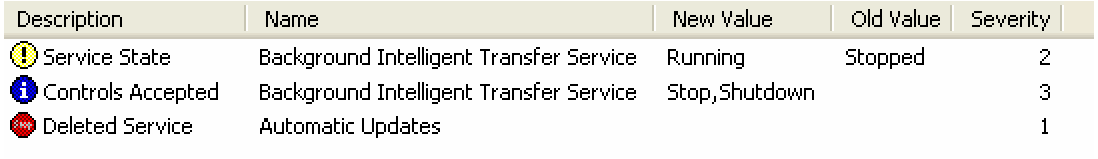
7.4 The malware sample created the following new registry keys, Subkeys, and values.



ℹ New Key	3	HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_BITS\0000\Control		
ℹ New Key	3	HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_BITS\0000\Control		
ℹ New Value	3	HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_VMMEMCTL\0000\Capabilities	0	
ℹ New Value	3	HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_BITS\0000\Control\ActiveService	BITS	
ℹ New Value	3	HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_VMMEMCTL\0000\Capabilities	0	
ℹ New Value	3	HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_BITS\0000\Control\ActiveService	BITS	
ℹ Number of Subkeys	3	HKLM\SYSTEM\CurrentControlSet\Services	282	283
ℹ Number of Subkeys	3	HKLM\SYSTEM\CurrentControlSet\Enum\Root	110	111
ℹ Number of Subkeys	3	HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_BITS\0000	1	0
ℹ Number of Subkeys	3	HKLM\SYSTEM\ControlSet001\Services	282	283
ℹ Number of Subkeys	3	HKLM\SYSTEM\ControlSet001\Enum\Root	110	111
ℹ Number of Subkeys	3	HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_BITS\0000	1	0
ℹ Number of Values	3	HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_VMMEMCTL\0000	7	6
ℹ Number of Values	3	HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_VMMEMCTL\0000	7	6
⚠ Value Changed	2	HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Start	4	3
⚠ Value Changed	2	HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Start	4	3

7.5 The malware sample modified the following services on the victim machine.

It started the BITS service with two new control parameters, and deleted the automatic updates service, and registry key values. This means that the malware sample has effectively disabled windows update, and prevented the download and installation of critical Windows updates for the victim machine. This most likely means that it is covering it tracks because it takes advantage of an existing unpatched Windows vulnerability, and updating the OS will likely kill/disable the infection/communication/propogation vector of this malware variant.



Description	Name	New Value	Old Value	Severity
⚠ Service State	Background Intelligent Transfer Service	Running	Stopped	2
ℹ Controls Accepted	Background Intelligent Transfer Service	Stop,Shutdown		3
🛑 Deleted Service	Automatic Updates			1

7.6 Running processes before, and after the malware sample was executed. Note the “tyh.exe” that is now running.

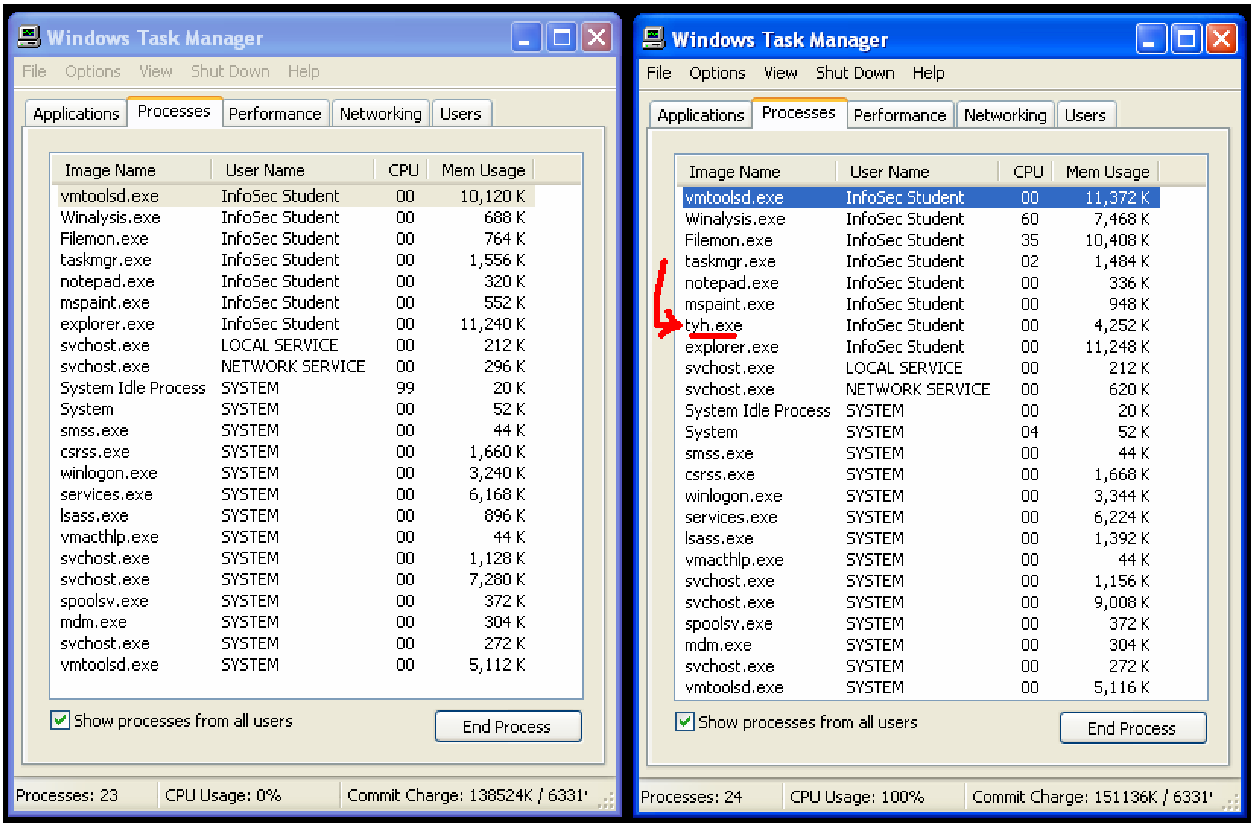

Windows Task Manager
File Options View Shut Down Help
Applications Processes Performance Networking Users
☑ Show processes from all users
End Process

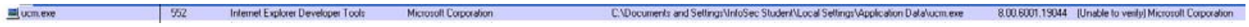
Image Name	User Name	CPU	Mem Usage
vmtoolsd.exe	InfoSec Student	00	10,120 K
Winalysis.exe	InfoSec Student	00	688 K
Filemon.exe	InfoSec Student	00	764 K
taskmgr.exe	InfoSec Student	00	1,556 K
notepad.exe	InfoSec Student	00	320 K
mspaint.exe	InfoSec Student	00	552 K
explorer.exe	InfoSec Student	00	11,240 K
svchost.exe	LOCAL SERVICE	00	212 K
svchost.exe	NETWORK SERVICE	00	296 K
System Idle Process	SYSTEM	99	20 K
System	SYSTEM	00	52 K
smss.exe	SYSTEM	00	44 K
csrss.exe	SYSTEM	00	1,660 K
winlogon.exe	SYSTEM	00	3,240 K
services.exe	SYSTEM	00	6,168 K
lsass.exe	SYSTEM	00	896 K
vmacthlp.exe	SYSTEM	00	44 K
svchost.exe	SYSTEM	00	1,128 K
svchost.exe	SYSTEM	00	7,280 K
spoolsv.exe	SYSTEM	00	372 K
mdm.exe	SYSTEM	00	304 K
svchost.exe	SYSTEM	00	272 K
vmtoolsd.exe	SYSTEM	00	5,112 K

Processes: 23 CPU Usage: 0% Commit Charge: 138524K / 6331'

Image Name	User Name	CPU	Mem Usage
vmtoolsd.exe	InfoSec Student	00	11,372 K
Winalysis.exe	InfoSec Student	60	7,468 K
Filemon.exe	InfoSec Student	35	10,408 K
taskmgr.exe	InfoSec Student	02	1,484 K
notepad.exe	InfoSec Student	00	336 K
mspaint.exe	InfoSec Student	00	948 K
tyh.exe	InfoSec Student	00	4,252 K
explorer.exe	InfoSec Student	00	11,248 K
svchost.exe	LOCAL SERVICE	00	212 K
svchost.exe	NETWORK SERVICE	00	620 K
System Idle Process	SYSTEM	00	20 K
System	SYSTEM	04	52 K
smss.exe	SYSTEM	00	44 K
csrss.exe	SYSTEM	00	1,668 K
winlogon.exe	SYSTEM	00	3,344 K
services.exe	SYSTEM	00	6,224 K
lsass.exe	SYSTEM	00	1,392 K
vmacthlp.exe	SYSTEM	00	44 K
svchost.exe	SYSTEM	00	1,156 K
svchost.exe	SYSTEM	00	9,008 K
spoolsv.exe	SYSTEM	00	372 K
mdm.exe	SYSTEM	00	304 K
svchost.exe	SYSTEM	00	272 K
vmtoolsd.exe	SYSTEM	00	5,116 K

Processes: 24 CPU Usage: 100% Commit Charge: 151136K / 6331'

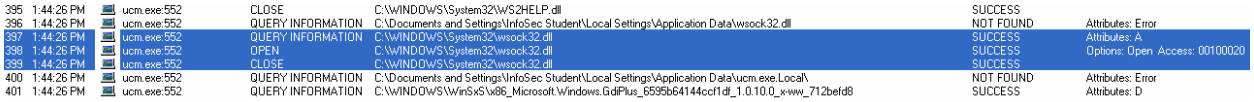
7.7 Process explorer output. Note that it is not able to verify that it is from Microsoft. And each time I execute the malware sample the name of the executable changes. Before it was tyh.exe, and now it is ucm.exe as example.



