TLP: GREEN

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

23 May 2016

Alert Number

A-000073-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information please contact **FBI CYWATCH immediately**.

Email:

cywatch@ic.fbi.gov

Phone:

1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

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.

(U) 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 publically accessible channels.

Summary

The FBI is providing the following information with HIGH confidence:

The FBI has obtained information regarding a malicious cyber group that has compromised the networks of foreign banks. The actors have exploited vulnerabilities in the internal environments of the banks and initiated unauthorized monetary transfers over an international payment messaging system. In some instances, the actors have been present on victim networks for a significant period of time. Contact law enforcement immediately regarding any activity related to the indicators of compromise (IOCs) in the attached appendix that are associated with this group.

Technical Details

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

The enclosed IOCs have been employed by a cyber group linked to intrusions at foreign banks. Malicious insiders or external attackers have managed to submit international payment messages from financial institutions' back-offices, PCs or workstations connected to their local interface to the international payment messaging system network. The group utilized malware that appears to have been customized for each victim environment. The malware is designed to hide evidence by removing some of the traces of the fraudulent messages. The observed malware samples were designed to securely delete themselves once they completed their tasks, removing evidence of their existence. Additionally, the intruders appear to have performed extensive network reconnaissance using remote access Trojans, keyloggers, screen grabbers, and a variety of legitimate Windows system administration utilities. In addition to these IOCs, the FBI recommends recipient organizations be alert to any changes to directories where international payment messaging system software has been installed.

Indicators of Compromise (IOCs)

Please see Appendix A for a list of known IOCs.

Recommended Mitigations for Institutions with Connections to Payment Messaging Systems

Logically Segregate Your Operating Environment

- Use firewalls to divide your operating environment into enclaves.
- Use access control lists to permit/deny specific traffic from flowing between those enclaves.
- Give special consideration to segregating enclaves holding sensitive information (for example, systems with customer records) from enclaves that require Internet connectivity (for example, email systems)

Isolate Payment Messaging Platforms

- For institutions that access payment messaging platforms through private networks, confirm perimeter security controls prevent Internet hosts from accessing the private network infrastructure.
- For institutions that access payment messaging platforms over the Internet, confirm perimeter security controls prevent Internet hosts *other than payment messaging platform endpoints* from accessing the infrastructure used for payment system access.

Routinely Confirm the Integrity of Secondary Security Controls

- Perform monthly validation of transactional integrity systems, such as printers or secondary storage systems.
- Perform monthly validation of payment messaging activity by performing telephone confirmation of transfer activity.

Routinely Test Operating Protocols

- Confirm staffing plans for non-business, non-critical operating hours.
- Ensure staff members understand payment messaging transfer protocols, along with emergency transfer protocols.

Monitor for Anomalous Behavior as Part of Layered Security

- Develop baseline of expected software, users and logons. Monitor hosts running payment applications for unusual software installations, updates, account changes, or other activities outside of expected behavior.
- Develop baseline of expected transaction participants, amounts, frequency and timing. Monitor and flag anomalous transactions for suspected fraudulent activity.

Recommended Mitigations for All Alert Recipients

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

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) 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 mitigation 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 Slick sheet - 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 administrator 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. Having different passwords and credentials for user, local administrator, and domain administrator accounts prevents an adversary from reusing a stolen credential from one to gain more access.
    e. *Admin Access Protection:* Using encrypted protocols across the network where credentials especially administrative credentials, are sent in the clear enables an adversary to grab them in transit and reuse them. Be sure to use encrypted protocols (e.g. HTTPS, SSH, RDP, SFTP, etc.) for all management connections where credentials are passed, and disable the use of unencrypted protocols (e.g. Telnet, FTP, HTTP, etc.).
    f. *Ensure Administrative Accounts do not have email accounts or Internet access*.
    g. *Utilize Strong Authentication:* By enforcing multi-factor authentication (e.g., using smart cards), especially for privileged account and remote access (e.g. VPNs), you dramatically reduce when and where stolen credentials can be reused by an adversary. Until then, create, enforce, and maintain strong password policies across the organization. The use of strong password policies must be mandated for all users and is especially critical for administrator accounts and service accounts. Passwords should be complex and contain a combination of letters, numbers, and special characters, and they should be of a sufficient length (greater than 14 characters); require regular password changes for all administrative

and other privileged account; and prevent the reuse of usernames and passwords across multiple domains and/or multiple systems.

