www.fidelissecurity.com
www.threatgeek.com
@FidSecSys
+1800.652.4020

Fidelis Threat Advisory #1014

Bots, Machines, and the Matrix

Dec 12, 2014

Document Status: 1.0
Last Revised: 2014-12-11

Executive Summary

In the recent past, a Fidelis XPS user reported seeing detections of what appeared to be botnet-related malware. While that customer was protected, we at General Dynamics Fidelis Cybersecurity Solutions decided to take a closer look. The analysis of the malicious code revealed that it appeared to be Andromeda but the delivery infrastructure looked interesting. Further telemetry from our sensors showed that this server in China was also hosting and distributing many other malicious specimens. Analysis of the data revealed a pattern in the filenames. Our analysts used this pattern to discover other systems distributed across the globe serving up various botnet malware, so far assumed to be used in distinct campaigns but clearly related in this case:

- Andromeda
- Beta Bot
- Neutrino Bot
- NgrBot/DorkBot

Analysis also showed how attackers continue to benefit from the use of globally-distributed hosting providers to perform their malicious activities. Further, the analysis revealed how attackers are hosting and distributing identical copies of the malware from servers in different countries including China, Poland, Russia, and the United States.

For the period of time researched in this activity, we observed the following targeted sectors in the US:

- Manufacturing / Biotechnology & Drugs
- Professional Services / Engineering
- Information Technology / Telecommunications
- Government / State

Note that our footprint is largely in the Enterprise space and it is possible that we're seeing spillover from wider campaigns.

This document uncovers various servers hosting Bots and other related malware, provides a triage analysis of various pieces of malware hosted by these malicious servers, and provides indicators that network defenders can use to protect their networks.

Threat Overview

The threat activity observed in the past weeks against various targets in our customer base has shown patterns that allowed us to discover multiple servers hosting and distributing malicious software (Bots).

As it is known by the network defenders and the security community, it is important to defend against these attacks since systems infected with these malicious specimens could be used for credential theft, Distributed Denial of Service Attacks, spreading malware, lateral propagation, etc. This is of great concern as the first stage attack continues to bypass network security defenses infecting user's computers that beacon to malicious servers to download or create the second stage malware into the victim systems.

Some of the main Bot types of malware detected through this research include:

- **Andromeda**

  Andromeda is a modular bot that downloads modules and updates from its command and control (C&C) server during execution. The malware has both anti-VM and anti-reversing features. Its code is obfuscated to make it more difficult for malware reverse engineers to analyze and antivirus tools to detect.

  Andromeda bot features include: self-propagation, injection into trusted processes to hide itself, network traffic encryption, download and installation of files/malware, form grabber, keylogger, ring3 rootkit, proxy, etc. Features like form grabber, rootkit, and proxy are delivered to the malware in the form of modules that are then loaded into the victim system after the malware makes a connection with its C&C. It appears that in 2012, some of the modules were sold for $500 (form grabber), $300 (Ring3 rootkit), and $200 (keylogger).

- **DorkBot/NgrBot**

  DorkBot is a modified IRCBot that is very similar in features to NgrBot. DorkBot has a loader and a module. The bot includes the following features: process injection, hard drive wiping, etc. Different from NgrBot, DorkBot uses modified IRC commands. Some of the commands supported include: !die, !dl, !http.inj, !logins, !rc,!speed, !ssyn, !stop, !up, and !udp.

  NgrBot can also be remotely controlled via Internet-Relay-Chat (IRC) protocol. It has capabilities to join different IRC channels to perform various attacks according to the IRC-based commands from the C&C server. Its code is obfuscated to make it more difficult for malware reverse engineers to analyze and antivirus tools to detect.

  NgrBot features include: self-propagation (e.g. through USB removable drives, social networking sites, and messaging clients), process injection, hard drive wiping, blocking access to multiple antivirus/security vendor websites, denial of service attacks, credentials stealing (usernames and passwords), download and execute file, etc. Some of the commands supported are: ~pu, ~dw, ~http.inj, ~logins, ~rc, ~speed, ~ssyn, ~stop, and ~udp.

- **Beta Bot**

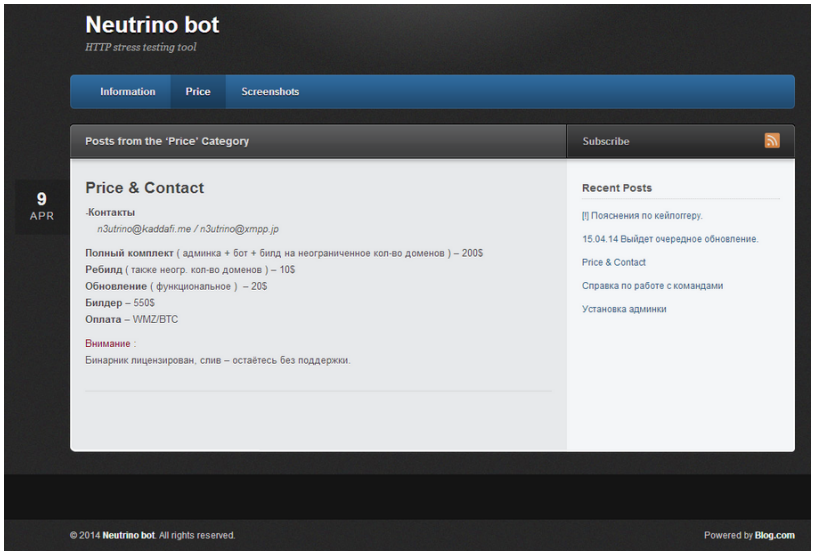
  It is said that Beta bot started out as an HTTP bot. The Bot is also known by some security vendors as 'Trojan.Neurevt'. Its code is obfuscated to make it more difficult for malware reverse engineers to analyze and antivirus tools to detect.