ucm.exe	552	Internet Explorer Developer Tools	Microsoft Corporation	C:\Documents and Settings\InfoSec Student\Local Settings\Application Data\ucm.exe	8.00.6001.19044	(Unable to verify) Microsoft Corporation

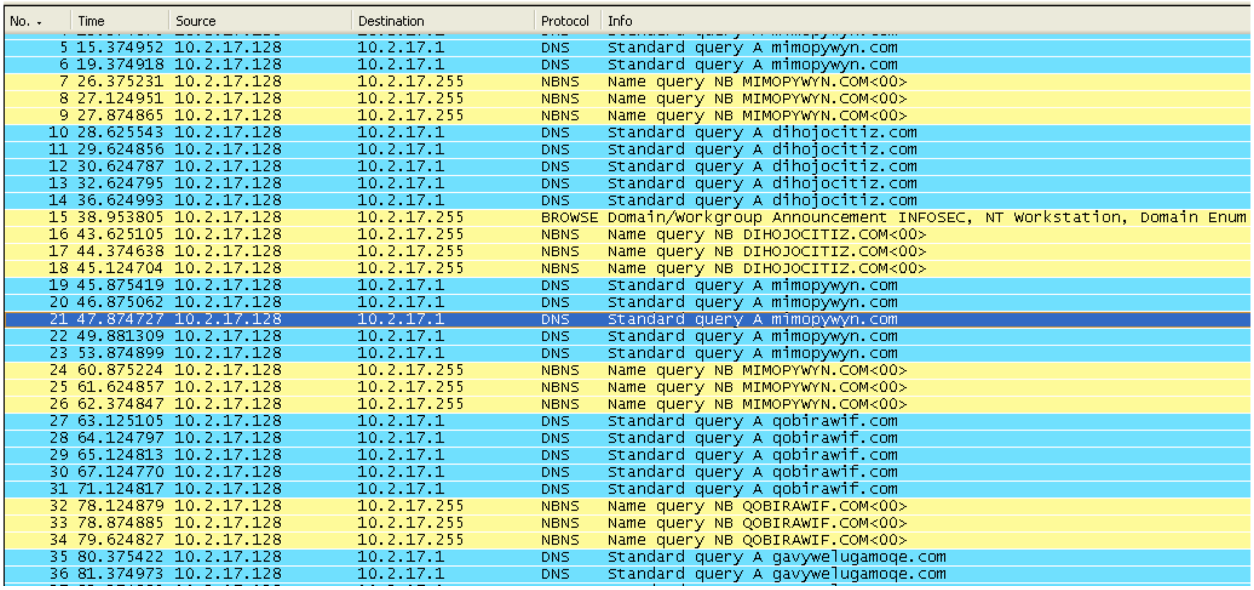
8. NETWORK BEHAVIOR (INCLUDING HOSTS, DOMAINS AND IP'S ACCESSED)

8.1 This malware sample makes a function call to the native Windows API C:\WINDOWS\System32\winsock32.dll which is the Windows Sockets API used by most Internet and Network applications to handle network connections, denoted below in highlighted blue.



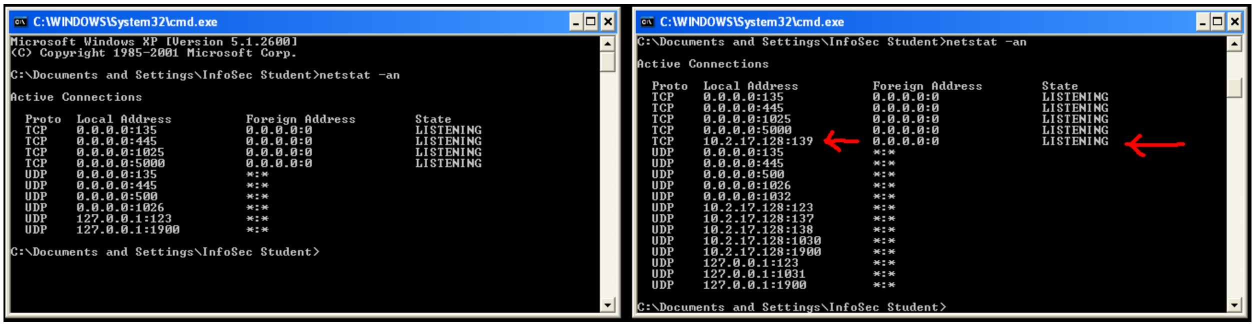
```
395  1:44:26 PM  ucm.exe:552  CLOSE              C:\WINDOWS\System32\WS2HELP.dll                                                     SUCCESS
396  1:44:26 PM  ucm.exe:552  QUERY INFORMATION  C:\Documents and Settings\InfoSec Student\Local Settings\Application Data\wsock32.dll  NOT FOUND  Attributes: Error
397  1:44:26 PM  ucm.exe:552  QUERY INFORMATION  C:\WINDOWS\System32\wsock32.dll                                                     SUCCESS    Attributes: A
398  1:44:26 PM  ucm.exe:552  OPEN               C:\WINDOWS\System32\wsock32.dll                                                     SUCCESS    Options: Open  Access: 00100020
399  1:44:26 PM  ucm.exe:552  CLOSE              C:\WINDOWS\System32\wsock32.dll                                                     SUCCESS
400  1:44:26 PM  ucm.exe:552  QUERY INFORMATION  C:\Documents and Settings\InfoSec Student\Local Settings\Application Data\ucm.exe.Local\  NOT FOUND  Attributes: Error
401  1:44:26 PM  ucm.exe:552  QUERY INFORMATION  C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.10.0_x-ww_712befd8  SUCCESS  Attributes: D
```

8.2 The malware sample also makes DNS requests in an attempt to resolve numerous malicious sites including mimopywyn.com, dihojocitiz.com, qobirawif.com, QOBIRAWIF.com, gavywelugamoqe.com, sesusihyt.com, and xybobimaholos.com, etc. A total of 32 different DNS requests were made but not shown for brevity.



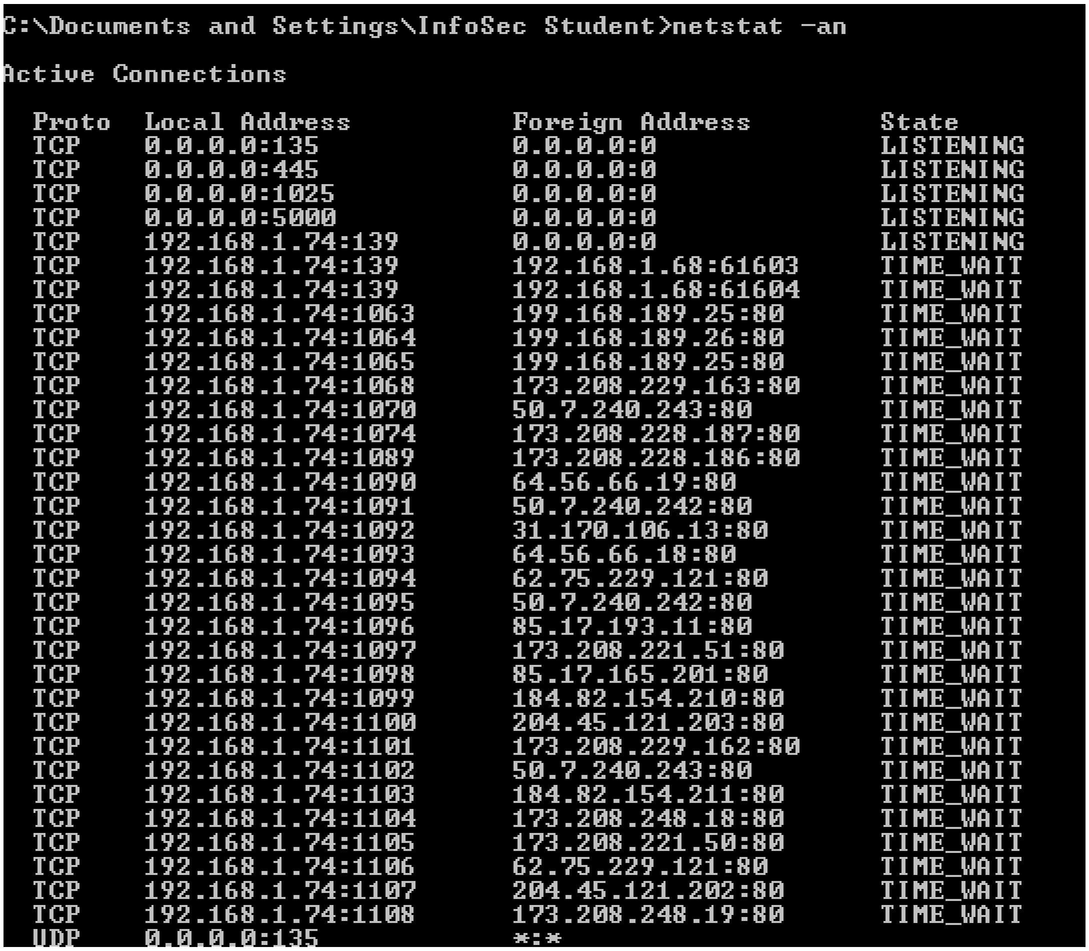
No.	Time	Source	Destination	Protocol	Info
5	15.374952	10.2.17.128	10.2.17.1	DNS	Standard query A mimopywyn.com
6	19.374918	10.2.17.128	10.2.17.1	DNS	Standard query A mimopywyn.com
7	26.375231	10.2.17.128	10.2.17.255	NBNS	Name query NB MIMOPYWYN.COM<00>
8	27.124951	10.2.17.128	10.2.17.255	NBNS	Name query NB MIMOPYWYN.COM<00>
9	27.874865	10.2.17.128	10.2.17.255	NBNS	Name query NB MIMOPYWYN.COM<00>
10	28.625543	10.2.17.128	10.2.17.1	DNS	Standard query A dihojocitiz.com
11	29.624856	10.2.17.128	10.2.17.1	DNS	Standard query A dihojocitiz.com
12	30.624787	10.2.17.128	10.2.17.1	DNS	Standard query A dihojocitiz.com
13	32.624795	10.2.17.128	10.2.17.1	DNS	Standard query A dihojocitiz.com
14	36.624993	10.2.17.128	10.2.17.1	DNS	Standard query A dihojocitiz.com
15	38.953805	10.2.17.128	10.2.17.255	BROWSE	Domain/Workgroup Announcement INFOSEC, NT Workstation, Domain Enum
16	43.625105	10.2.17.128	10.2.17.255	NBNS	Name query NB DIHOJOCITIZ.COM<00>
17	44.374638	10.2.17.128	10.2.17.255	NBNS	Name query NB DIHOJOCITIZ.COM<00>
18	45.124704	10.2.17.128	10.2.17.255	NBNS	Name query NB DIHOJOCITIZ.COM<00>
19	45.875419	10.2.17.128	10.2.17.1	DNS	Standard query A mimopywyn.com
20	46.875062	10.2.17.128	10.2.17.1	DNS	Standard query A mimopywyn.com
21	47.874727	10.2.17.128	10.2.17.1	DNS	Standard query A mimopywyn.com
22	49.881309	10.2.17.128	10.2.17.1	DNS	Standard query A mimopywyn.com
23	53.874899	10.2.17.128	10.2.17.1	DNS	Standard query A mimopywyn.com
24	60.875224	10.2.17.128	10.2.17.255	NBNS	Name query NB MIMOPYWYN.COM<00>
25	61.624857	10.2.17.128	10.2.17.255	NBNS	Name query NB MIMOPYWYN.COM<00>
26	62.374847	10.2.17.128	10.2.17.255	NBNS	Name query NB MIMOPYWYN.COM<00>
27	63.125105	10.2.17.128	10.2.17.1	DNS	Standard query A qobirawif.com
28	64.124797	10.2.17.128	10.2.17.1	DNS	Standard query A qobirawif.com
29	65.124813	10.2.17.128	10.2.17.1	DNS	Standard query A qobirawif.com
30	67.124770	10.2.17.128	10.2.17.1	DNS	Standard query A qobirawif.com
31	71.124817	10.2.17.128	10.2.17.1	DNS	Standard query A qobirawif.com
32	78.124879	10.2.17.128	10.2.17.255	NBNS	Name query NB QOBIRAWIF.COM<00>
33	78.874885	10.2.17.128	10.2.17.255	NBNS	Name query NB QOBIRAWIF.COM<00>
34	79.624827	10.2.17.128	10.2.17.255	NBNS	Name query NB QOBIRAWIF.COM<00>
35	80.375422	10.2.17.128	10.2.17.1	DNS	Standard query A gavywelugamoqe.com
36	81.374973	10.2.17.128	10.2.17.1	DNS	Standard query A gavywelugamoqe.com

