Cyber FLASH ALERT

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

15 October 2014

Alert Number
A-000042-MW

There is no additional information available on this topic at this time.

Please contact the **FBI CYWATCH** with any questions related to this FLASH Report.

Email:
cywatch@ic.fbi.gov
Phone:
1-855-292-3937

TLP GREEN – The information in this product is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share this information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

The following information was obtained through FBI investigations and is provided in accordance with the FBI's mission and policies to prevent and protect against federal crimes and threats to the national security.

The FBI is providing the following information with **HIGH confidence:**

SUMMARY: The FBI obtained information regarding a group of Chinese Government affiliated cyber actors who routinely steal high value information from US commercial and government networks through cyber espionage. These state-sponsored hackers are exceedingly stealthy and agile by comparison with the People's Liberation Army Unit 61398 ("APT1") whose activity was publicly disclosed and attributed by security researchers in February 2013. This Chinese Government affiliated group previously documented by private sector reports by the names of Operation Deputy Dog, Snowman, Ephemeral Hydra, APT17, the Bit9 and Google security alerts and parts of Hidden Lynx, has heavily targeted the high tech information technology industry including microchip, digital storage and networking equipment manufacturers, as well as defense contractors in multiple countries and multinational corporations. These actors have deployed at least four zero-day exploits in the attacks which compromised legitimate websites to deliver malicious payloads. Any activity related to this group detected on a network should be considered an indication of a compromise requiring extensive mitigation and contact with law enforcement.

The following information was obtained through FBI investigations and is provided in accordance with the FBI's mission and policies to prevent and protect against federal crimes and threats to the national security.

Cyber FLASH ALERT

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

The FBI is providing the following information with **HIGH confidence:**

TECHINICAL DETAILS:

This group uses some custom tools that should be immediately flagged if detected, reported to FBI CYWATCH, and given highest priority for enhanced mitigation. The presence of such tools is typically part of a comprehensive, multifaceted effort to maintain persistent network access and exfiltrate data. The custom tools used by this group are as follows:

HIKIT

A first generation version of HiKit uses rootkit functionality to sit between the network interface card and the operating system enabling the malware to sniff all traffic to/from the compromised host. The rootkit driver spawns processes and executes arbitrary commands. Also, the capability to chain multiple HiKit compromised hosts, enables the actors to use multi-homed hosts located within the DMZ to channel traffic from internal hosts to the Internet using the DMZ hosts. Therefore, organizations should also monitor internal traffic to DMZ hosts for indicators of compromise.

FEXEL-DEPUTY DOG

FBI analysis has indicated that the FEXEL Trojan, used during the Deputy Dog campaign identified in open source reporting, is generally packaged as an x86. A *FEXEL* beacon contains HTTP Header with the name *agtid* whose value is a four byte pseudo random number generated using the Windows *CryptGenRandom* API. The malware generates another four byte pseudorandom number using the same API and prepends it to the body of the HTTP request. The pseudorandom numbers and payload are delimited by the string *08x.* The payload is encrypted using &'$%"# !./,-*+() as a static RC4 Key and then Base64 encoded.

This group also acquires legitimate credentials and uses commonly available tools as part of their effort to maintain persistent network access. Mitigation efforts should also focus on identifying such access and removing it. FBI has identified the following specific, but not wholly exclusive tools, previously used by this group:

- China Chopper lightweight webshell
- GhOst
- 9002
- Poison Ivy
- Derusbi

The following information was obtained through FBI investigations and is provided in accordance with the FBI's mission and policies to prevent and protect against federal crimes and threats to the national security.

- Sogu/PlugX
- Fexel/Deputy Dog
- Zox/ZoxPNG
- ZXShell

RECOMMENDED STEPS FOR INITIAL MITIGATION

The FBI and NSA recommend the following mitigation measures be taken within the first 72 hours of detection:

Prepare Your Environment for Incident Response

- Establish Out-of-Band Communications methods for dissemination of intrusion response plans and activities, inform NOCs/CERTs according to institutional policy and SOPs
- Maintain and actively monitor centralized host and network logging solutions after ensuring that all devices have logging enabled and their logs are being aggregated to those centralized solutions
- Disable all remote (including RDP & VPN) access until a password change has been completed
- Implement full SSL/TLS inspection capability (on perimeter and proxy devices)
- Monitor accounts and devices determined to be part of the compromise to prevent reacquisition attempts

