FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

17 NOV 2016

Alert Number

E-000078-MW

WE NEED YOUR HELP!

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

E-mail:

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.

This FLASH has been released TLP: GREEN: The information in this product is useful for the awareness of all participating organizations within their sector or community, but not via publicly accessible channels.

Advanced Persistent Threat Targets US Public and Private Sector Entities with Spear Phishing Campaign Featuring New Exploits

Summary

Likely Advanced Persistent Threat (APT) cyber actors have targeted US private sector and government networks since August 2016 with spear phishing campaigns, using newly identified exploits contained within lures related to foreign affairs and the recent US presidential election. The FBI analyzed malicious Microsoft Office documents, a zip archive, a first-stage downloader, a second-stage in-memory-only PNG wrapped malware, and a BAT-initiated PowerShell script associated with the campaigns. This FLASH provides rules and signatures to assist in network defense efforts.

Technical Details

FBI analysis indicates exploitation begins with a victim receiving a spear phishing email containing either a malicious Microsoft Office document that will drop and execute the first-stage downloader or a link to a zip archive containing both the first and second stages. Once dropped to disk, the first-stage implant is responsible for downloading and loading the second-stage in-memory-only PNG wrapped malware, at which point the second-stage malware will conduct malicious activities.

The env.bat-initiated PowerShell script appears to be another Remote

Access Tool (RAT) associated with the campaign. It creates a Net.WebClient object and uses the DownloadData() and UploadData() functions for network communication. The WebClient object is setup with GetDefaultProxy() and DefaultCredentials, so it is authenticating-proxy-aware.

In an attempt to blend in with "natural" network communications, the PowerShell script first attempts to connect to http://gmail.com or http://google.com (chosen randomly) and only proceeds if the connection succeeded. It also attempts a request to the callback base URL + /favicon.ico every 12 hours. There are also several sleep statements throughout, which will cause some variance in the periodicity of the network activity.

When a connection to the RAT controller is successful, the returned HTML is searched for IMG tags and parsed if the ALT value is "Send message to contact" and the SRC value contains a comma followed by a base64 string. The base64 string is then extracted, parsed using a custom unpacking method, decrypted, unpacked some more, and eventually passed to an Invoke-Expression call.

This toolset, and these adversaries, are known for using in-memory-only modules, so any network defense measures should include imaging of the device's memory before any shutdown or reboot of the suspected compromised system.

Rules and Signatures

The following rules and signatures are provided for network defense purposes and are also included in an attached STIX file.

YARA RULES:

```
rule MD_VernalDrop_DOC
{
  meta:
    author = "FBI 2be9be918bb8cc2b"
    date = "2016/10/27"
    description = "Suspected malicious macro used in MS Word documents"
    Version = 1
```

```
  strings:
    $t1 = "WScript.Shell"
    $t2 = "Scripting.FileSystemObject"
    $t3 = "Execzy"
    $t4 = "AutoOpen"
    $t5 = "DocumentBeforeClose"
    $t6 = "SMBIOSBIOSVersion"
    $h1 = { 41 74 74 72 69 62 75 74 00 65 20 56 42 5F 4E 61 6D 00 65 }
//Attribut.e VB_Nam.e

  condition:
    all of them
}

rule MD_VernalDrop_XLS
{
  meta:
    author = "FBI 2be9be918bb8cc2b"
    date = "2016/10/27"
    description = "Suspected malicious macro used in MS Excel documents"
    Version = 1
  strings:
    $t1 = "WScript.Shell"
    $t2 = "Scripting.FileSystemObject"
    $t3 = "Execzy"
    $t4 = "WScript.StdOut.Write"
    $t5 = "rundll32.exe"
    $t6 = "Auto_OpenV"
    $h1 = { 41 74 74 72 69 62 75 74 00 65 20 56 42 5F 4E 61 6D 00 65 }
//Attribut.e VB_Nam.e

    condition:
      all of them
}

rule MW_Tadpole
{
  meta:
    author = "FBI 2be9be918bb8cc2b"
    date = "2016/11/14"
```

```
    description = "Suspected downloader"
    Version = 1
  strings:
    $h1 = { 68 74 74 70 0F 85 86 01 00 00 AC 66 AD 66 3D 2F 2F 0F }
    $h2 = { C7 45 ?? 61 64 76 61 C7 45 ?? 70 69 33 32 C7 45 ?? 2E 64 6C 6C }
    $h3 = { 30 10 49 44 41 54 74 }

  condition:
    all of them
}

rule MW_Spikerush
{
  meta:
    author = "FBI 2be9be918bb8cc2b"
    date = "2016/10/27"
    description = "Suspected PNG-wrapped encrypted malicious module"
    Version = 1
  strings:
    $h1 = { 49 44 41 54 08 C9 DC 62 2F 04 89 DD A9 01 B2 A5 C0 22 5C BF 29
28 }
    $h2 = { 49 44 41 54 78 DA ED BD 79 BC 64 65 7D E7 FF FE 3E E7 9C AA BA
6B }

  condition:
    all of them
}
```