8.3 Listening network sockets before and after execution of the malware sample on the victim machine. It is clear from the below snapshot that it opened TCP:139 NetBIOS Session, Windows File and Printer Sharing port. But also with any other system running Samba (SMB). The single most dangerous port on the internet.



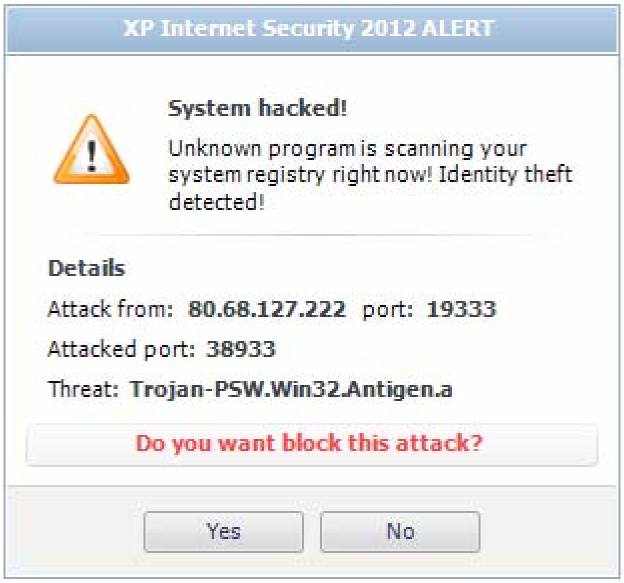
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\InfoSec Student>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5000           0.0.0.0:0              LISTENING
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:1026           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1900         *:*

C:\Documents and Settings\InfoSec Student>
```

```
C:\Documents and Settings\InfoSec Student>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5000           0.0.0.0:0              LISTENING
  TCP    10.2.17.128:139        0.0.0.0:0              LISTENING
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:1026           *:*
  UDP    0.0.0.0:1032           *:*
  UDP    10.2.17.128:123        *:*
  UDP    10.2.17.128:137        *:*
  UDP    10.2.17.128:138        *:*
  UDP    10.2.17.128:1030       *:*
  UDP    10.2.17.128:1900       *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1031         *:*
  UDP    127.0.0.1:1900         *:*