  Beta bot features include: anti-VM and anti-reversing, self-propagation, rootkit, process injection, blocking access to multiple antivirus/security vendor websites, AV-disabling, form grabbing, download and execution of files, termination of competing malware communications by terminating their processes or blocking their code injections, and denial of service. It appears that

in May 2013, the pre-built bot could be purchase for $320-$500, and $20 for variant rebuilds for those requiring configuration changes. According to online research, Beta Bot sales are being handled by “Lord Huron,” although “betamonkey” appears to be the author. The following image was found during online research:

- **Neutrino**

The Neutrino bot was advertised as an HTTP stress-testing tool. It has some of the following features: anti-VM and anti-reversing/debugging, denial of service (HTTP/TCP/UDP flood), keylogger, command shell, credential stealing, self-spreading, etc. It appears at some point the bot was sold for $550 (Builder), $200 (Full set including Bot and Admin Panel), and $20 (Update). Online research revealed the following contact information for this bot: n3utrino@kaddafi[.]me / n3utrino@xmpp[.]jp / n3utrino.blog[.]com. The following images were found during online research:



The following table provides information about some of the servers hosting and distributing malware and some of the filename patterns discovered:

Last Observed	IP	Location	Filename Pattern
December 2014	121.11.83[.]7	China	and*[2_digits]**[single character]**[2_digits]*.exe bet*[2_digits]**[single character]**[2_digits]*.exe ng*[2_digits]**[single character]**[2_digits]*.exe nut*[2_digits]**[single character]**[2_digits]*.exe
December 2014	155.133.18[.]45	Poland	bet*[2_digits]**[single character]**[2_digits]*.exe bnew*[2_digits]**[single character]**[2_digits]*.exe ng*[2_digits]**[single character]**[2_digits]*.exe nut*[2_digits]**[single character]**[2_digits]*.exe *[3_digits]**[single character]**[1_digit]*.exe *[2_digits]**[single character]**[1_digit]*.exe
December 2014	54.69.90[.]62	US (Amazon)	and*[2_digits]**[single character]**[2_digits]*.exe bet*[2_digits]**[single character]**[2_digits]*.exe bnew*[2_digits]**[single character]**[2_digits]*.exe dq*[2_digits]**[single character]**[2_digits]*.exe dqnew*[2_digits]**[single character]**[2_digits]*.exe ng*[2_digits]**[single character]**[2_digits]*.exe nut*[2_digits]**[single character]**[2_digits]*.exe
November 2014	117.21.191[.]47	China	and*[2_digits]**[single character]**[2_digits]*.exe and*[single character]**[1_digit]*.exe bet*[2_digits]**[single character]**[2_digits]*.exe bet*[1_or_2_digits].exe* bet*[single character]**[1_digit]**.exe* ng*[2_digits]**[single character]**[2_digits]*.exe nut*[2_digits]**[single character]**[2_digits]*.exe
November 2014	121.14.212[.]184	China	and*[2_digits]**[single character]**[2_digits]*.exe and*[2_digits]*.exe and*[2_digits]**[single character]*.exe bet*[2_digits]**[single character]**[2_digits]*.exe bet*[2_digits]*.exe ng*[2_digits]**[single character]**[2_digits]*.exe ng*[2_digits]*.exe nut*[2_digits]**[single character]**[2_digits]*.exe nut*[2_digits]*.exe nut*[2_digits]**[single character]*.exe zpm*[2_digits]**[single character]*.exe
November 2014	155.133.18[.]44	Poland	3307*[2_digits]**[single character]**[2_digits]*.exe and*[2_digits]**[single character]**[2_digits]*.exe bet*[2_digits]**[single character]**[2_digits]*.exe bnew*[2_digits]**[single character]**[2_digits]*.exe