h. *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.

i. *Log and Monitor Use of Administrative Tools:* Non-administrative use of built-in OS administrative tools should be locked down in accordance with applicable guidance and hardening policies. Use of these tools, such as Windows® PowerShell® and Windows Management Instrumentation Command-line (WMIC), should be logged and monitored to help enable early detection of a compromise. Though administration activities take place on a constant basis, certain behaviors, or sets of activities, in concert with others, are suspicious and can lead to a discovery of intrusion. For example, the 'ping' command by itself has legitimate uses. However, the 'ping' command followed by a PowerShell command from one workstation to another is very suspicious.

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

a. *Know Your Network:* Enterprise networks often become unmanageable leading to inefficient administration and ineffective security. In order to have any sort of control over your network, you first need to know what and where everything is and does. Ensure information about your networks is documented and is updated regularly. Create an accurate list of ALL devices and ALL protocols that are running on your network. Identify network enclaves and examine your network trust relationships within and between those enclaves as well as with external networks to determine whether they are really necessary for your organization's mission.

b. *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.

c. *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.

d. *Limit Workstation-to-Workstation Communications:* Pass-the-Hash (PtH) and other forms of legitimate credential reuse are serious vulnerabilities existing in all environments that implement Single Sign-on. PtH allows an attacker to reuse legitimate administrator or user credentials to move from system to system on a network without ever having to crack password. Once an attacker compromises a single host, s/he will typically reuse stolen hashed credentials to spread to other systems on the network, gain access to a privileged user's workstation, grab domain administrator credentials, and subsequently take control of the entire environment. Limiting workstation-to-workstation communication will severely restrict attackers' freedom of movement via techniques such as PtH. In general, limiting the number and type of communication flows between systems also aids in the detection of potentially malicious network activity. Because there are fewer allowed communication paths, abnormal flows become more apparent to attentive network defenders.
e. *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.
f. *Use Web Domain Name System (DNS) Reputation:* Various commercial services offer feeds rating the trustworthiness of web domains. Enterprises can protect their hosts by screening web accesses against such services and redirecting dangerous web requests to a warning page. Inspection can be implemented at either the web proxy or browser level.
g. *Restrict or Prevent Remote Admin Access:* Prior to an intrusion, remote access should be severely restricted and highly monitored. Once an intrusion is detected, all remote administration should be completely disallowed. Not only does this clear up the network traffic coming and going from a network, it also allows the network defenders to determine that the remote administration activities are malicious and better track and block them.

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. ***Implement Host Intrusion Prevention System (HIPS) Rules***: Standard signature-based host defenses are overwhelmed by exploit kits that continually morph attack components. HIPS technology focuses on threat behaviors and can better scale to entire sets of intrusion activities. For an enterprise with a well-configured and managed network, HIPS can be tuned to learn and allow normal network functionality while flagging anomalies characteristic of intrusions.

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, HIPS or firewall rule hits, as a few examples) into a centralized location that protects it from tampering and enables analytics, the network admin and intrusion response team would be able to more efficiently detect and understand the tools, tactics, and procedures of the adversary. This paper does not detail the entirety of logs that could be aggregated, however, specific recommendations of particular logs that should be targeted for aggregation can be obtained via consultation with the network's Computer Network Defense-Service Provider (CND-SP) or with any of the organizations listed in the introduction of this section.