C:\Documents and Settings\InfoSec Student>
```



```
C:\Documents and Settings\InfoSec Student>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5000           0.0.0.0:0              LISTENING
  TCP    192.168.1.74:139       0.0.0.0:0              LISTENING
  TCP    192.168.1.74:139       192.168.1.68:61603     TIME_WAIT
  TCP    192.168.1.74:139       192.168.1.68:61604     TIME_WAIT
  TCP    192.168.1.74:1063      199.168.189.25:80      TIME_WAIT
  TCP    192.168.1.74:1064      199.168.189.26:80      TIME_WAIT
  TCP    192.168.1.74:1065      199.168.189.25:80      TIME_WAIT
  TCP    192.168.1.74:1068      173.208.229.163:80     TIME_WAIT
  TCP    192.168.1.74:1070      50.7.240.243:80        TIME_WAIT
  TCP    192.168.1.74:1074      173.208.228.187:80     TIME_WAIT
  TCP    192.168.1.74:1089      173.208.228.186:80     TIME_WAIT
  TCP    192.168.1.74:1090      64.56.66.19:80         TIME_WAIT
  TCP    192.168.1.74:1091      50.7.240.242:80        TIME_WAIT
  TCP    192.168.1.74:1092      31.170.106.13:80       TIME_WAIT
  TCP    192.168.1.74:1093      64.56.66.18:80         TIME_WAIT
  TCP    192.168.1.74:1094      62.75.229.121:80       TIME_WAIT
  TCP    192.168.1.74:1095      50.7.240.242:80        TIME_WAIT
  TCP    192.168.1.74:1096      85.17.193.11:80        TIME_WAIT
  TCP    192.168.1.74:1097      173.208.221.51:80      TIME_WAIT
  TCP    192.168.1.74:1098      85.17.165.201:80       TIME_WAIT
  TCP    192.168.1.74:1099      184.82.154.210:80      TIME_WAIT
  TCP    192.168.1.74:1100      204.45.121.203:80      TIME_WAIT
  TCP    192.168.1.74:1101      173.208.229.162:80     TIME_WAIT
  TCP    192.168.1.74:1102      50.7.240.243:80        TIME_WAIT
  TCP    192.168.1.74:1103      184.82.154.211:80      TIME_WAIT
  TCP    192.168.1.74:1104      173.208.248.18:80      TIME_WAIT
  TCP    192.168.1.74:1105      173.208.221.50:80      TIME_WAIT
  TCP    192.168.1.74:1106      62.75.229.121:80       TIME_WAIT
  TCP    192.168.1.74:1107      204.45.121.202:80      TIME_WAIT
  TCP    192.168.1.74:1108      173.208.248.19:80      TIME_WAIT
  UDP    0.0.0.0:135            *:*
```

8.4 It did not take long before a fake A/V scanner showed me false scan results that my machine was infected with a malware infection. Clearly this Trojan wanted to steal my credit card information. The malicious software was titled “XP Internet Security 2012”. The malicious site that I was redirected to is intended to steal/collect victims credit card information, and forward the results to the following server http://bekukokymyje.com/support.html with IP of 199.168.189.25 on TCP:80. The malicious server is located in Orlando Florida U.S.A.



XP Internet Security 2012 ALERT

System hacked!

Unknown program is scanning your system registry right now! Identity theft detected!

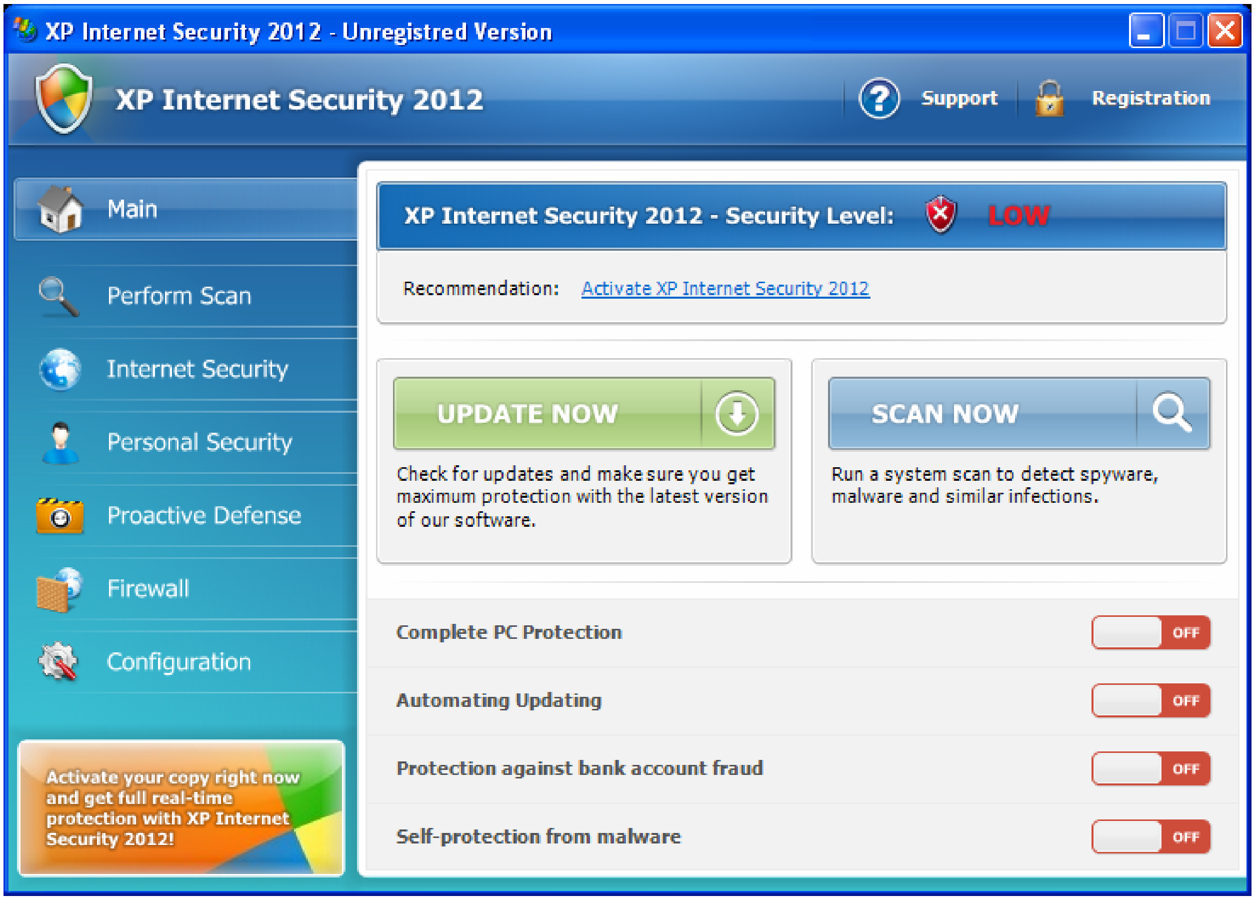
Details

Attack from: **80.68.127.222** port: **19333**

Attacked port: **38933**

Threat: **Trojan-PSW.Win32.Antigen.a**

Do you want block this attack?



XP Internet Security 2012 - Unregistred Version

XP Internet Security 2012

XP Internet Security 2012 - Security Level: LOW

Recommendation: Activate XP Internet Security 2012

Check for updates and make sure you get maximum protection with the latest version of our software.

Run a system scan to detect spyware, malware and similar infections.

Complete PC Protection OFF

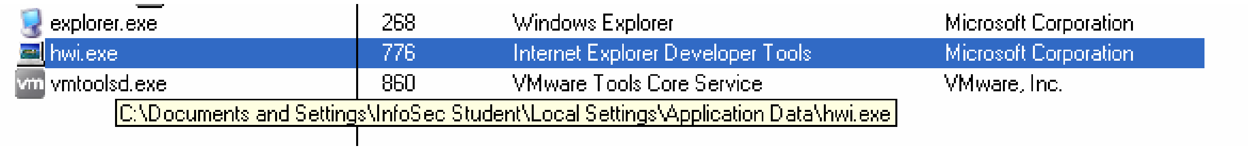
Automating Updating OFF

Protection against bank account fraud OFF

Self-protection from malware OFF

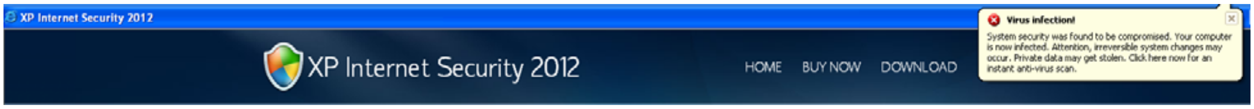
Activate your copy right now and get full real-time protection with XP Internet Security 2012!

The above GUI/Application is running under process “hwi.exe” in the directory pictured below.



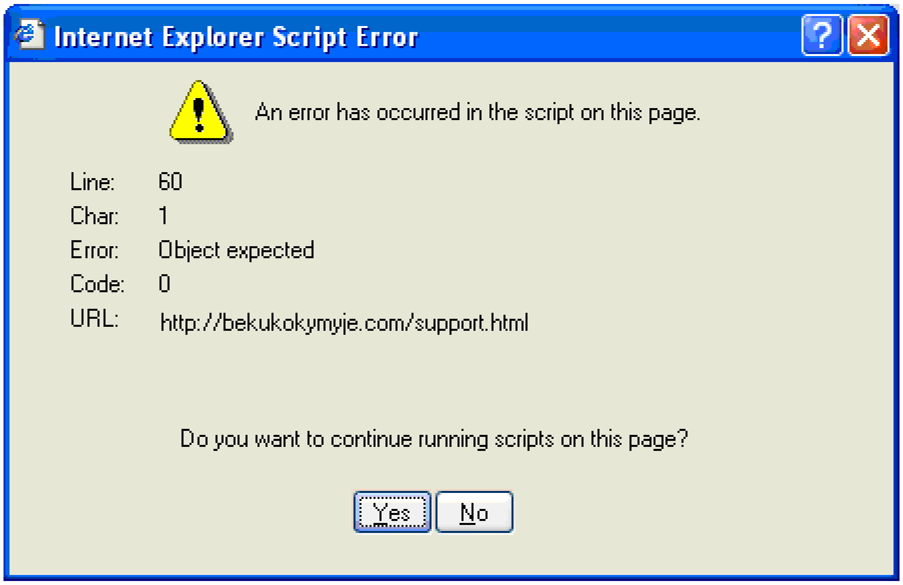
```
explorer.exe    268    Windows Explorer                    Microsoft Corporation