November 2014	54.68.121[.]73	US (Amazon)	and*[2_digits][single character][2_digits]*.exe bet*[2_digits][single character][2_digits]*.exe bnew*[2_digits][single character][2_digits]*.exe ng*[2_digits][single character][2_digits]*.exe nut*[2_digits][single character][2_digits]*.exe
November 2014	54.68.194[.]154	US (Amazon)	and*[2_digits][single character][2_digits]*.exe bet*[2_digits][single character][2_digits]*.exe ng*[2_digits][single character][2_digits]*.exe nut*[2_digits][single character][2_digits]*.exe
November 2014	54.69.90[.]62	US (Amazon)	3307*[2_digits][single character][2_digits]*.exe and*[2_digits][single character][2_digits]*.exe bet*[2_digits][single character][2_digits]*.exe bnew*[2_digits][single character][2_digits]*.exe ng*[2_digits][single character][2_digits]*.exe
October 2014	119.1.109[.]44	China	and*[2_digits][single character][2_digits]*.exe and*[2_digits]*.exe bet*[2_digits][single character]*.exe bet*[2_digits]*.exe ng*[2_digits][single character][2_digits]*.exe nut*[2_digits]*.exe
October 2014	158.255.1[.]241	Russia	and*[2_digits]*.exe ng*[2_digits]*exe nut*[2_digits][single character][2_digits]*.exe nut*[2_digits]*.exe
October 2014	54.191.142[.]124	US (Amazon)	bnew*[2_digits]*.exe ng*[2_digits]*.exe nut*[2_digits]*.exe zpm*[2_digits]*.exe

The following table provides information about the relationship between the malicious servers, detection names by antivirus tools, and vertical market affected (based on unique hashes and detections):

IP	Location	Generic AV detection	Vertical Market/Specialization
121.11.83[.]7	China	Worm.Win32.Ngrbot Worm.Win32.Dorkbot	Professional Services/Engineering

		Backdoor.Win32.Ruskill Trojan.Win32.Yakes Trojan.Win32.Munchies	
155.133.18[.]45	Poland	Backdoor.Win32.Androm Trojan.Win32.Lethic Trojan.Win32.Inject Trojan.Win32.Munchies Trojan.Win32.Yakes	
54.69.90[.]62	US (Amazon)	Backdoor.Win32.Androm Worm.Win32.Ngrbot Worm.Win32.Dorkbot Backdoor.Win32.Ruskill Trojan.Win32.Lethic Trojan.Win32.Yakes Trojan.Win32.Munchies	
117.21.191[.]47	China	Backdoor.Win32.Androm Trojan.Win32.Betabot Worm.Win32.Dorkbot Backdoor.Win32.Ruskill Trojan.Win32.Neurevt Worm.Win32.Ngrbot Trojan-Spy.Win32.SpyEyes Trojan-Spy.Win32.Zbot Backdoor.Win32.Azbreg Trojan.Win32.Badur Trojan.Win32.Inject Trojan.Win32.Sharik Trojan.Win32.Yakes Trojan-Downloader.Win32.Agent Trojan-Dropper.Win32.Injector	Manufacturing/Healthcare
121.14.212[.]184	China	Backdoor.Win32.Androm Worm.Win32.Ngrbot Backdoor.Win32.Ruskill Trojan.Win32.Badur Trojan.Win32.Inject Trojan.Win32.Yakes Trojan.Win32.Sysn	Manufacturing/Healthcare/Government
155.133.18[.]44	Poland	Backdoor.Win32.Androm Worm.Win32.Ngrbot Trojan.Win32.Badur Trojan.Win32.Yakes	
54.68.121[.]73	US (Amazon)	Backdoor.Win32.Androm Trojan.Proxy.Win32.Lethic Worm.Win32.Ngrbot	Government

		Trojan.Win32.Badur Trojan.Win32.Inject	
54.68.194[.]154	US (Amazon)	Backdoor.Win32.Androm Backdoor.Win32.Ruskill Trojan.Win32.Yakes	

119.1.109[.]44	China	Backdoor.Win32.Androm Worm.Win32.Ngrbot Backdoor.Win32.Ruskill Trojan.Win32.Badur Trojan.Win32.Yakes	
158.255.1[.]241	Russia	Backdoor.Win32.Androm Worm.Win32.Ngrbot Trojan.Win32.Badur Trojan.Win32.Yakes	Government
54.191.142[.]124	US (Amazon)	Backdoor.Win32.Androm Worm.Win32.Ngrbot Trojan.Win32.Badur Worm.Win32.Hamweq Trojan.Win32.Sysn	

Risk Assessment

A bot malware has features like anti-reversing, credential stealing/keystroke logging/form grabbing, DNS changer, process injection, antivirus process killing, blocking of security related websites, backdoor, and others. They also have features to spread themselves through USB removable drives, social networking sites, and messaging clients. In addition, they could also infiltrate the network when the victim user visits a website hosting a browser exploit.

Once the attacker gains control, the infected system could be used to launch Distributed Denial of Service attacks, spread the bot to other victims, download more advanced malware to perform lateral propagation, etc. The attackers (Bot Masters/Herders) could also rent their botnets to other cybercriminals.