7. ***Take Advantage of Software Improvement***: Apply patches for vulnerabilities as soon as they are released by the vendor. Upgrade as new versions of applications, software and operating systems become available. Delaying or ignoring patches for vulnerabilities considerably increases the chance of systems being exploited, in particular Internet/public facing systems (VPN, web, email servers). Open source research has shown that a working exploit is often available on the same day vulnerabilities are publicly disclosed, making it imperative to patch immediately. Vendors typically perform extensive testing of patches prior to release so misconceptions about negative effects on systems are often overstated. The cost of pre-deployment testing by the enterprise is miniscule compared to the potential costs incurred from a security breach. Application deployment and updating is becoming increasingly automated. Many operating systems and applications provide automatic update features to minimize the human factor.

8. ***Public Services Utilization***: Enterprises are embracing the use of public services such as Cloud Storage and Social Networking Sites (SNS) as they offer capabilities not available with traditional software. These services also introduce a new set of vulnerabilities that must be considered. Open source reporting has shown these services to be an increasingly used vector for both malware delivery and data exfiltration. Establish a comprehensive public services policy and framework. Discover and document all the Cloud and Social Networking Services used and establish a policy that includes IT sanctioned sites permitted and prohibited within the enterprise as well as what is

considered acceptable use. Integrate traffic logs to/from these sites into your centralized logging environment and implement analytics to detect and alert on potentially suspicious or abnormal traffic that could be indicative of a compromise.

9. ***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.

10. ***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.

11. ***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_web.pdf

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

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey

Filename	Size	MD5	SHA1	SHA256
evtdiag.exe	65536	24d76abbc0a10e4c977a28b33c879248	525a8e3ae4e3df8c9c61f2a49e38541d196e9228	4659dadbf5b07c8c3c36ae941f71b631737631bc3fded2fe2af250ceba98959a
evtsys.exe	16384	5d0ffbc8389f27b0649696f0ef5b3cfe	76bab478dcc70f979ce62cd306e9ba50ee84e37e	ae086350239380f56470c19d6a200f7d251c7422c7bc5ce74730ee8bab8e6283
nroff_b.exe	24576	1d0e79feb6d7ed23eb1bf7f257ce4fee	70bf16597e375ad691f2c1efa194dbe7f60e4eeb	5b7c970fee7ebe08d50665f278d47d0e34c04acc19a91838de6a3fc63a8e5630
gpca.dat	33848	f7272bb1374bf3af193ea1d1845b27fd	6207b92842b28a438330a2bf0ee8dcab7ef0a163	b07b37f0246bd436addbe5d702b12485d7bc8a9ef1475b54bff513a18e68fef7

SSDeep	Filetype	PETime	FileType2	Subsystem
525a8e3ae4e3df8c9c61f2a49e38541d196e9228	PE32 executable (console) Intel 80386, for MS Windows	2/5/16 11:46	Win32 EXE	Windows command line
76bab478dcc70f979ce62cd306e9ba50ee84e37e	PE32 executable (GUI) Intel 80386, for MS Windows	2/4/16 13:45	Win32 EXE	Windows GUI
70bf16597e375ad691f2c1efa194dbe7f60e4eeb	PE32 executable (GUI) Intel 80386, for MS Windows	2/5/16 8:55	Win32 EXE	Windows GUI
6207b92842b28a438330a2bf0ee8dcab7ef0a163	data	N/A	N/A	N/A