hwi.exe         776    Internet Explorer Developer Tools   Microsoft Corporation
vmtoolsd.exe    860    VMware Tools Core Service           VMware, Inc.
C:\Documents and Settings\InfoSec Student\Local Settings\Application Data\hwi.exe
```

8.5 The above popup redirected me to the following website. The actual form was not even a website nor an actual .html file, it was a Windows Form/GUI. The GUI did not contain any .html/JavaScript. But it made a good attempt to fool the casual user with its Internet Explorer logo.



Virus infection!

System security was found to be compromised. Your computer is now infected. Attention, irreversible system changes may occur. Private data may get stolen. Click here now for an instant anti-virus scan.

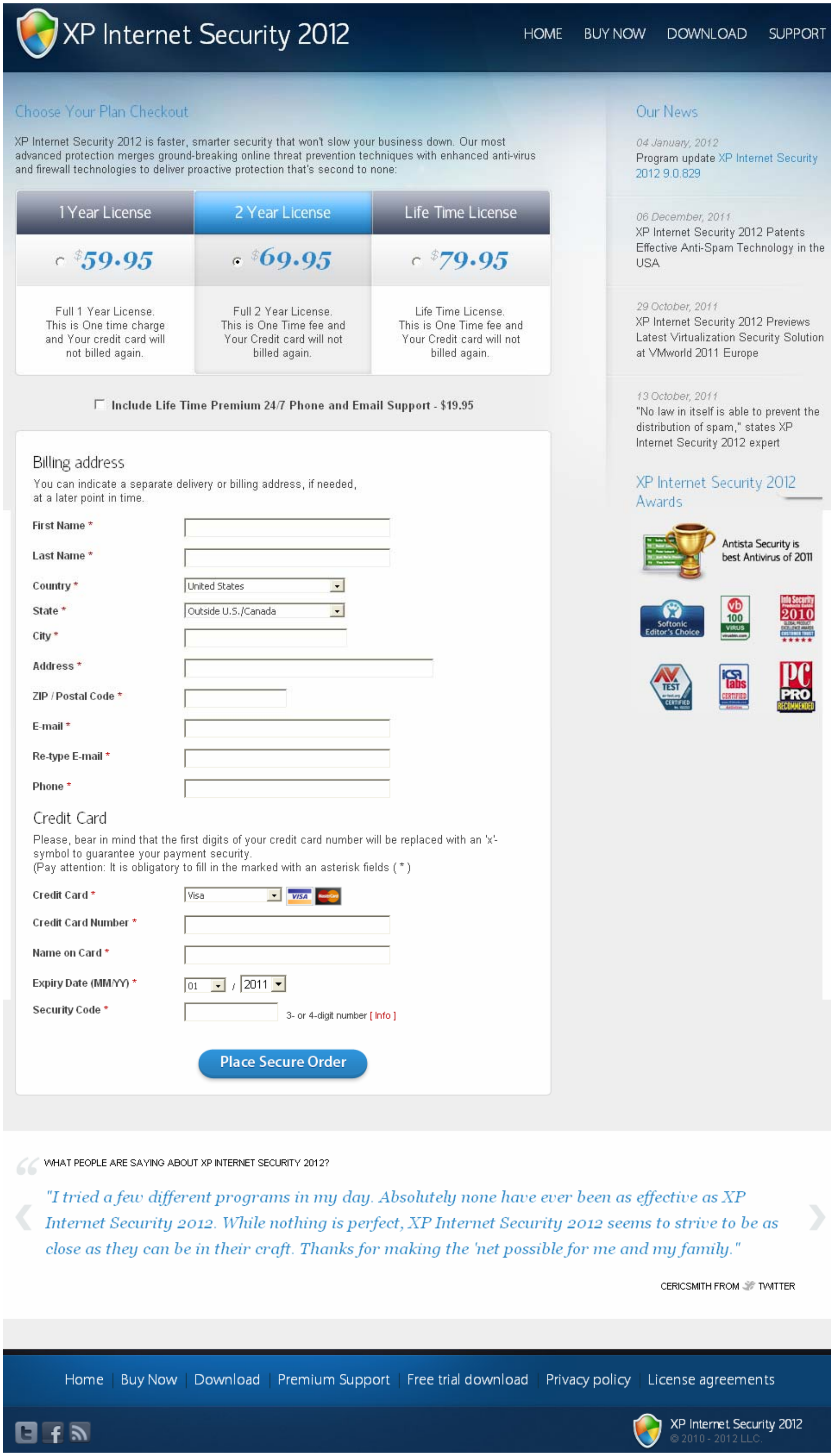


Internet Explorer Script Error

An error has occurred in the script on this page.

Line: 60
Char: 1
Error: Object expected
Code: 0
URL: http://bekukokymyje.com/support.html

Do you want to continue running scripts on this page?



XP Internet Security 2012

HOME BUY NOW DOWNLOAD SUPPORT

Choose Your Plan Checkout

XP Internet Security 2012 is faster, smarter security that won't slow your business down. Our most advanced protection merges ground-breaking online threat prevention techniques with enhanced anti-virus and firewall technologies to deliver proactive protection that's second to none:

1 Year License	2 Year License	Life Time License
○ $59.95	● $69.95	○ $79.95
Full 1 Year License. This is One time charge and Your credit card will not billed again.	Full 2 Year License. This is One Time fee and Your Credit card will not billed again.	Life Time License. This is One Time fee and Your Credit card will not billed again.

□ Include Life Time Premium 24/7 Phone and Email Support - $19.95

Billing address

You can indicate a separate delivery or billing address, if needed, at a later point in time.

First Name *	
Last Name *	
Country *	United States
State *	Outside U.S./Canada
City *	
Address *	
ZIP / Postal Code *	
E-mail *	
Re-type E-mail *	
Phone *	

Credit Card

Please, bear in mind that the first digits of your credit card number will be replaced with an 'x'-symbol to guarantee your payment security.
(Pay attention: It is obligatory to fill in the marked with an asterisk fields (*)

Credit Card *	Visa
Credit Card Number *	
Name on Card *	
Expiry Date (MM/YY) *	01 / 2011
Security Code *	3- or 4-digit number [Info]

Place Secure Order

Our News

04 January, 2012
Program update XP Internet Security 2012 9.0.829

06 December, 2011
XP Internet Security 2012 Patents Effective Anti-Spam Technology in the USA

29 October, 2011
XP Internet Security 2012 Previews Latest Virtualization Security Solution at VMworld 2011 Europe

13 October, 2011
"No law in itself is able to prevent the distribution of spam," states XP Internet Security 2012 expert

XP Internet Security 2012 Awards

Antista Security is best Antivirus of 2011

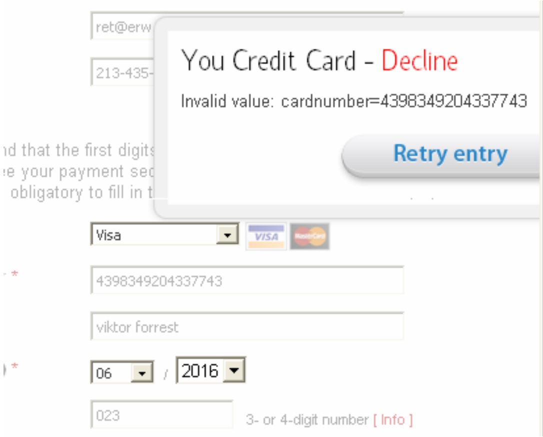
WHAT PEOPLE ARE SAYING ABOUT XP INTERNET SECURITY 2012?

"I tried a few different programs in my day. Absolutely none have ever been as effective as XP Internet Security 2012. While nothing is perfect, XP Internet Security 2012 seems to strive to be as close as they can be in their craft. Thanks for making the 'net possible for me and my family."

CERICSMITH FROM TWITTER

Home | Buy Now | Download | Premium Support | Free trial download | Privacy policy | License agreements

XP Internet Security 2012
© 2010 - 2012 LLC



ret@erw

213-435-

You Credit Card - Decline

Invalid value: cardnumber=4398349204337743

Retry entry

nd that the first digits
e your payment sec
obligatory to fill in t

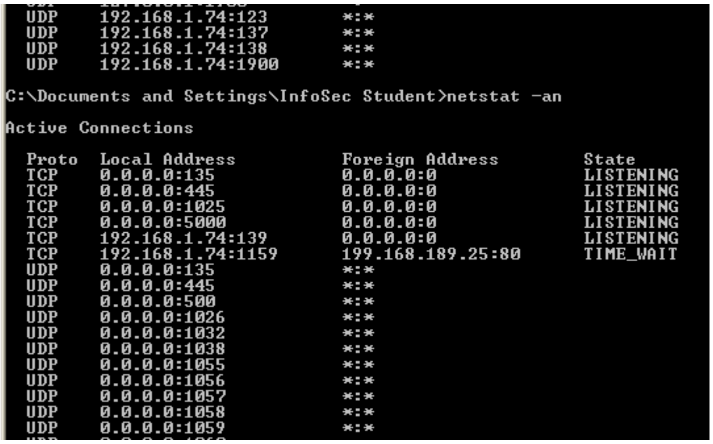
Visa

4398349204337743

viktor forrest

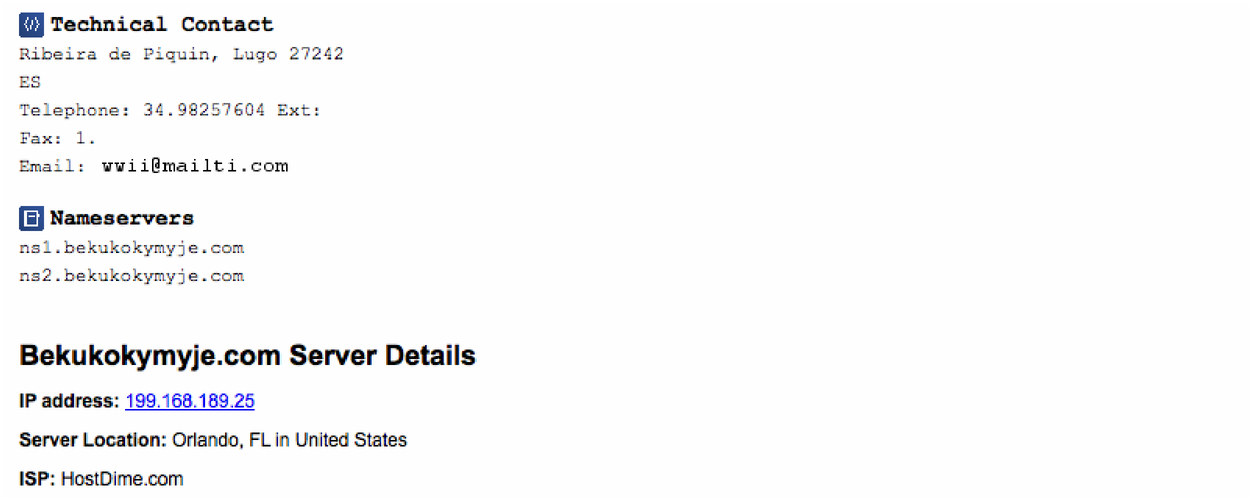
06 / 2016

023 3- or 4-digit number [Info]