SNORT SIGNATURES

```
/* These rules are medium fidelity and have not been thoroughly tested.
Please test in your environment before deploying and provide feedback so
that we may improve the quality if necessary. */

alert tcp any any -> any any (msg:"Potentially malicious Spikerush
encrypted in PNG"; flow:to_client,established; content:"|49 44 41 54 08 C9
DC 62 2F 04 89 DD A9 01 B2 A5 C0 22 5C BF 29 28|"; sid:324000001; rev:1;)
alert tcp any any -> any any (msg:"Potentially malicious Spikerush
encrypted in PNG"; flow:to_client,established; content:"|49 44 41 54 78
DA ED BD 79 BC 64 65 7D E7 FF FE 3E E7 9C AA BA 6B|"; sid:324000002;
```

rev:1;)

/* The following rules may only be useful if SSL-inspection is actively being used in your environment. The connections seen thus far have all been within HTTPS traffic */

alert tcp any any -> any any (msg:"Suspected malware communication in HTML IMG tag's SRC parameter"; flow:to_client,established; content:"<img src=|22|"; content:"|22| alt=|22|Send message to contact|22|"; sid:324000003; rev:1;)
alert tcp any any -> any any (msg:"Suspected malware HTTP Accept header"; flow:to_server,established; content:"text/html,application/xhtml+xml,application/xml|3b|q=0.9,*/*|3b|q=0.8"; sid:324000003; rev:1;)

OTHER SIGNATURES

The Powershell script attempts to read the Registry key "HKEY_CURRENT_USER\Software\Apple Inc\Updater" and key value name "EditFlags." This appears to be a fairly unique value, but we encourage testing in your environment before deploying detection capabilities broadly.

The following User-Agent string was found hardcoded within the PowerShell implant. All communications thus far have been seen over HTTPS, so it may only be signaturable if you use SSL-inspection or a host-based solution for inspecting network communications.

Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)

Recommended Mitigations

Precautionary measures to mitigate these techniques include:

- Prepare an incident response plan to be rapidly implemented in case of a cyber intrusion.
- Patch all systems for critical vulnerabilities, prioritizing timely patching of Internet-connected servers for known vulnerabilities, especially in the products listed above, and software that processes

Internet data, such as web browsers, browser plugins, and document readers.
- Scrutinize links contained in e-mails, and do not open attachments included in unsolicited e-mails.
- Implement application whitelisting to block execution of malware, or at least block execution of files from TEMP directories where most phishing malware attempts to execute from.
- Randomize local administrator passwords to inhibit lateral movement across workstations.
- Upgrade PowerShell to new versions with enhanced logging features and centralize logs to detect usage of commonly used malware-related PowerShell commands.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). 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. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@ic.fbi.gov or (202) 324-3691.

Administrative Note

This product is marked 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. No portion of this product should be released to the media, posted to public-facing Internet Web sites, or transmitted over non-secure, external communications channels.

The FBI is aware of private industry reporting that provides further detail on this activity. These cyber actors also continue to exploit vulnerabilities

associated with Cacti software; see FBI FLASH E-000072-MW, disseminated 11 May 2016, for additional information.

For comments or questions related to the content or dissemination of this product, contact CyWatch.

General information on defending networks can be found at:

- https://www.nsa.gov/ia/_files/factsheets/NSA_Methodology_for_Adversary_Obstruction.pdf
- https://www.nsa.gov/ia/_files/app/spotting_the_adversary_with_windows_event_log_monitoring.pdf
- https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_ControlAdministrativePrivileges_Web.pdf
- https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_ApplicationWhitelisting_Standard.pdf
- https://www.nsa.gov/ia/_files/app/Reducing_the_Effectiveness_of_Pass-the-Hash.pdf

Phishing mitigations:

- https://www.us-cert.gov/ncas/alerts/TA15-213A
- http://www.pcworld.com/article/114629/article.html
- https://www.fireeye.com/current-threats/best-defense-against-spear-phishing-attacks.html

Malicious use of Windows PowerShell:

- https://dl.mandiant.com/EE/library/MIRcon2014/MIRcon_2014_IR_Track_Investigating_Powershell_Attacks.pdf