File Info

```
import "pe"

private rule IsPE
{
  condition:
    uint16(0) == 0x5A4D and
    uint32(uint32(0x3C)) == 0x00004550
}

rule banswift_gpca
{
  meta:
    description = "Look for encrypted magic bytes with known key(s)"
  condition:
     uint32(0) == 0xade4e1f5
}

rule banswift_rc4_key
{
  meta:
    description = "Look for known RC4 key(s)"
  strings:
    $key1 = {4e 38 1f a7 7f 08 cc aa 0d 56 ed ef f9 ed 08 ef}
  condition:
    IsPE and any of ($key*)
}

rule banswift_delbat
{
  meta:
    description = "Look for specific embedded batch file with delete loop."
  strings:
    $delbat = {3A 4C 31 0D 0A 44 45 4C 20 22 25 73 22 0D 0A 50 49 4E 47 20 30 2E 30 2E 30 2E 30 20 3E 20 6E 75 6C 0D 0A 49 46 20 45 58 49 53 54 20 22 25 73 22 20 47 4F 54 4F 20 4C 31 0D 0A 44 45 4C 20 22 25 25 30 22 0D 0A}
  condition:
    IsPE and $delbat
}


rule path_strings
{
```

```
  meta:
    description = "Look for file path strings associated with samples' config and log files."
  strings:
    $s1 = "recas.dat" wide ascii nocase
    $s2 = "gpca.dat" wide ascii nocase
    $s3 = "Users\\%s\\AppData\\Local\\%s" ascii
    $s5 = "Allians" ascii
  condition:
    IsPE and 2 of ($s*)
}

rule transaction_strings
{
  meta:
    description = "Look for strings associated with transactions"
  strings:
    $fin1 = "FIN 900" wide ascii nocase
    $fin2 = "FIN 950" wide ascii nocase
    $ts1 = "debit" wide ascii nocase
    $ts2 = "credit" wide ascii nocase
    $ts3 = "balance" wide ascii nocase
    $ts4 = "closing" wide ascii nocase
    $ts5 = "transaction" wide ascii nocase
    $ts6 = "sender" wide ascii nocase
    $ts7 = "avail" wide ascii nocase
  condition:
    IsPE and (1 of ($fin*) and 3 of ($ts*) )
}

rule custom_rc4_routine
{
  meta:
    description = "Custom RC4 routine."
  strings:
    $rc4_cipher_loop = {8A 98 00 01 00 00 FE C3 8A CB 88 98 00 01 00 00 8A 98 01 01 00 00 81 E1 FF 00 00 00 8D 14 01 8A 0C 01 02 D9 8A CB 88 98 01 01 00 00 81 E1 FF 00 00 00 03 C8 8B F9 8A 0A 8A 1F 88 1A 88 0F 33 D2 33 C9 8A 90 01 01
  condition:
    IsPE and all of ($rc4*)
}

rule renamedelete
```

```
{
  meta:
    description = "Look for specific delete file routines."
  strings:
    $call1 = "strrchr" ascii
    $call2 = "rand" ascii
    $call3 = "MoveFileA" ascii
    $call4 = "CreateFileA" ascii
    $call5 = "SetFilePointer" ascii
    $call6 = "WriteFile" ascii
    $call7 = "FlushFileBuffers" ascii
    $call8 = "GetFileSizeEx" ascii
    $call9 = "CloseHandle" ascii
    $random_filename = {FF ?? 99 B? 1A 00 00 00 F7 ?? 80 ?? 61 88 16 8A 46 01 46 84 C0 75 E9}
    $write_nulls = {8D 54 ?? ?? 53 52 8D 44 ?? ?? 51 50 56 FF 15 ?? ?? ?? ?? 85 C0}
    $rand_data = {FF D3 25 FF 00 00 80 79 07 48 0D 00 FF FF FF 40 88 04 37 8B CE 4E 85 C9 7F E6}
  condition:
    IsPE and all of ($call*) and $random_filename and
      (
        $write_nulls or $rand_data
      )
}
```

Yara

```
2 FF 00 00 00 8A 0C 02 32 CB 88 0E 8B 4C 24 20 46 49 89 4C 24 20 75 8E}
```

Yara

Yara

```
alert tcp any any -> any 80 (msg:"Banswift Beacon"; flow: to_server,established; content: "/al?---"; pcre: "/[CON]/"; detection_filter: track by_src, count 30, seconds 30; metadata: service http; SID: 2016051601)
```

Snort