```
  UDP    192.168.1.74:123       *:*
  UDP    192.168.1.74:137       *:*
  UDP    192.168.1.74:138       *:*
  UDP    192.168.1.74:1900      *:*

C:\Documents and Settings\InfoSec Student>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5000           0.0.0.0:0              LISTENING
  TCP    192.168.1.74:139       0.0.0.0:0              LISTENING
  TCP    192.168.1.74:1159      199.168.189.25:80      TIME_WAIT
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:1026           *:*
  UDP    0.0.0.0:1032           *:*
  UDP    0.0.0.0:1038           *:*
  UDP    0.0.0.0:1055           *:*
  UDP    0.0.0.0:1056           *:*
  UDP    0.0.0.0:1057           *:*
  UDP    0.0.0.0:1058           *:*
  UDP    0.0.0.0:1059           *:*
```

8.6 Whois, and geolocation trace of the two malicious IP's http://bekukokymyje.com/support.html that the victim made the connection to.



Technical Contact

Ribeira de Piquin, Lugo 27242
ES
Telephone: 34.98257604 Ext:
Fax: 1.
Email: wwii@mailti.com

Nameservers

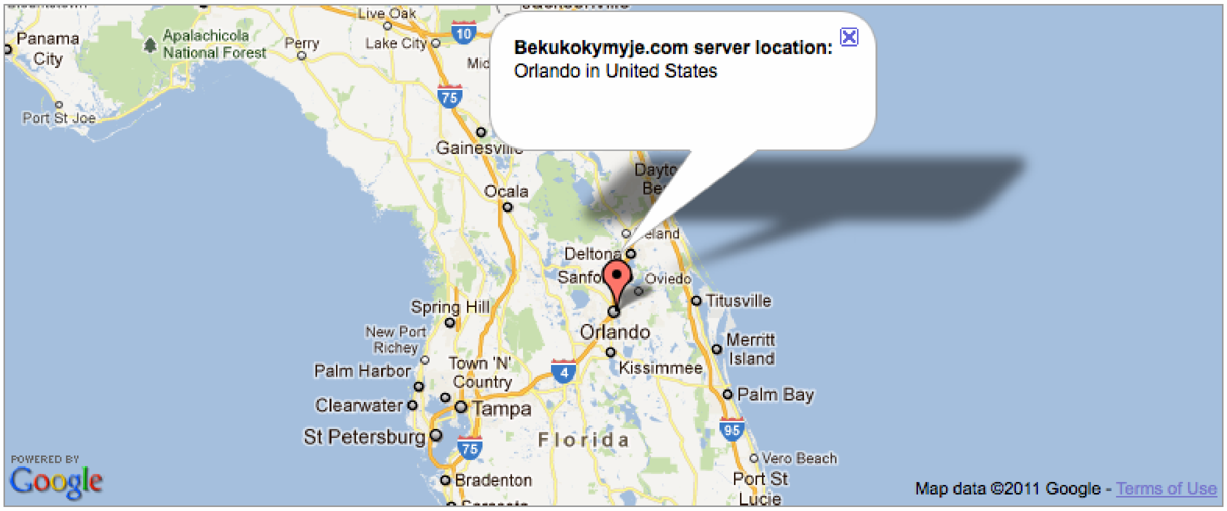
ns1.bekukokymyje.com
ns2.bekukokymyje.com

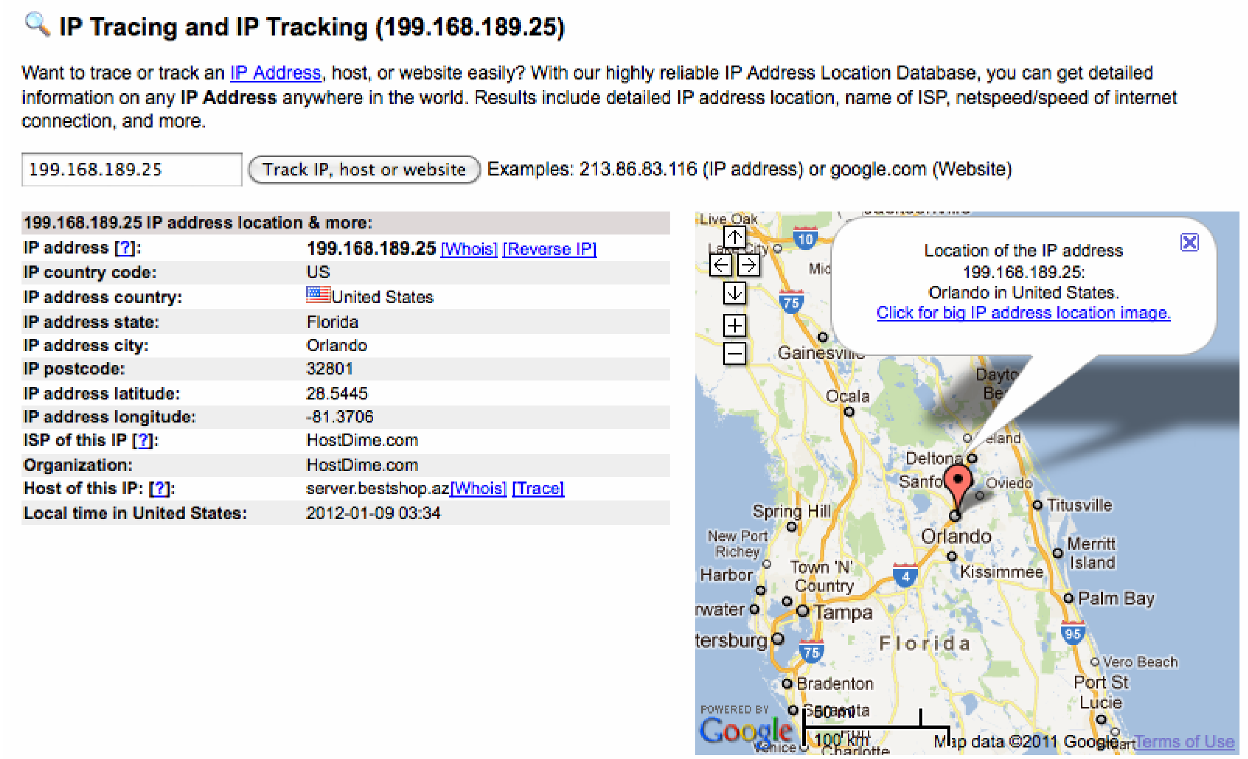
Bekukokymyje.com Server Details

IP address: 199.168.189.25

Server Location: Orlando, FL in United States

ISP: HostDime.com





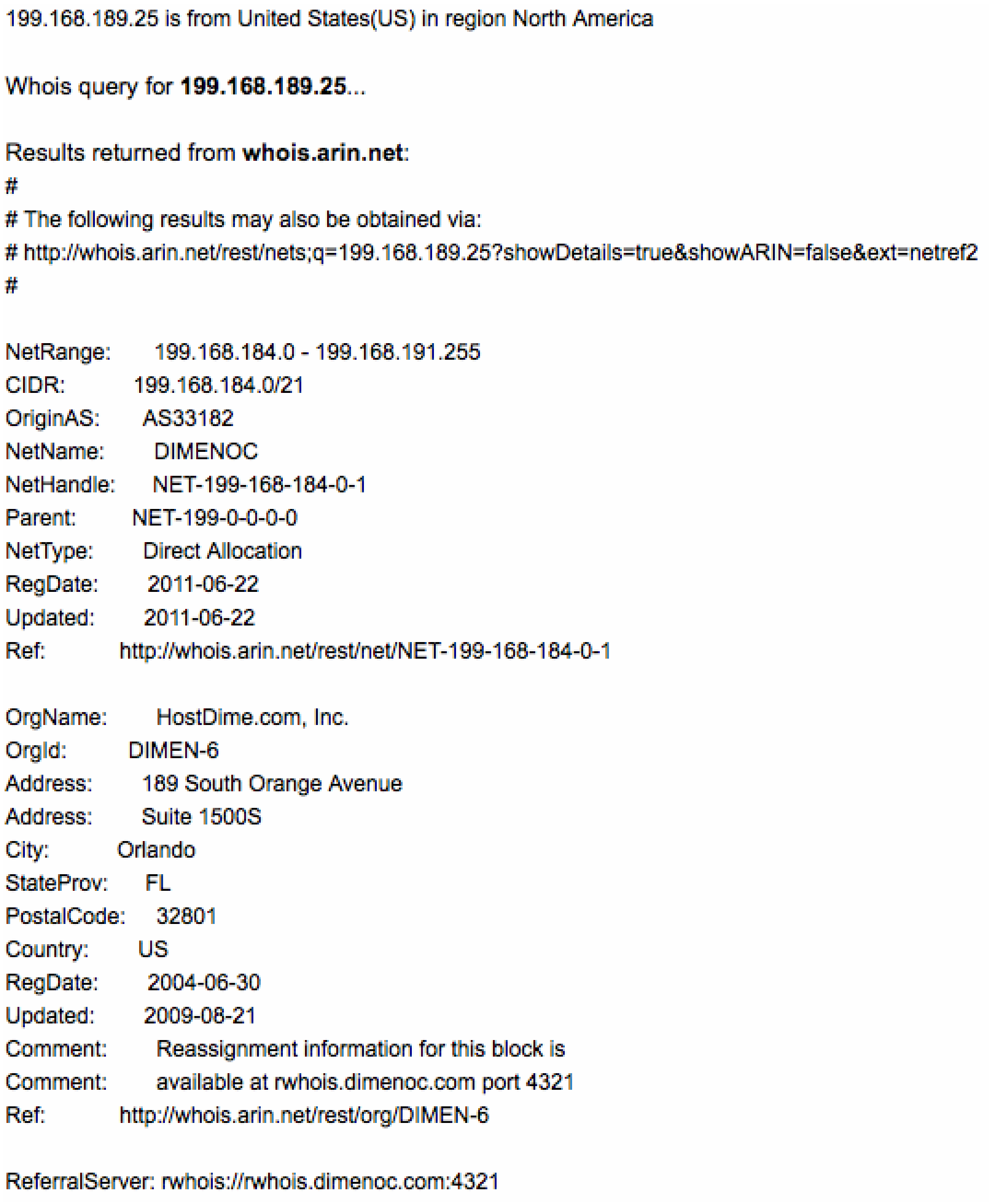
IP Tracing and IP Tracking (199.168.189.25)

Want to trace or track an IP Address, host, or website easily? With our highly reliable IP Address Location Database, you can get detailed information on any **IP Address** anywhere in the world. Results include detailed IP address location, name of ISP, netspeed/speed of internet connection, and more.

199.168.189.25 [Track IP, host or website] Examples: 213.86.83.116 (IP address) or google.com (Website)

199.168.189.25 IP address location & more:	
IP address [?]:	**199.168.189.25** [Whois] [Reverse IP]
IP country code:	US
IP address country:	United States
IP address state:	Florida
IP address city:	Orlando
IP postcode:	32801
IP address latitude:	28.5445
IP address longitude:	-81.3706
ISP of this IP [?]:	HostDime.com
Organization:	HostDime.com
Host of this IP: [?]:	server.bestshop.az[Whois] [Trace]
Local time in United States:	2012-01-09 03:34

Location of the IP address 199.168.189.25:
Orlando in United States.
Click for big IP address location image.