Indicators and Mitigation Strategies

This section presents information about some of the servers we have observed hosting and distributing malware, filename patterns, as well as a triage analysis of various pieces of malware observed delivered by these servers

- Servers observed hosting and distributing malware:

121.11.83[.]7	121.14.212[.]184	119.1.109[.]44	117.21.191[.]47
155.133.18[.]44	155.133.18[.]45	158.255.1[.]241	217.23.6[.]112
54.191.142[.]124	54.68.121[.]73	54.68.194[.]154	54.69.90[.]62

77.87.79[.]128			

- Some of the filename patterns observed:

121.11.83[.]7/and40a70.exe	121.11.83[.]7/bet40a71.exe	121.11.83[.]7/ng40a71.exe
155.133.18[.]45/37a1.exe	54.69.90[.]62/330740a71.exe	54.69.90[.]62/bnew40a71.exe
155.133.18[.]45/109a7.exe	155.133.18[.]45/51a5.exe	155.133.18[.]45/62.exe
121.14.212[.]184/ng33.exe	121.14.212[.]184/zpm39a.exe	155.133.18[.]45/141a1.exe
217.23.6[.]112/98.exe	54.191.142[.]124/zpm37.exe	54.69.90[.]62/bnew40a85.exe
121.11.83[.]7/nut40a71.exe	54.69.90[.]62/dqnew40a81.exe	119.1.109[.]44/and33.exe
217.23.6[.]112/330740x.exe	77.87.79[.]128/37extra.exe	158.255.1[.]241/ng38a.exe

- Triage analysis of various pieces of malware observed delivered by servers mentioned in this report: (Please note that the activity in this section has been recorded per initial file infection and not individually per file downloaded and executed by the initial malware under investigation)

  - **Andromeda**
    MD5: 036eb11a5751c77bc65006769921c8e5

    This file was observed hosted in the following servers:

    1. 119.1.109[.]44/and37.exe (China)
    2. 121.14.212[.]184/and37.exe (China)
    3. 54.68.121[.]73/and37.exe (US)

    File information:

```
File Name:  and37.exe
File Size:  118784 bytes
MD5:        036eb11a5751c77bc65006769921c8e5
SHA1:       c6966d9557a9d5ffbbcd7866d45eddff30a9fd99
PE Time:    0x5431A1E4 [Sun Oct 05 19:54:12 2014 UTC]
PEID Sig:   Microsoft Visual C++ 8
Sections (4):
  Name      Entropy  MD5
  .text     6.48     851019d9ac5c3c1853a62535bb42fe25
  .rdata    5.48     5e0faee1b5962f3b0e7ef0cd07b07d90
  .data     4.99     87595d36a05bbbfdab643e78f1b1dad4
  .rsrc     6.59     5923da4653b7fcb4ee9062367873a2ed
```

    The malware appears to implement anti-reversing techniques preventing its executing inside a virtual machine environment (VME). This malware is believed to be a variant from the 'Andromeda Bot' malware family.

    When the file was executed in a Windows 7 system, the following activity was observed:

    Domain: a2kiaymoster14902[.]com
    Resolved IP: **121.14.212[.]248 (China)**
    POST request: /bla02/gate.php
    GET request: **54.69.90[.]62/and40a90.exe (US)**
    File downloaded: b62391f3f7cbdea02763614f60f3930f (msitygyd.exe)
    Full path and name: C:\ProgramData\msitygyd.exe
    Process injection: C:\Windows\SysWOW64\msiexec.exe

- **Beta Bot**
  MD5: 9e8b203f487dfa85dd47e32b3d24e24e

  This file was observed hosted in the following servers:

  1. 117.21.191.47/betw9.exe (China)
  2. 54.191.142.124/bet4.exe (US)

  File information:

```
File Name:  betw9.exe
File Size:  379904 bytes
MD5:        9e8b203f487dfa85dd47e32b3d24e24e
SHA1:       de6a4d53b5265f8cddf08271d17d845f58107e82
PE Time:    0x5414994B [Sat Sep 13 19:21:47 2014 UTC]
PEID Sig:   Microsoft Visual C++ 8
Sections (4):
  Name      Entropy  MD5
  .text     6.47     4e347b4bb29e39a97c5803db1ee53321
  .rdata    1.99     692d4fc093dc013fa7d86bee7b85c0f9
  .data     4.22     52daa66602eb4a3aa8effd3a287efbf7
  .rsrc     6.1      9b2a41b9bc48ccff04effe10bb0fb839
  .rsrc     6.59     5923da4653b7fcb4ee9062367873a2ed
```

  The malware did not appear to implement anti-reversing techniques and properly executed inside a VME. This malware is believed to be a variant from the 'Beta Bot' malware family.

