FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

05 June 2015

Alert Number

A-000061-MW

Please contact the FBI with any questions related to this FLASH Report at either your local **Cyber Task Force** or **FBI CYWATCH**.

Email:
cywatch@ic.fbi.gov

Phone:
1-855-292-3937

Local Field Offices:
www.fbi.gov/contact-us/field

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.

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 cyber actors who have compromised and stolen sensitive business information and Personally Identifiable Information (PII). 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 these groups. Any activity related to these groups 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**:

Groups responsible for these activities have been observed across a variety of intrusions leveraging a diverse selection of tools and techniques to attempt to gain initial access to a victim including using credentials acquired during previous intrusions. These groups have also been observed compromising using the technique of DNS hijacking facilitated through the compromise of DNS registrars.

Federal Bureau of Investigation, Cyber Division

FLASH NOTIFICATION

Following such an exploit, such groups have been observed recently using custom Remote Access Tools (RAT).

Sakula- A RAT that has the capabilities to launch remote command shells, enumerate processes, download files, and beacon to Command and Control (C2) domains. Sakula attempts to send a two-beacon set over TCP port 80 to a configured domain. If the domain is unavailable, it will attempt to connect to a secondary domain over TCP port 80 and 443 using HTTP.

Specific Sakula MD5 hash values are attached in the accompanying Excel spreadsheet.

Beaconing

```
POST /script.asp?imageid=ivpgvz2085205250&type=0&resid=93863828&nmsg=up HTTP/1.1
Accept: */*
User-Agent: iexplorer
Host: [varies]
Content-Length: 173
Cache-Control: no-cache

GET /photo/ivpgvz2085205250.jpg?resid=93864218 HTTP/1.1
User-Agent: iexplorer
Host: [varies]
Cache-Control: no-cache
```

The following are example POST and GET requests to the secondary C2 domain

```
GET /newimage.asp?imageid=
POST /view.asp?cstring=
POST /view.asp?cstring=%s&tom=0&id=
POST /script.asp?imageid=
GET /photo/%s.jpg?id=%d
POST /viewpre.asp?cstring=
User-Agent: HttpDump 1.1

POST /script.asp?imageid=ivpgvz2085205250&type=0&resid=100391156&nmsg=up HTTP/1.1
Accept: */*
User-Agent: iexplorer
Host: [varies]
Content-Length: 173
Cache-Control: no-cache

GET /photo/ivpgvz2085205250.jpg?resid=100391156 HTTP/1.1
User-Agent: iexplorer
Host: [varies]
```

Federal Bureau of Investigation, Cyber Division

FLASH NOTIFICATION

FF RAT- a RAT that has the capabilities to download Trojan DLL files to memory and beacon back to C2 domains and was named based on the unique string "FF-RAT USER" found within the malware. The data sent in the beacon is XOR-encoded using the key 0x27.

Trojan.IsSpace - a RAT that contains multiple files that include a dropper (EWSNH.exe), Trojan (AOFVPMJXVT.exe), privilege escalation tool (SensrSvc2013.exe), and a module used by the tool (SensrSvc2013.dll). This malware is capable of bypassing dyndns categorization by using a proxy through Google AppProxy's hosted on appspot domains.

Filename: EWSNH.exe
MD5: bfdbf09072b58e90aef726c2d1ecf8b7
File Size (bytes): 1990136

Filename: AOFVPMJXVT.exe
MD5: 25631f5ccec8f155a8760b8568ca22c5
File Size (bytes): 63488

Filename: SensrSvc2013.exe
MD5: 38f29e955b76de69c8e97f4491202b8b
File Size (bytes): 197120

Filename: <VARIES>.tmp / SensrSvc2013.dll / CRYPTBASE.dll
MD5: 75416711fc782a3e2a2b54c4b86677bf
File Size (bytes): 42496

Protocol variations in the URI:

SSports.asp?
HostID=
SWeather.asp?
HostID=
&PackNo=
SJobs.asp?HostID=
STravel.asp?HostID=
SGames.asp?
HostID=
SNews.asp?HostID=
STTip.asp

Trojan.BLT- a RAT that is executed from its export *CreateInstance*, the mutex HFRM_ is created and a process instance of cmd.exe is launched to execute the command "ipconfig/all" to collect the victim system's MAC address. Trojan.BLT will test network connectivity by establishing a connection with a legitimate website. This malware is capable of bypassing dyndns categorization by using a proxy through Google AppProxy's hosted on appspot domains.

Trojan.BLT will validate the connection by checking the HTTP header "Service:IIS". Trojan.BLT will then conduct further C2 activity.