Implement core mitigations to prevent re-exploitation (within 72 hours)

Implement a network-wide password reset (preferably with local host access only, no remote changes allowed) to include:

- All domain accounts (especially high-privileged administrators)
- Local Accounts
- Machine and System Accounts

Patch all systems for critical vulnerabilities:

A patch management process that regularly patches vulnerable software remains a critical component in raising the difficulty of intrusions for cyber operators. While a few adversaries use zero-day exploits to target victims, many adversaries still target known vulnerabilities for which patches have been released, capitalizing on slow patch processes and risk decisions by network owners not to patch certain vulnerabilities or systems. A few of these more widely targeted vulnerabilities are: CVE-2014-0322, CVE-

2013-3893 and 2012-0158. While watching for infections from the malware families detailed above, we also recommend ensuring that you are patched against older vulnerabilities commonly exploited by cyber operators, such as CVE-2012-0158.

After initial response activities, deploy and correctly configure Microsoft's Enhanced Mitigation Experience Toolkit (EMET). EMET employs several mitigations techniques to combat memory corruption techniques. It is recommended that all hosts and servers on the network implement EMET, but for recommendations on the best methodology to employ when deploying EMET, please see NSA/IAD's Anti-Exploitation Slicksheet - http://www.nsa.gov/ia/ files/factsheets/l43V Slick Sheets/Slicksheet AntiExploitationFeatures Web.pdf

Implement long-term mitigations to further harden systems

Implement Pass-the-Hash mitigations. For more information, please see the NSA/IAD Publication Reducing the Effectiveness of Pass-the-Hash at - http://www.nsa.gov/ia/ files/app/Reducing the Effectiveness of Pass-the-Hash.pdf

Baseline File Systems and Accounts in preparation for Whitelisting implementation. Consider using a Secure Host Baseline. See NSA/IAD's guidance at - http://www.nsa.gov/ia/ files/factsheets/l43V Slick Sheets/Slicksheet SecureHostBaseline Web.pdf

Deploy, configure and monitor Application Whitelisting. For detailed guidance, please see NSA/IAD's Application Whitelisting Slicksheet at - http://www.nsa.Rov/ia/ files/factsheets/l43V Slick Sheets/Slicksheet ApplicationWhitelisting Standard.pdf

Please report any compromise believed to be attributable to this group of actors to the calling or emailing FBI CYWATCH. Email: **cywatch@ic.fbi.gov** Phone: **1-855-292-3937**

APPENDIX A -TECHNICAL INDICATORS

HIKIT A:

HiKit A has the following characteristics:

- The HiKit A configuration file is named to match its malicious DLL or EXE. Therefore, a malicious EXE named *netddesrvs.exe* will have configuration file named *netddesrvs.conf.* FBI has observed numerous DLL and EXE names used. The configuration files, which are generally 456 bytes in size, contain command and control (C2) information which is obfuscated using a 4-byte XOR key. The key is the first four bytes of the file which can be viewed using a hex editor.

- The HiKit variants that FBI has observed were located in the following folders on compromised hosts:

  C: *Windows\certen vsrv. Exe*
  C:\Windows\System32\netddesrvs.exe
  C: \ Windows \System32 \ wbem\FVEAPI.dll
  C: \ Windows\System32 \ oci. dll

***NOTE:** The presence of 'oci.dll' should only be considered on indicator provided that Oracle Database products are not installed on the system.*

It should be noted that several HiKit samples were discovered with ".conf" files which contained raw C2 IP addresses as opposed to C2 DNS names.

Open source reporting indicates that HiKit A ensures persistence by a chained DLL hijacking attack using the legitimate (signed code) Microsoft Distributed Transaction Coordinator. The legitimate program *(msdtc.exe)* imports *msdtctm.dll* which inturn loads *mtxoci.dU,* a library that supports the Microsoft ODBC Driver for Oracle. This library in turn loads *oci.dll which* can either be a legitimate Oracle library or a HiKit A DLL.

