FBI FLASH

FBI LIAISON ALERT SYSTEM
#A-000049-MW

The following information was obtained through FBI investigation and is provided in conjunction with the FBI's statutory requirement to conduct victim notification as outlined in **42 USC § 10607**.

This FLASH has been released 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.

Summary

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

The FBI has obtained information regarding a group of cyber actors who have compromised and stolen sensitive business information and Personally Identifiable Information (PII) from US commercial and government networks through cyber espionage. Analysis of malware samples indicate a singnificant amount of the computer network exploitation activities emanated from infrastructure located within China. The tools used in the attack were referenced in open source reports on Deep Panda. This group has previously used Adobe Flash zero-day exploits in order to gain initial access to victim networks. Information obtained from victims indicates that PII was a priority target. The FBI notes that stolen PII has been used in other instances to target or otherwise facilitate various malicious activities such as financial fraud though the FBI is not aware of such activity by this group. 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.

TECHNICAL DETAILS

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

This group uses a wide variety of tools including generic hacking utilities in order to gain access, establish persistent network access, and move laterally through the victim network. The presence of such tools should be immediately flagged if detected, reported to FBI CYWATCH, and given priority for enhanced mitigation. The tools used by this group are as follows:

Infoadmin (Trojan.Kakfum)

Infoadmin is a Remote Administration Tool (RAT) that includes a dropper and a malicious payload in the form of Dynamic Link Libraries (DLLs), which initiate a number of processes to give the attacker remote access to the infected host. During installation, Infoadmin will attempt to establish persistent presence by direct access through API calls. If the installation in this method fails, it will fall back to a direct write to the victim system's Windows Registry.

Infoadmin has been observed to conduct network activity using a custom protocol over TCP port 443 to the following malicious domains:

- images.googlewebcache.com
- smtp.outlookssl.com

The dropper binary has in several instances contained an icon that resembles the Google Chrome logo. In some samples, the command and control beacon is encrypted using an XOR/ADD loop which utilizes a static key of 0x1C.

This group also utilizes variants of other generic RAT utilities that utilize a dropper file that evaluates the victim system architecture (32bit/64bit) to determine which DLL files to drop in the system directory. These then inject into legitimate system process and have been observed to conduct network activity using http protocol over TCP port 80.

Additional Tools

This group also acquires legitimate credentials and uses commonly available hacking tools as part of their effort to maintain persistent network access, obtain additional credentials, conduct lateral network movement, and exfiltrate files. 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:

- Mimikatz
- ScanLine
- HUC Packet Transmit tool (HTran)
- PwDump
- gsecdump

FBI FLASH

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.

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 - https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_AntiExploitationFeatures_Web.pdf

FBI FLASH

Implement Data-At-Rest (DAR) Protections.

- The goal for DAR protections is to prevent an attacker from compromising sensitive data when the End User Device (EUD) is powered off or unauthenticated.
- The use of multiple encryption layers that meet IAD and CNSSP-15 guidance, implemented with components meeting the Commercial Solution for Classified (CSfC) vendor diversity requirements, reduces the likelihood that a single vulnerability or failure can be exploited to compromise EUDs, move laterally through a network, and access sensitive data.
- Receiving and validating updates or code patches for these components only through direct physical administration or an NSA approved Data in Transit (DIT) solution mitigates the threat of malicious attempts to push unverified updates or code updates.
- Procure products that have been validated through NIAP's DAR Protection Profiles (PPs) and utilize the DAR Capability Package (CP) that provides configurations allowing customers to independently implement secure solutions using layered Commercial Off-the-Shelf (COTS) products. The CP is vendor-agnostic and provides high-level security and configuration guidance for customers and/or Solution Integrators.

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 https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_SecureHostBaseline_Print.pdf

Deploy, configure and monitor Application Whitelisting. For detailed guidance, please see NSA/IAD's Application Whitelisting Slicksheet at – https://www.nsa.gov/ia/_files/factsheets/i43v_slick_sheets/slicksheet_applicationwhitelisting_standard.pdf

POINT OF CONTACT

- In furtherance of public-private partnerships, the FBI routinely advises private industry of various cyber threat indicators observed during the course of our investigations. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.
- The FBI encourages recipients who identify the use of tool(s) or techniques discussed in this document to report information to their local FBI field office or the FBI's 24/7 Cyber Watch. Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at 855-292-3937 or by e-mail at cywatch@ic.fbi.gov.
- Press inquiries should be directed to the FBI's National Press Office at npo@ic.fbi.gov or 202-324-3691.