```
199.168.189.25 is from United States(US) in region North America

Whois query for 199.168.189.25...

Results returned from whois.arin.net:
#
# The following results may also be obtained via:
# http://whois.arin.net/rest/nets;q=199.168.189.25?showDetails=true&showARIN=false&ext=netref2
#

NetRange:       199.168.184.0 - 199.168.191.255
CIDR:           199.168.184.0/21
OriginAS:       AS33182
NetName:        DIMENOC
NetHandle:      NET-199-168-184-0-1
Parent:         NET-199-0-0-0-0
NetType:        Direct Allocation
RegDate:        2011-06-22
Updated:        2011-06-22
Ref:            http://whois.arin.net/rest/net/NET-199-168-184-0-1

OrgName:        HostDime.com, Inc.
OrgId:          DIMEN-6
Address:        189 South Orange Avenue
Address:        Suite 1500S
City:           Orlando
StateProv:      FL
PostalCode:     32801
Country:        US
RegDate:        2004-06-30
Updated:        2009-08-21
Comment:        Reassignment information for this block is
Comment:        available at rwhois.dimenoc.com port 4321
Ref:            http://whois.arin.net/rest/org/DIMEN-6

ReferralServer: rwhois://rwhois.dimenoc.com:4321
```

9. TIME AND LOCAL SYSTEM DEPENDANT FEATURES

9.1 This malware sample requires a valid internet connection, and execution to activate its payload. Once executed it makes numerous DNS requests to over 32 malicious sites to download the payload/instructions in a call home fashion.

10. METHOD AND MEANS OF COMMUNICATION

10.1 It communications, and receives the payload/instructions from the malicious server via port TCP 80.

10.2 Server details are : http://bekukokymyje.com/support.html with IP of 199.168.189.25 on TCP:80. The malicious server is located in Orlando Florida U.S.A.

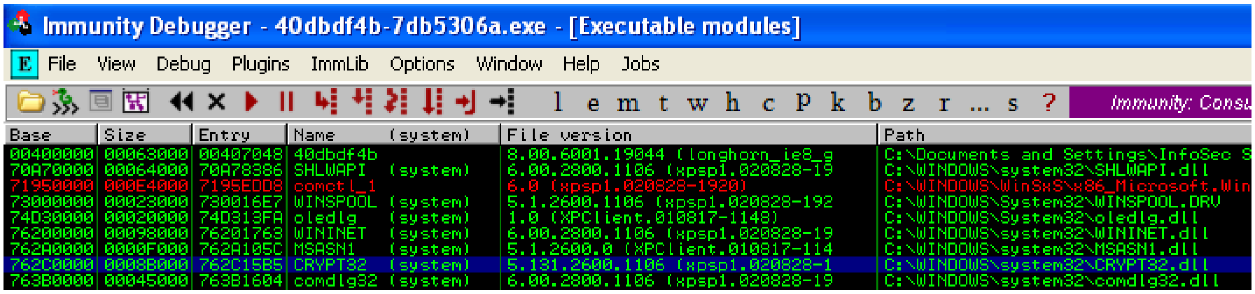
11. ORIGINAL INFECTION VECTOR AND PROPOGATION METHODOLOGY

11.1 The victim could have visited a normal looking site or may have been the victim of a brower exploit running an unpatched version of Internet Explorer. Typical drive by download is another scenario.

12. USE OF ENCRYPTION FOR STORAGE, DELIVERY AND OR COMMUNICATION

12.1 Nowadays advanced malware applications are either protected, obfuscated, encrypted (armoring) and/or packed (the original code is compressed, encrypted or both). This technique is applied in an attempt to evade signature based malware detection, and to hinder the efforts of static analysis by malware analysts by employing anti-reversing, anti-debugging and self-modifying code tactics. This malware sample is no different. The unpacking or decrypting of the malware layers remains the most complicated & sophisticated task in the overall process of malware analysis and finding the original entry point (OEP). True analysis of packed malicious binary code can only be performed after the payload is unpacked.

12.2 Loading the malware sample in Immunity debugger I noticed the following loaded module. C:\WINDOWS\system32\CRYPT32.dll is the module that implements many of the Certificate and Cryptographic Messaging functions in the CryptoAPI, such as CryptSignMessage. Crypt32.dll is a module that comes with the Windows and Windows Server operating systems, but different versions of this DLL provide different capabilities. There is no API to determine the version of CryptoAPI that is in use, but I can determine the version of crypt32.dll that is in use via the GetFileVersionInfo and VerQueryValue functions. The function is highlighted in blue below.


Immunity Debugger - 40dbdf4b-7db5306a.exe - [Executable modules]
E File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Immunity: Consu

Base	Size	Entry	Name (system)	File version	Path
00400000	00063000	00407048	40dbdf4b	8.00.6001.19044 (longhorn_ie8_g	C:\Documents and Settings\InfoSec S
70A70000	00064000	70A78386	SHLWAPI (system)	6.00.2800.1106 (xpsp1.020828-19	C:\WINDOWS\system32\SHLWAPI.dll
71950000	000E4000	7195EDD8	comctl_1	6.0 (xpsp1.020828-1920)	C:\WINDOWS\WinSxS\x86_Microsoft.Win
73000000	00023000	730016E7	WINSPOOL (system)	5.1.2600.1106 (xpsp1.020828-192	C:\WINDOWS\System32\WINSPOOL.DRV
74D30000	00020000	74D313FA	oledlg (system)	1.0 (XPClient.010817-1148)	C:\WINDOWS\System32\oledlg.dll
76200000	00098000	76201763	WININET (system)	6.00.2800.1106 (xpsp1.020828-19	C:\WINDOWS\system32\WININET.dll
762A0000	0000F000	762A105C	MSASN1 (system)	5.1.2600.0 (XPClient.010817-114	C:\WINDOWS\system32\MSASN1.dll
762C0000	0008B000	762C15B5	CRYPT32 (system)	5.131.2600.1106 (xpsp1.020828-1	C:\WINDOWS\system32\CRYPT32.dll
763B0000	00045000	763B1604	comdlg32 (system)	6.00.2800.1106 (xpsp1.020828-19	C:\WINDOWS\system32\comdlg32.dll

Executable modules, item 7

Base=762C0000

Size=0008B000 (569344.)

Entry=762C15B5 CRYPT32.<ModuleEntryPoint>

Name=CRYPT32 (system)

File version=5.131.2600.1106 (xpsp1.020828-1

Path=C:\WINDOWS\system32\CRYPT32.dll

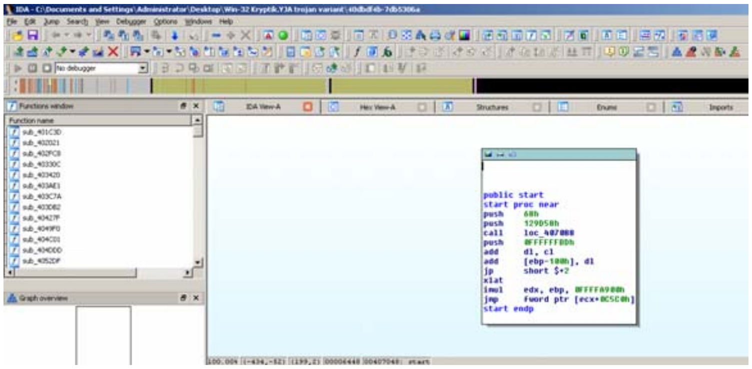
13. USE OF SELF MODIFYING/REPLICATING OR ENCRYPTED CODE

13.1 I noticed each time I executed the malware sample that the names of the dropped malicious files ".exe's" always changed to a random string/name. Different every single time. This might indicate the use of the rand function within the code. Other than the random naming convention on the malicious executables, the network traffic seemed to be always the same. The malware sample stuck to the same 32 malicious domains in it's C&C structure.

14. ANY INFORMATION CONCERNING DEVELOPMENT OF MALWARE (COMPILER TYPE, PACKER USED, COUNTRY OF ORIGIN, AUTHOR, NAMES/HANDLES, ETC.)

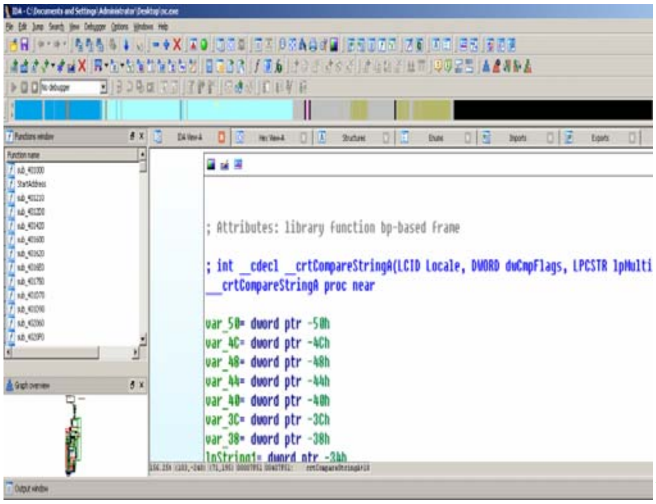
14.1 Reverse engineering using static analysis on the malware sample allows me to understand its functionality. Loading the malware sample indicated it might be packed/compressed for several reasons. The memory visualization bar within the

IDA GUI was not able to find any encoded/executable data. Usually normal un-packed executables have several blue sections with readable data. Below is a comparison of a packed executable vs a non packed executable application.