If your organization discovers compromised hosts through network monitoring (either for HiKit DNS resolutions, known HiKit IP addresses or with the below SNORT rule), searching for 456 byte files with extension ".conf" is highly suggested to locate additional infected hosts.

HIKIT A - RC4 ENCRYPTED:

FBI has observed another subvariant of HiKit A which uses a loader to decrypt and execute the HiKit backdoor on compromised hosts. This HiKit A subvariant has been observed as *ACWConCA.inf* coupled with loader file named *srv.dll.* The execution of the loaders depends on the extension of the backdoor as well as one of two conditions below:

- If the backdoor file extension is .dll, then the .dll file must be in the same directory as the *srv.dll* file for a successful loading.
- If the backdoor file extension is .inf, then the .inf file must be in the C:\windows\inf directory for a successful loading. The location of the srv.dll file in this case does not matter.

If the backdoor and the *srv.dll* file are in the appropriate location, the *srv.dll* file will decrypt the backdoor file using the RC4 key 'hijkqt' and load the backdoor into memory. After the HiKit backdoor is decrypted and loaded into memory, it has similar functionality to other indentified HiKit A variants.

HIKIT B:

The HiKit B variants were observed with configuration files (624 bytes in size) named as a random 8 alphanumeric characters (e.g. "2'66C5F4B"). The configuration files contain command and control (C2) information and are obfuscated using a 4-byte XOR key. However, unlike HiKit A, the XOR key is not located in the first four bytes of the file. The 4-byte XOR key can be identified by using a hex editor to locate sections of the file which contain repeating 4-byte sequences. The location of the configuration file also depends on the host's operating system.

In Windows Vista and above, the file is located in:

C:\ProgramData\Microsoft Corporation\{D2423620-51A0-llD2-9CAF-0060B0EC3D39}\

In Windows XP, the file is located in:

C:\Documents and Settings\All Users\Application Data\Microsoft Corporation\{D2423620-51A0-llD2-9CAF-0060B0EC3D39}\

The HiKit variants observed were found in the following location:
C:\WINDOWS\system32\FontCache.exe

HIKIT A RC4 ENCRYPTED IOCs:

Initial triage of this malware provided the following information:

Filename: srv.dll
Size (bytes): 71167
MD5 Hash: d2c06fa38c626a6cbe48171e69336a02
File PE Compile Time: 2014-07-08 11:22:12
File Import Hash: CA0873C243F99959507A25AF645824EC (74 imports)
Architecture Type: 32 bit
Packer: none
This is a HiKit loader. It decrypts and executes ACWConCA.dll.

Filename: ACWConCa.dll
-Pre-decryption-
Size (bytes): 182335
MD5 Hash: abc63alb923643659acbd319224fl96e

-Post-decryption-
Size (bytes): 181271
MD5 Hash:70E87B2898333E11344B16A72183F8E9
File PE Compile Time: 2013-09-19 10:12:10

File Import Hash: 9040A3EBC41AF9D148D43892275574F1 (58 imports)
Architecture Type: 32 bit
Packer: none

Fexel/Deputy Dog Snort rule:

Alert tcp any any -> any any (content:"agtid="; content:"08x"; msg:"FEXEL/Deputy Malware";)

REPORT REFERENCES:

Bit9, Bit9 Security Incident Update, https://blog.bit9.com/2013/02/25/bit9-securitv-incident-update/

FireEye, Operation DeputyDog, http://www.fireeye.com/blog/technical/cyber-exploits/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html

FireEye, Operation Ephemeral Hydra, http://www.fireeye.com/blog/technical/cyber-exploits/2013/ll/operation-ephemeral-hydra-ie-zero-day-linked-to-deputydog-uses-diskless-method.html

FireEye, Operation Snowman, http://www.fireeye.com/blog/technical/cyber-exploits/2014/02/operation-snowman-deputydog-actor-compromises-us-veterans-of-foreign-wars-website.html

Google, Ensuring your information is safe online, http://googleblog.blogspot.com/2011/06/ensuring-your-information-is safe.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+blogspot%2FMKuf+%280fficial+Google+Blog%29&utm_content=Google+Feedfetcher

Symantec, Hidden Lynx, https://www.svmantec.com/content/en/us/enterprise/media/securitv response/whitepapers/ hidden lynx.pdf