APPENDIX A – TECHNICAL INDICATORS

INFOADMIN (TROJAN.KAKFUM):

Filename: sqlsrv32.dll
Size (bytes): 126976
MD5 Hash: 7BC8A2EF08F51CF6EEB777B261DA3367
File PE Compile Time: 2014-08-11 17:38:33
File Import Hash: 814AD3F8CF39C672A612FF1264720025
Architecture Type: 32 bit
Packer: none
This is a dropper.

Filename: sqlsrv32.dll
Size (bytes): 126976
MD5 Hash: EF498EA09BF51B002FC7EB3DFD0D19D3
File PE Compile Time: 2014-08-11 17:38:33
File Import Hash: 814AD3F8CF39C672A612FF1264720025
Architecture Type: 32 bit
Packer: none
This is a dropper.

MIMIKATZ:
Description:
Tool used to dump password hashes and clear text credentials from memory.

Notable strings:
[*] FullPath : %s
[-] Err In_AjustPriv: %s %d
[-] Err OpenProcess: %d
[-] Err hModule : %s %d
[-] Err Virtualxxx: %d
[-] Err Writexxx: %d
[-] Err CreatexxxThread: %d
[-] Err Waitxxx: %d
[-] Ok ThreadId: %u
Ret:%s Err:%d
Ret:%s Err:%d pid: %s:%d %s
Usage: xxx.exe dllpath [get/exit]

SCANLINE:

Description:
ScanLine is a command-line port scanner for all Windows platforms.

File: sl.txt

Attributes (UPX Packed):
File Size: 20480 bytes
MD5: 3a97d9b6f17754dcd38ca7fc89caab04
SHA1: ffb1d8ea3039d3d5eb7196d27f5450cac0ea4f34
SHA256: eaef901b31b5835035b75302f94fee27288ce46971c6db6221ecbea9ba7ff9d0
PE Time: 0x3DB03EE0 [Fri Oct 18 17:03:28 2002 UTC]

Attributes (Unpacked):
File Size: 34304 bytes
MD5: 02fc4e3a7998e0213fa5e768239bd0b0
SHA1: 52e661f201d6e26085cb97b27c8eeca52861d2ec
SHA256: d2383b921f341c19b935b0e8be047eb82c59d90408a3ac2bd7b8281d41177539

HUC PACKET TRANSMIT TOOL (HTran):

Description:
Packet Transmit command line tool which allows a user to redirect or transmit network communications from a listening port on a local machine to a remote port.

File: ht.log

Attributes:
File Size: 15872 bytes
MD5: f34914dd1faabfc94a8695e7229d0192
SHA1: 38e21f0b87b3052b536408fdf59185f8b3d210b9
SHA256: b54ab14a7ad0460c7ac6416a9ad01e7015d32573571114b569f4769a2eb12e70
PE Time: 0x52945D64 [Tue Nov 26 08:35:48 2013 UTC]

Usage Statement:
[Usage of Packet Transmit:]
ht.log -<listen|tran|slave> <option> [-log logfile]
[option:]
-listen <ConnectPort> <TransmitPort>
-tran <ConnectPort> <TransmitHost> <TransmitPort>
-slave <ConnectHost> <ConnectPort> <TransmitHost> <TransmitPort>

PWDUMP:

Description:
Command line tool version of **PwDump.exe** which takes either a "-c <target>" or "-d <target>" argument to dump password hash / user account information. The embedded PE files are used to conduct this activity dependent upon whether the compromised system is 32-bit or 64-bit.

File: lot1.tmp

Attributes:
File Size: 400384 bytes
MD5: 3d16542d4ee5c8f77e6c0281d283c7bc
SHA1: 5d201a0fb0f4a96cefc5f73effb61acff9c818e1
SHA256: 07af1c5208985bd00ef746391ce426a0ebf0949ab7f0f638f3f1bde50c5e97a9
PE Time: 0x512EF9E0 [Thu Feb 28 06:32:00 2013 UTC]

GSECDUMP:

Description:
gsecdump v2.0b5, which is a command line password hash dumping tool.

Usage Statement:
USAGE
gsecdump [OPTIONS]
OPTIONS
-h / --help
Show this text
-a / --dump_all
Dump all secrets
-s / --dump_hashes
Dump hashes from SAM/AD
-l / --dump_lsa
Dump LSA secrets
-u / --dump_usedhashes
Dump hashes from active logon sessions
-w / --dump_wireless
Dump Microsoft wireless connections
-S / --system
Force elevation to SYSTEM
DESCRIPTION
Extract security related information from Windows 2000/XP/2003/Vista/7/2008.
Both x86 and amd64 are supported.