FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

11 MAY 2016

Alert Number

E-000072-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.

Vulnerabilities and Post Exploitation IOCs for an Advanced Persistent Threat

Summary

Advanced Persistent Threat (APT) cyber actors continue to target sensitive information stored on US commercial and government networks through cyber espionage. The CVEs and post-exploitation tools in this document were utilized in compromises in the last year. In addition to utilizing the exploits identified in this document, the adversary also uses spear-phishing e-mails as a vector to compromise networks. The FBI is making these CVEs, MD5s, and YARA rules available for network defense.

Technical Details

The CVEs below were used by APT actors[1] to compromise networks in the last year. The compromises were to build infrastructure and for exploitation. The FBI recommends patching Internet-connected servers for vulnerabilities in the following products:

Software:	CVE(s):	Notes:
Adobe ColdFusion	CVE-2013-0625; CVE-2013-0632	Affects versions 10 and earlier. The vulnerability allows for the circumvention of authentication controls, allowing the attacker to take control of the server.
Adobe ColdFusion	CVE-2013-0629	Affects version 10 and earlier. The vulnerability permits an unauthorized user to access restricted directories.
Apache Tomcat/JBoss	CVE-2010-0738	JBoss EAP JMX authentication bypass with crafted HTTP request.
Cacti	CVE-2013-2618	XSS vulnerability in editor.php in Networking Weathermap before 0.97b.
Drupal	CVE-2014-3704	SQL injection attack in Drupal core 7.x before 7.32.
Joomla	CVE-2015-8562	Joomla object injection RCE vulnerability.
Oracle E-Business Suite	CVE-2015-2652	Allows remote attackers to affect integrity via unknown vectors related to web management.

Of the vulnerabilities listed above, only two were from 2015, reinforcing that older CVEs continue to be exploited even though patches have been publically available for extended periods of time. With web-based applications, it is imperative to engage in proactive patch management, as this is the primary line of defense for public facing infrastructure.

[1] Some of these vulnerabilities are also exploited by cyber criminals in addition to state-sponsored cyber operators.

In addition to the use of the CVEs identified above, this APT utilizes spear-phishing e-mails containing links or documents to compromise systems. Previous spear-phish e-mails sent by these actors contained decoy documents, such as an US letter fax test page and an office monkeys video.

Once on computer networks, the actors utilizing these exploits are extremely adept at lateral movement through the enterprise, to include the ability to gain administrative access, including domain-level access, within a short time frame. They have utilized Mimikatz for credential harvesting and both Windows Management Instrumentation and a Python executable named LogonUI for persistence. In addition, they have utilized PowerShell scripts to push post-exploitation tools to the host. Below are MD5 hash values for identified instances of these files:

Filename	MD5	Notes:
m64.exe	3517b5d972955f86e02c5abe2a1693bd	64-bit version of Mimikatz
mimi_morph.exe	afa6d09443ed9414e7ac395b77ec3144	32-bit version of Mimikatz
wu.ps1	59cdaabe07f5ae504cc83def99fd7fe3	PowerShell script to push out Mimikatz
LogonUI.exe	7170ea924e749b4c9e26120ba5e72264	Python executable backdoor
LogonUI.exe	cc11b319bd53208649eb699045bd5053	Unpacked executable

The actor has utilized public storage mechanisms for exfiltration, as well as malware delivery, such as Google Drive, Microsoft OneDrive, and Dropbox. Recently, the CNE operator escalated to using The Onion Router (TOR) to obfuscate remote access and potentially for exfiltration.

More specifically, the CNE operator is implementing the TOR plugin, Meek, to obfuscate C2. Meek utilizes transport layer security (TLS) to encrypt communications and relay traffic through a legitimate third-party server, such as Google, to legitimize the traffic further.