Federal Bureau of Investigation, Cyber Division

FLASH NOTIFICATION

Beaconing:

```
POST /fetch.py HTTP/1.1
Accept: */*
Cache-Control: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: snecma-secure.appspot.com
Content-Length: 56
Connection: Close

POST /asp/STTip.asp HTTP/1.1
Accept: */*
Cache-Control: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: facebook.from-pr.com
Content-Length: 11
Connection: Close

GET / HTTP/1.1
User-Agent: Mozilla/5.0 (compatible; MSIE 7.0;Windows NT 5.1)
Host: www.microsoft.com
Cache-Control: no-cache
```

Recommended Mitigations

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

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 inhibit 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

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

1. ***Protect Credentials:*** By implementing the following credential protections, the threat actor's ability to gain highly privileged account access and move throughout a network is severely hampered.
    a. *Implement Least Privilege:* Least privilege is the limiting of rights assigned to each group of accounts on a network to only the rights required for the user, as in a normal user is only granted user level privileges and cannot perform any administrative tasks such as installing software.
    b. *Restrict Local Accounts:* By restricting the usage of local accounts, especially local administer accounts, you are able to reduce the amount of usable credentials found within a network. When utilizing local accounts, passwords and their corresponding hashes are stored on the host and are

more readily available for harvesting by an adversary who seeks to establish persistence. Adversaries are known to use this information to move across the network through Pass the Hash.

c. *Limit lateral movement:* This mitigation reduces the adversary's ability to go from exploiting one machine to taking over the entire network. Host firewall rules, Active Directory structuring, and/or Group Policy settings, can be tailored to stop communications between systems and increase the survivability and defensibility of a network under attack.

d. *Admin Access Segregation:* Once an adversary gains administrator credentials, especially domain administrator credentials, the network becomes wide open to their malicious activity. By decreasing the surface area where admin credentials can be stolen, through restricting where administrators can use their accounts and what they can use their accounts for, the threat actor will have a much harder time fully compromising a network.

e. *Log and Monitor Privileged Admin Account Usage:* Implementing logging and monitoring capabilities on privileged accounts can provide insight to system owners and incident response professionals of account misuse and potential compromise by malicious actors. For instance it may be discovered that a domain admin is logging in at 2200 every night even though that admin is done working for the day and gone from the building. This mitigation would also enable discovery of any privileged admin accounts that were created by the actor for persistence.

2. ***Segregate Networks and Functions:***

   a. *DMZ Isolation:* By ensuring that the DMZ is properly segregated both through physical and logical network architecture and admin/user accounts, a network owner can greatly decrease the external attack surface. Since webservers and corresponding databases usually sit in this location and are also externally accessible, they regularly are the first target during CNO. If these systems are compromised and the DMZ is not configured properly or at all, it could mean the loss of the entire enterprise.

   b. *Network Function Segregation:* A network owner should implement a tiered system when determining the switching within a network. This way the lower security systems, like user workstations or machines with email and internet access, cannot insecurely communicate with higher security systems like domain controllers and other member servers. This can be achieved through multiple methods including VLANs, physical network topologies, and Firewall rule sets. In the same vein, networks need to apply the same segregation principle to the various tiers of accounts within a network, ensuring highly privileged accounts cannot access lower security tiered systems and low privilege accounts cannot access higher security tiered systems.

   c. *Perimeter Filtering:* Perimeter filtering refers to properly implementing network security devices, such as proxies, firewall, web content filters, and IDS/IPS. The intent is to block malicious traffic from reaching a user's machine and provide protection against data exfiltration and command and control.

3. ***Implement Application Whitelisting:*** Application whitelisting is the configuring of host system to only execute a specific, known set of code. Basically, if a program or executable code, such as a piece of malware, is not included in the whitelist it's never allowed to run.

4. ***Install and correctly use EMET:*** One of the frequently used tactics by an adversary is to initially infect a host through spear-phishing and drive-by's/water-holing websites. The best way to counter this initial exploitation is through the implementation of an anti-exploitation tool, such as Microsoft's Enhanced Mitigation Experience Toolkit (EMET). These tools can render useless entire classes of malware and malicious TTP instead of eliminating one piece of malware at a time; an enormous boon to a network's security.

5. ***Use a Standard Baseline:*** Implementing a uniform image with security already baked in and standardized applications affords the incident response team the ability to look at exploited machines and distinguish what is malicious vs. allowed. It also ensures that each machine on network is at least at a certain level of security prior to further customization for a user's needs. Within the DoDIN this can be satisfied through the Unified Master Gold Disk, maintained and distributed through DISA.
6. ***Centralize logging of all events:*** By pulling all of the system logs, such as Windows Event or Error logs, and any logs from security devices, such as SNORT or firewall rule hits, into a centralized location, the network admin and intrusion response team would be able to more efficiently detect and understand the tools, tactics, and procedures of the adversary. Using this information then increases the responder's ability to effectively corner and expel the adversary.
7. ***Data-at-Rest and Data-in-Transit Encryption:*** Implementing encryption for both data at rest and data in transit ensures that what is meant to be kept private stays private, whether it is stored on a disk or moving across a network. It means that exfiltration and espionage attempts can be thwarted since a threat actor cannot access the information.

Additional guidance to follow can be found at the following:

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.