  When the file was executed in a Windows XP system, the following activity was observed:

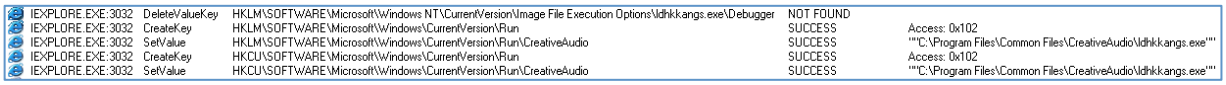
Domain:	b.9thegamejuststarted14k9[.]com
Resolved IP:	**116.255.202[.]74 (China)**
POST request:	/direct/mail/order.php?id=9156969
GET request:	**121.14.212[.]184/ng40a54.exe (China)**
File downloaded:	fe8c978f05f3a83af7c8905f94f71213 (mxbrwtqjjvk.exe)
Full path and name:	%TEMP%\mxbrwtqjjvk.exe
GET request:	**121.14.212[.]184/and40a54.exe (China)**
File downloaded:	7599016887b4d6c0e3bc2ecda983161f (cmqgvyqtpkh.exe)
Full path and name:	%TEMP%\cmqgvyqtpkh.exe
Made a copy itself to:	%CommonProgramFiles%\CreativeAudio\ldhkkangs.exe
Hash of file copy:	9e8b203f487dfa85dd47e32b3d24e24e

  Registry entrenchment:

Key:	**HKEY_LOCAL_MACHINE**\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Value Name:	CreativeAudio
Value Data:	C:\Program Files\Common Files\CreativeAudio\ldhkkangs.exe
Key:	**HKEY_CURRENT_USER**\Software\Microsoft\Windows\CurrentVersion\Run
Value Name:	CreativeAudio
Value Data:	C:\Program Files\Common Files\CreativeAudio\ldhkkangs.exe

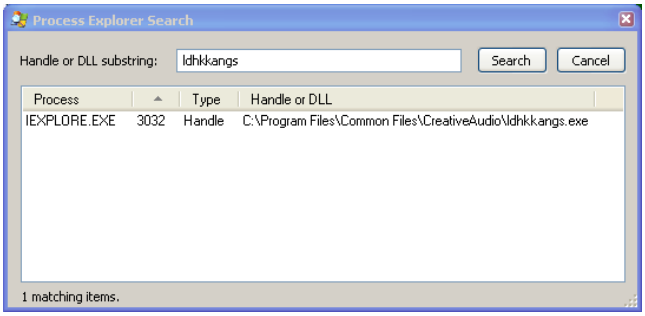
Process Injection: C:\Program Files\Internet Explorer\iexplore.exe

Screenshot of the registry activity:



IEXPLORE.EXE:3032	DeleteValueKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ldhkkangs.exe\Debugger	NOT FOUND	
IEXPLORE.EXE:3032	CreateKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Access: 0x102
IEXPLORE.EXE:3032	SetValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\CreativeAudio	SUCCESS	""C:\Program Files\Common Files\CreativeAudio\ldhkkangs.exe""
IEXPLORE.EXE:3032	CreateKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Access: 0x102
IEXPLORE.EXE:3032	SetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\CreativeAudio	SUCCESS	""C:\Program Files\Common Files\CreativeAudio\ldhkkangs.exe""

Screenshot showing a handle of the malware in the “iexplorer.exe” process:



- **Neutrino Bot**
  MD5: 463f7191363d0391add327c1270d7fe6

  This file was observed hosted in the following servers:

  1. 121.14.212[.]184/nut40a52.exe (China)
  2. 155.133.18[.]45/nut40a52.exe (Poland)

  File information:

```
File Name:  nut40a52.exe
File Size:  145408 bytes
MD5:        463f7191363d0391add327c1270d7fe6
SHA1:       a87c5b6a588ef4b351ce1a3a0fe2b035e685e96c
PE Time:    0x546D0881 [Wed Nov 19 21:15:45 2014 UTC]
PEID Sig:   Microsoft Visual C++ 8
Sections (4):
  Name      Entropy  MD5
  .text     6.65     6fe50af0b54ed30227099ea6b9e7178b
  .rdata    5.54     43ff7c660e83eeff9a7db4abf0ceab04
  .data     5.74     e19f755461a13879499bd1e8e7471807
  .rsrc     7.66     399357dac81db1ae19c69e8a2b7e5311
```

  The malware appears to implement anti-reversing techniques preventing it from properly executing inside a VME. In a bare-metal system, the malware worked properly. This malware is believed to be a variant from the ‘Neutrino Bot’ malware family.

  When the file was executed in a Windows 7 system, the following activity was observed:

  Domain: nutqlfkq123a10[.]com
  Resolved IP: **121.61.118[.]140 (China)**
  POST request: /newfiz3/tasks.php
  Data: ping=1

Server response: pong
POST request: /newfiz3/tasks.php
Data: getcmd=1&uid=*[removed]*&os=Win+7+Enterprise+(x64)&av=Symantec+Endpoint+Protection&nat=yes&version=3.2.1&serial=*[removed]*&quality=0
POST request: /newfiz3/tasks.php
Data: taskexec=1&task_id=1416470040933917

GET request: 54.69.90[.]62/330740a91.exe
File downloaded: b21e4c8f73151d7b0294a3974fe44421
Full name: 330740a91.exe

Made a copy itself to: %APPDATA%\Roaming\WIN-S0MT3UJUS2O\splwow64.exe
Hash of file copied: 463f7191363d0391add327c1270d7fe6