YARA Rules

YARA rules for malware associated with compromises involving the APT actors:

a.

```
rule INDICATOR_IMPLANT_Loader
{
strings:
   $STR1 = {F7 C1 00 00 00 04 BA 00 02 00 00 0F 45 C2 F7 C1 00 00 00 20}
condition:
   (uint16(0) == 0x5A4D) and all of them
}
```

b.

```
rule INDICATOR_Implant_Loader2
{
strings:
   $STR1 = "%ws_out%ws" wide
condition:
   (uint16(0) == 0x5A4D) and $STR1
}
```

c.

```
rule IMPLANT2_3
{
strings:
   $STR1 = "miniDionis"
   $STR2 = "get_BotID"
   $STR3 = "TrExtractKey"
   $STR4 = "File {0} has been uploaded in {1}" wide
   $STR5 = "Process (pid:{1}) {0} has been started" wide
condition:
    (uint16(0) == 0x5A4D) and any of them

}
```

d.

```
/*    Benjamin DELPY `gentilkiwi`
http://blog.gentilkiwi.com
benjamin@gentilkiwi.com
Licence : http://creativecommons.org/licenses/by/3.0/fr/
*/
rule mimikatz
{
meta:
description      = “mimikatz”
author           = “Benjamin DELPY (gentilkiwi)”
tool_author      = “Benjamin DELPY (gentilkiwi)”
strings:
$exe_x86_1       = { 89 71 04 89 [0-3] 30 8d 04 bd }
$exe_x86_2       = { 89 79 04 89 [0-3] 38 8d 04 b5 }

$exe_x64_1       = { 4c 03 d8 49 [0-3] 8b 03 48 89 }
$exe_x64_2       = { 4c 8b df 49 [0-3] c1 e3 04 48 [0-3] 8b cb 4c 03 [0-3] d8 }

$dll_1           = {    c7 0? 00 00 01 00 [4-14] c7 0? 01 00 00 00 }
$dll_2           = { c7 0? 10 02 00 00 ?? 89 4? }

$sys_x86       = { a0 00 00 00 24 02 00 00 40 00 00 00 [0-4] b8 00 00 00 6c
02 00 00 40 00 00 00 }
$sys_x64       = { 88 01 00 00 3c 04 00 00 40 00 00 00 [0-4] e8 02 00 00 f8
02 00 00 40 00 00 00 }
condition:
(all of ($exe_x86_*)) or (all of ($exe_x64_*)) or (all of ($dll_*)) or (any of
($sys_*))
}
```

e.

```
rule mimikatz_lsass_mdmp
{
meta:
description       = “LSASS minidump file for mimikatz”
author            = “Benjamin DELPY (gentilkiwi)”
strings:
$lsass            = “System32\\lsass.exe”    wide nocase
condition:
(uint32(0) == 0x504d444d) and $lsass
}
```

f.

```
rule mimikatz_kirbi_ticket
{
meta:
description       = “KiRBi ticket for mimikatz”
author            = “Benjamin DELPY (gentilkiwi)”
strings:
$asn1             = { 76 82 ?? ?? 30 82 ?? ?? a0 03 02 01 05 a1 03 02 01 16 }
condition:
$asn1 at 0
}
```

g.

```
rule wce
{
meta:
description       = “wce”
author            = “Benjamin DELPY (gentilkiwi)”
tool_author       = “Hernan Ochoa (hernano)”
strings:
$hex_legacy       = { 8b ff 55 8b ec 6a 00 ff 75 0c ff 75 08 e8 [0-3] 5d c2 08 00 }
$hex_x86          = { 8d 45 f0 50 8d 45 f8 50 8d 45 e8 50 6a 00 8d 45 fc 50 [0-8] 50 72
69 6d 61 72 79 00 }
$hex_x64          = { ff f3 48 83 ec 30 48 8b d9 48 8d 15 [0-16] 50 72 69 6d 61 72 79
00 }
condition:
any of them
}
```

Recommended Mitigations

Precautionary measures to mitigate these techniques are:

- 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
- Implement tiered administrative models with dedicated administrator workstations to prevent Mimikatz from harvesting domain-level credentials
- Upgrade PowerShell to new versions with enhanced logging features and centralize logs to detect usage of often 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.

There is no additional information available on this topic at this time. For comments or questions related to the content or dissemination of this product, contact CyWatch.

Further 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

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

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