```
public start
start proc near
push    60h
push    129D58h
call    loc_407000
push    0FFFFFF0Dh
add     dl, cl
add     [ebp-100h], dl
jp      short $+2
xlat
imul    edx, ebp, 0FFFFA900h
jmp     fword ptr [ecx+0C5C0h]
start endp
```

← PACKED

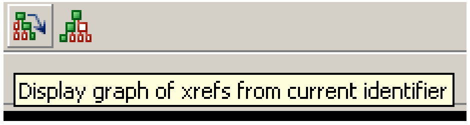


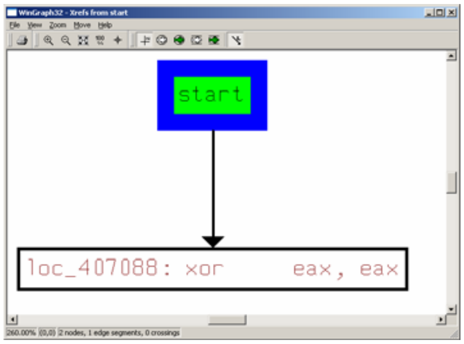
```
; Attributes: library function bp-based frame

; int __cdecl __crtCompareStringA(LCID Locale, DWORD dwCmpFlags, LPCSTR lpMulti
__crtCompareStringA proc near

var_50= dword ptr -50h
var_4C= dword ptr -4Ch
var_48= dword ptr -48h
var_44= dword ptr -44h
var_40= dword ptr -40h
var_3C= dword ptr -3Ch
var_38= dword ptr -38h
lpString1= dword ptr -34h
```

← UNPACKED

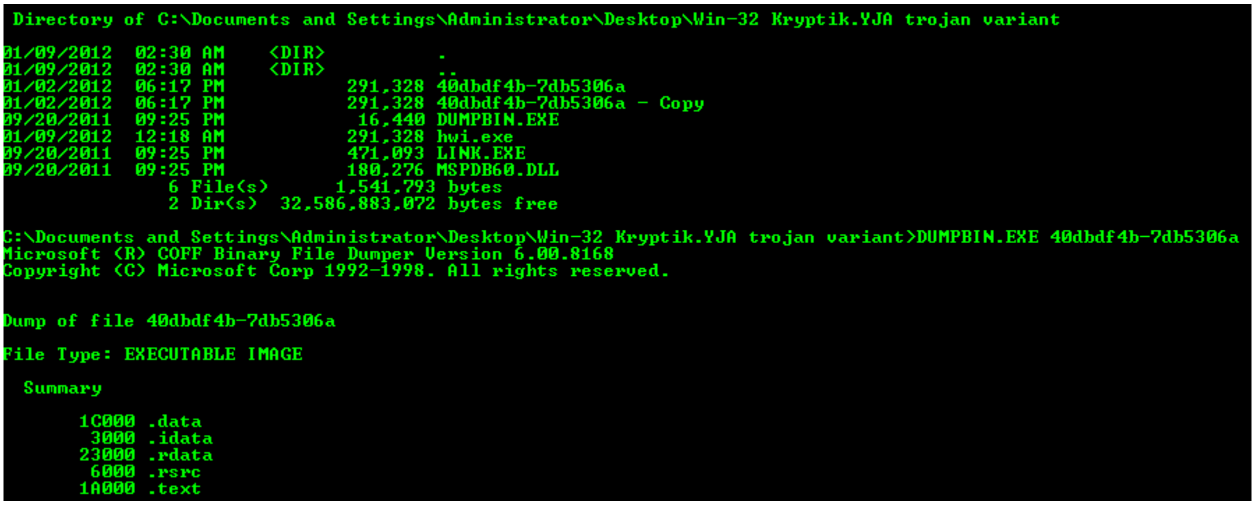
Note the memory visualization bar within the unpacked nc.exe application, and the graph overview.

14.2 Next is a high level overview of the malware sample which involves using the start function and the "display graph of xref's from current identifier" button. This method allows us to generate a visualization graph. The graph allows us to zoom in and inspect various portions of the program and see how much of it is actually system API calls versus custom implemented code. We can also use the graph overview to see all the function calls the application is making.



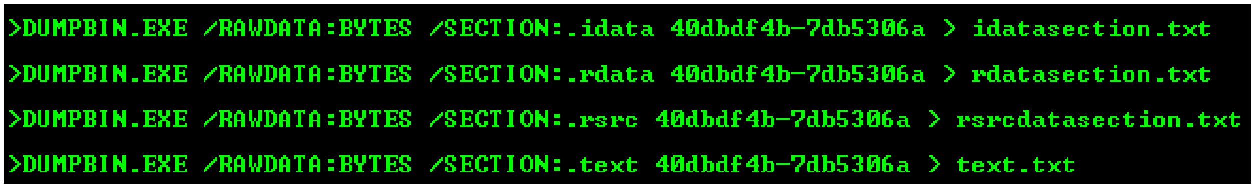

WinGraph32 - Xrefs from start
File View Zoom Move Help
start
loc_407088: xor eax, eax
260.00% (0,0) 2 nodes, 1 edge segments, 0 crossings

14.3 I began by dumping the basic headers and imports/export entries in the malware sample using the dumpbin program. I extracted all data from all available sections of the malware sample. Sections that are available are .data, .idata, .rdata (hardcoded passwords/sometimes), .rsrc (resource), and .text (program code) as pictured below.



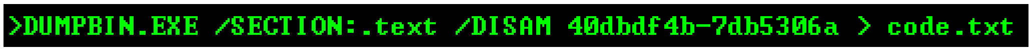
```
 Directory of C:\Documents and Settings\Administrator\Desktop\Win-32 Kryptik.YJA trojan variant

01/09/2012  02:30 AM    <DIR>          .
01/09/2012  02:30 AM    <DIR>          ..
01/02/2012  06:17 PM           291,328 40dbdf4b-7db5306a
01/02/2012  06:17 PM           291,328 40dbdf4b-7db5306a - Copy
09/20/2011  09:25 PM            16,440 DUMPBIN.EXE
01/09/2012  12:18 AM           291,328 hwi.exe
09/20/2011  09:25 PM           471,093 LINK.EXE
09/20/2011  09:25 PM           180,276 MSPDB60.DLL
               6 File(s)      1,541,793 bytes
               2 Dir(s)  32,586,883,072 bytes free

C:\Documents and Settings\Administrator\Desktop\Win-32 Kryptik.YJA trojan variant>DUMPBIN.EXE 40dbdf4b-7db5306a
Microsoft (R) COFF Binary File Dumper Version 6.00.8168
Copyright (C) Microsoft Corp 1992-1998. All rights reserved.


Dump of file 40dbdf4b-7db5306a

File Type: EXECUTABLE IMAGE

  Summary

       1C000 .data
        3000 .idata
       23000 .rdata
        6000 .rsrc
       1A000 .text
```

14.4 I ran the following commands and dumped the above sections into .txt files for further analysis.



```
>DUMPBIN.EXE /RAWDATA:BYTES /SECTION:.idata 40dbdf4b-7db5306a > idatasection.txt

>DUMPBIN.EXE /RAWDATA:BYTES /SECTION:.rdata 40dbdf4b-7db5306a > rdatasection.txt

>DUMPBIN.EXE /RAWDATA:BYTES /SECTION:.rsrc 40dbdf4b-7db5306a > rsrcdatasection.txt

>DUMPBIN.EXE /RAWDATA:BYTES /SECTION:.text 40dbdf4b-7db5306a > text.txt
```

14.5 Next I performed a full binary disassembly with all libraries included.



```
>DUMPBIN.EXE /SECTION:.text /DISAM 40dbdf4b-7db5306a > code.txt
```

15. KEY QUESTIONS AND ANSWERS

- How did the malware infection occur?

  [drive-by infection from site Yes]
- When did the malware infection occur?

  [On or before Jan. 04, 2012]
- What vulnerabilities allowed the infection to occur?

  [Unpatched Internet Explorer/ drive-by infection/banner Ad]
- What is the risk of data loss?

  [High: Kryptik/Data Stealing Trojan on machine for several days]

16. CONCLUSIONS AND RECOMMENDATIONS TO PREVENT INCIDENT FROM RECURRING

On Jan. 04, 2012, While browsing the internet, ANONYMOUS triggered a drive-by infection probably coming from a banner ad. The drive-by infection triggered a series of exploit steps, eventually resulting in installation of a trojan downloader and the Win-32 Kryptik.YJA trojan variant. Because Kryptic is a data-stealing trojan, any sensitive information handled by the victim between date of infection and the date of the investigation (January 09, 2012) should be considered potentially compromised.

IT Security should implement a hardened browser standard operating procedure.

This SOP should include for example, disabling JavaScript, browser hardening standards (NSA), installing no-script, and removing admin access for affected users. Also take a look at official DoD, Sans papers on browser hardening or

www.us-cert.gov/reading_room/secure_browser/

17. FOLLOWUP ACTIONS AND LESSONS LEARNED

17.1 Blacklist the entire offending IP block/s.

17.2 Reset user password. Re-image victim machine. If the user used ANY personal passwords to login to ANY websites (banking, social media, news feeds, educational, work websites), he should reset said passwords, and notify companies he does business. Especially if he logged on to any banking website. Users Active Directory account password should be reset, and be monitored for any unusual/unauthorized activity.

REFS used in my .pdf report.

Generic Unpacking of Self-modifying, Aggressive, Packed Binary Programs

http://arxiv.org/abs/0905.4581

Practical malware analysis

www.blackhat.com/.../bh-dc.../bh-dc-07-Kendall_McMillan-WP.pdf

What to Include in a Malware Analysis Report

http://zeltser.com/reverse-malware/malware-analysis-report.html

Malware Analysis 101

http://zeltser.com/reverse-malware/malware-analysis-webcast.html