Created file: C:\ProgramData\bett2f00\hemxccape.exe
File hash: 9cf7d079713fdf715131e16b144d3f52

Created file: C:\ProgramData\msitygyd.exe
File hash: 2983d957d4cdd9293682cfaf21147d07

Created file: %TEMP%\7403542.exe
File hash: 72380a9fcf7486bb731606d4f4c13f27

Created file: %TEMP%\7395367.exe
File hash: f220f0a48885bafc29b31fb7228cc4bb

USB drive infection:

Created file: c1fa3e4ee1e2e5b088bc657b0b5a3b8e
Full path and name: [USB_DRIVE]\autorun.inf
File contents:

```
[autorun]
OPEN=WinSystemKB001.exe
action=Run
```

Created file: 463f7191363d0391add327c1270d7fe6
Full path and name: [USB_DRIVE]\WinSystemKB001.exe
Note: *This is a copy of original file executed.*

Registry entrenchment:

Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run
Value Name: A38973873873
Value Data: C:\ProgramData\bett2f00\hemxccape.exe

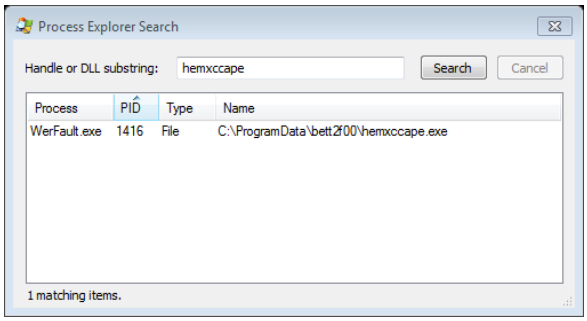
Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run
Value Name: splwow64.exe
Value Data: %APPDATA%\Roaming\WIN-S0MT3UJUS2O\splwow64.exe

Key: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
Value Name: 172157644

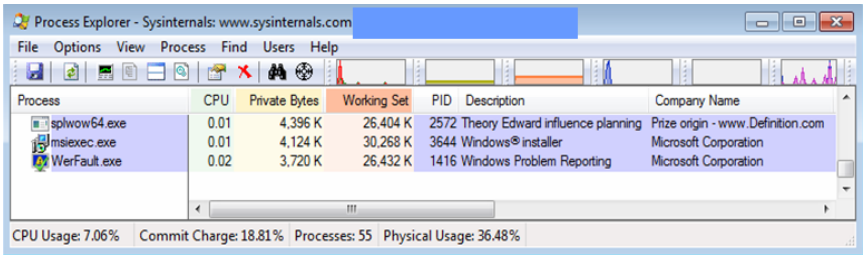
Value Data: C:\ProgramData\msitygyd.exe

Process Injection: C:\Windows\SysWOW64\WerFault.exe

Screenshot showing a handle of the malware in the “WerFault.exe” process:



Screenshot of related processes running in the victim system:



- **Andromeda Bot**
  MD5: 13475d0fdba8dc7a648b57b10e8296d5

  This file was observed hosted in the following servers:

  1. 117.21.191[.]47/and40a37.exe (China)
  2. 54.68.121[.]73/and40a37.exe (US)

  File information:

```
File Name:  and40a37.exe
File Size:  122368 bytes
MD5:        13475d0fdba8dc7a648b57b10e8296d5
SHA1:       feed5337c0a3b1fd55c78a976fbd5388512a22e1
PE Time:    0x54636BD2 [Wed Nov 12 14:16:50 2014 UTC]
PEID Sig:   Microsoft Visual C++ 8
Sections (4):
  Name      Entropy  MD5
  .text     6.42     c93f36300bb882b4671b7ef0a8bd4fba
  .rdata    5.43     55af9f1d8e50e49fdf10742179486281
```

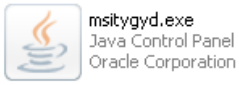
```
.data      5.32      1b24669aa9245cef2358a9d76dab97be
.rsrc      6.94      4f0f11c52935735aa0e65f04b95ed208
```

The malware appears to implement anti-reversing techniques preventing it from properly executing inside a VME. In a bare-metal system, the malware worked properly. This malware is believed to be a variant from the 'Andromeda Bot' malware family.

When the file was executed in a Windows 7 system, the following activity was observed:

Domain: a2kiaymoster14902[.]com
Resolved IP: **121.14.212[.]248 (China)**
POST request: /bla02/gate.php

Made a copy itself to: C:\ProgramData\msitygyd.exe
Hash of file copied: 13475d0fdba8dc7a648b57b10e8296d5



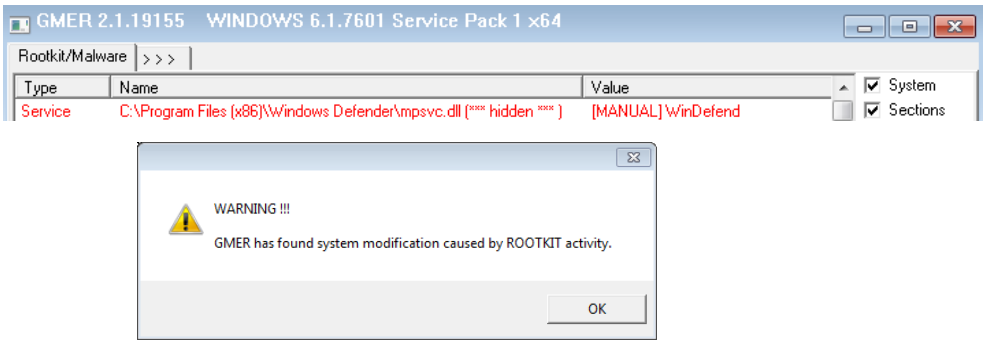
Registry entrenchment:

Key: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\
Value name: 172157644
Value data: C:\ProgramData\msitygyd.exe

Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
Value name: 172157644
Value data: C:\ProgramData\msitygyd.exe

Process Injection: C:\Windows\SysWOW64\msiexec.exe

The malware appears to have rootkit functionality. The hidden "WinDefend" service points to the following DLL: "C:\Program Files (x86)\Windows Defender**mpsvc.dll**". The system was found to have a valid "**mpsvc.dll**" file under the "C:\Program Files\Windows Defender\" directory. The following screenshot show GMER detecting the hidden service:



The following is a summary of all the domains and IPs observed during the analysis of the selected malware:

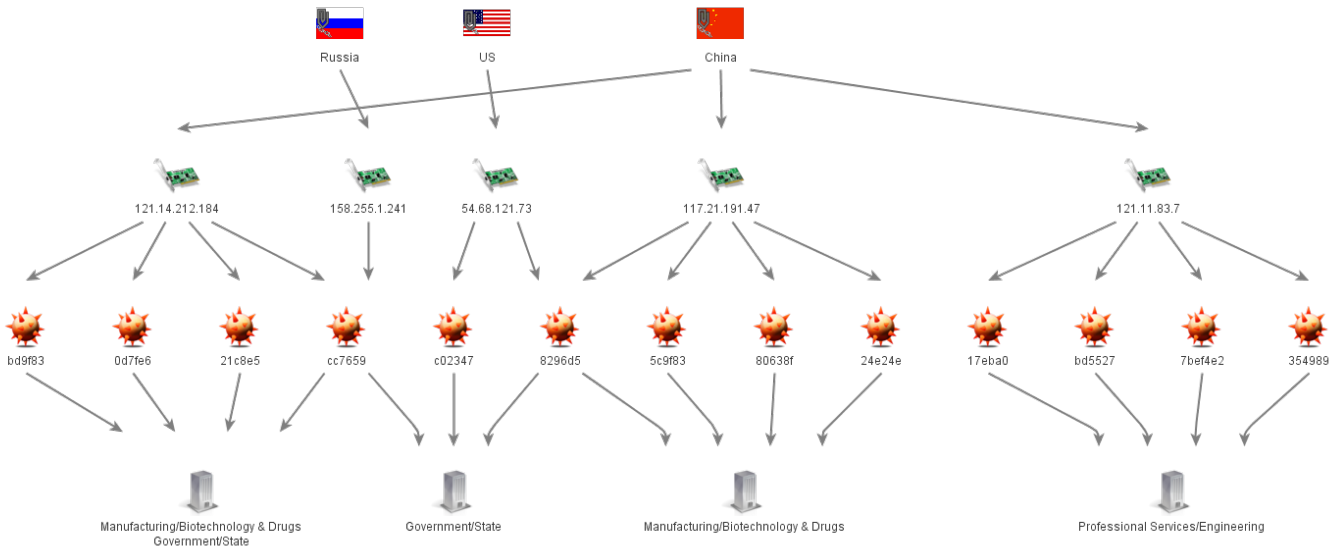
- a2kiaymoster14902[.]com - **121.14.212[.]248** (China)

- **54.69.90[.]62**/and40a90.exe (US)
- b.9thegamejuststarted14k9[.]com - **116.255.202[.]74** (China)
- **121.14.212[.]184**/ng40a54.exe / **121.14.212[.]184**/and40a54.exe (China)
- nutqlfkq123a10[.]com - **121.61.118[.]140** (China)

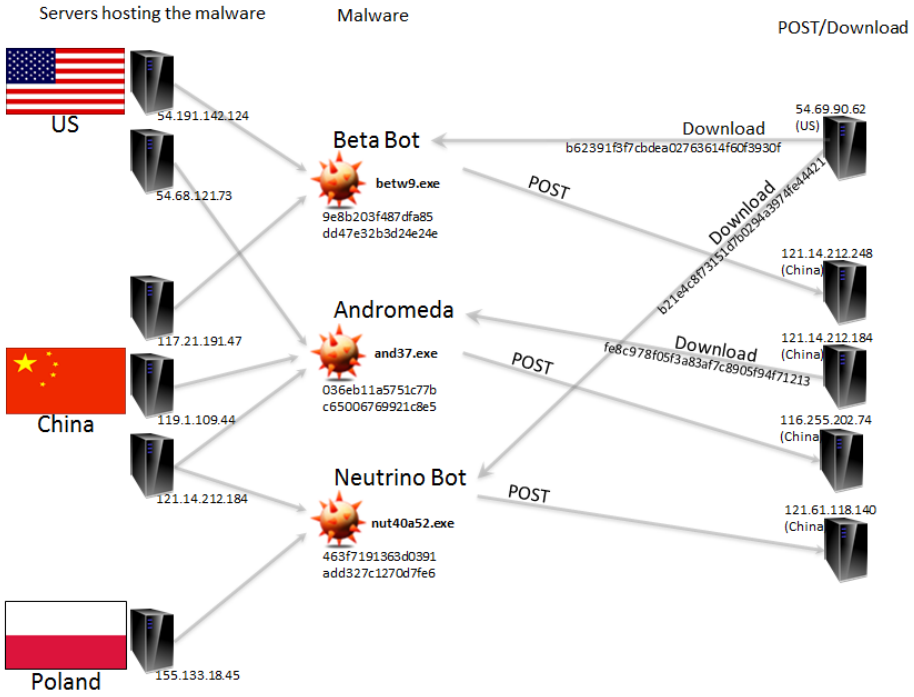
For information about hashes related to this activity, please look at the spreadsheet enclosed with this report which contains relationships between servers and hashes.

Further Analysis And Correlation

The following diagram illustrates the relationship between some of the malicious servers, malware hosted/distributed, and vertical markets:



The following diagram is based on the analysis/execution of some of the malware hosted and distributed by the malicious servers. It illustrates the relationship between some of the malicious servers, locations, malware hosted/distributed, and malicious servers to which the malware beacons to with POST requests and to download additional malware:



The Fidelis Take

This paper highlights campaigns that has compromised systems at significant enterprises worldwide, utilizing various bot malware. We are publishing these indicators so others in the security research community can monitor for this activity and potentially correlate against other campaigns and tools that are being investigated.

General Dynamics Fidelis' advanced threat defense product, Fidelis XPS™, detects all of the activity documented in this paper. Further, we will continue to follow this specific activity and actively monitor the ever-evolving threat landscape for the latest threats to our customers' security.

References

1. Neutrino Bot (aka MS:Win32/Kasidet), June 2014: http://malware.dontneedcoffee.com/2014/06/neutrino-bot-aka-kasidet.html

2. Renting a Zombie Farm: Botnets and the Hacker Economy, August 2014: http://www.symantec.com/connect/blogs/renting-zombie-farm-botnets-and-hacker-economy

3. DorkBot, a Twin Botnet of NgrBot, August 2014: http://blog.fortinet.com/post/dorkbot-a-twin-botnet-of-ngrbot

4. Big Box LatAm Hack (1st part - Betabot), January 2014: http://securelist.com/blog/research/58213/big-box-latam-hack-1st-part-betabot/

5. A Good Look at the Andromeda Botnet, April 2014: https://blog.fortinet.com/post/a-good-look-at-the-andromeda-botnet

6. CVE-2013-2729 and Andromeda 2.9 - A Massive HSBC themed email campaign, June 2014: http://stopmalvertising.com/spam-scams/cve-2013-2729-and-andromeda-2.9-a-massive-hsbc-themed-email-campaign/andromeda-botnet.html

7. Beta Bot – A Code Review, November 2013: http://www.arbornetworks.com/asert/2013/11/beta-bot-a-code-review/

8. Athena, A DDoS Malware Odyssey, Nov 2013: http://www.arbornetworks.com/asert/2013/11/athena-a-ddos-malware-odyssey/

9. Andromeda Botnet Gets an Update, July 2013: http://blog.trendmicro.com/trendlabs-security-intelligence/andromeda-botnet-gets-an-update/

10. New Commercial Trojan #INTH3WILD: Meet Beta Bot, May 2013: https://blogs.rsa.com/new-commercial-trojan-inth3wild-meet-beta-bot/

11. A new bot on the market: Beta Bot, May 2013: https://blog.gdatasoftware.com/blog/article/a-new-bot-on-the-market-beta-bot.html

12. Andromeda Botnet Resurfaces, March 2013: http://blog.trendmicro.com/trendlabs-security-intelligence/andromeda-botnet-resurfaces/

13. Fooled by Andromeda, March 2013: http://www.0xebfe.net/blog/2013/03/30/fooled-by-andromeda/

14. Botnets Die Hard - Owned and Operated – Defcon 20: July 2012: https://www.defcon.org/images/defcon-20/dc-20-presentations/Sood-Enbody/DEFCON-20-Sood-Enbody-Botnets-Die-Hard.PDF.pdf

15. A Chat With NGR Bot, June 2012: http://resources.infosecinstitute.com/ngr-rootkit/

16. Analysis of ngrBot, August 2011: http://stopmalvertising.com/rootkits/analysis-of-ngrbot.html