Global Accellion data breaches linked to Clop ransomware gang

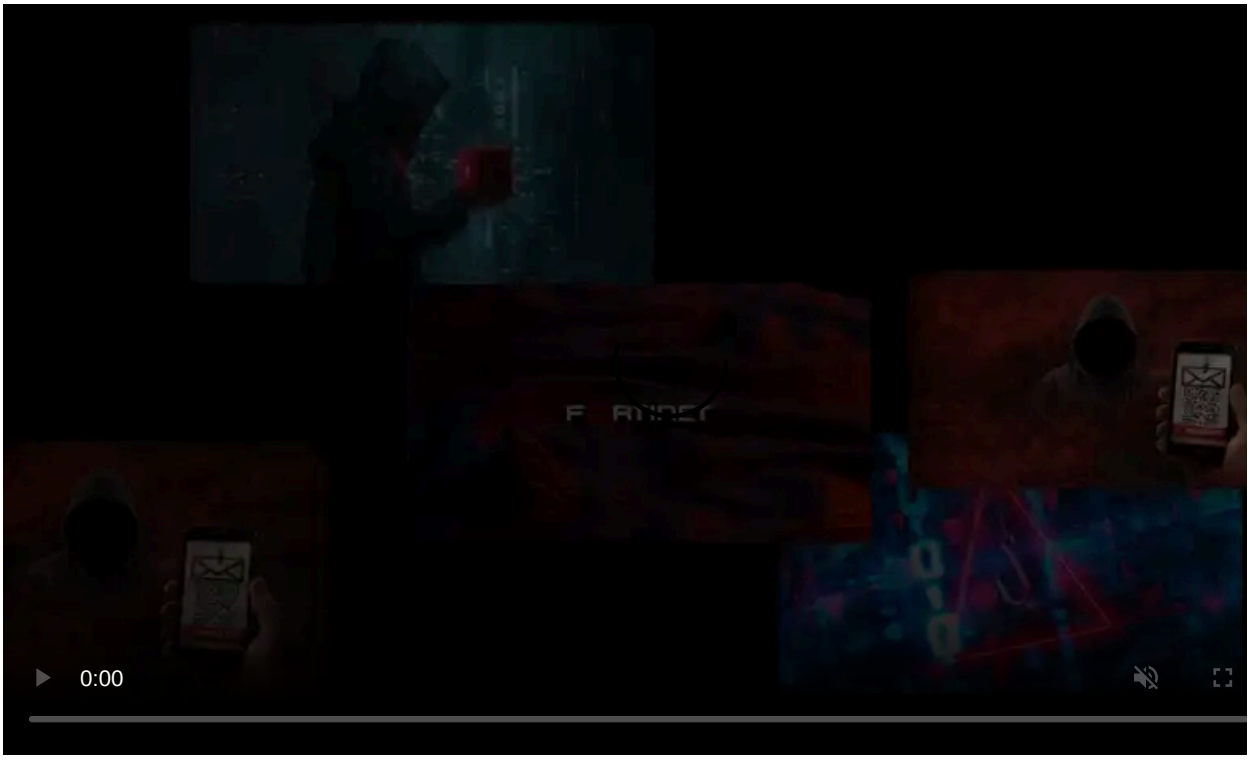
By Ionut Ilascu

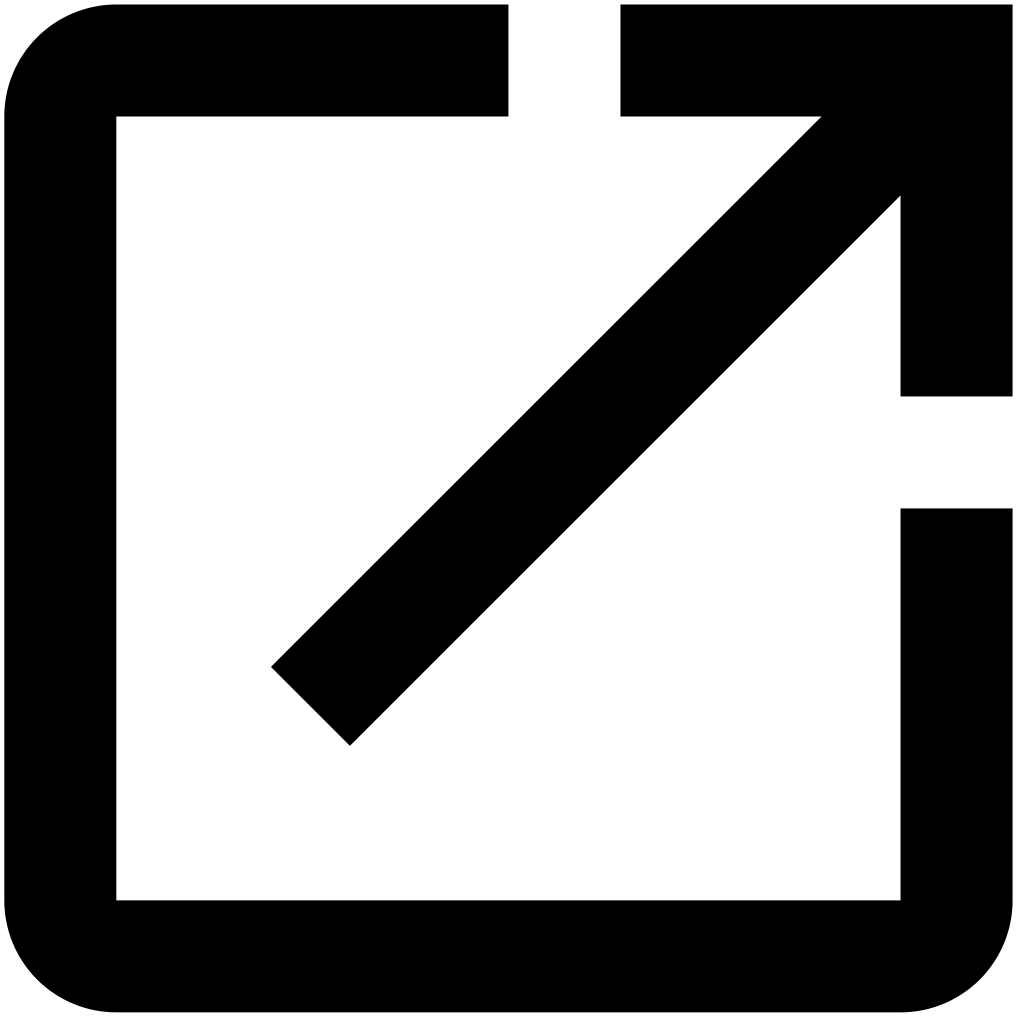
Published: 2021-02-22 · Archived: 2026-04-06 02:52:57 UTC

Threat actors associated with financially-motivated hacker groups combined multiple zero-day vulnerabilities and a new web shell to breach up to 100 companies using Accellion's legacy File Transfer Appliance and steal sensitive files.

The attacks occurred in mid-December 2020 and involved the Clop ransomware gang and the FIN11 threat group. Unlike previous attacks by these groups, the Clop file-encrypting malware was not deployed.

It appears that the actors opted for an extortion campaign. After stealing the data, they threatened victims over email with making stolen information publicly available on the Clop leak site unless a ransom was paid.


0:00



> 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.

BleepingComputer has been tracking these Accellion-related breaches and discovered almost a dozen victims.

Among them are supermarket giant Kroger, Singtel, QIMR Berghofer Medical Research Institute, Reserve Bank of New Zealand, the Australian Securities and Investments Commission (ASIC), and the Office of the Washington State Auditor ("SAO").

Additional victims tracked by BleepingComputer include :

- technical services company ABS Group
- law firm Jones Day
- Fortune 500 science and technology corporation Danaher
- geo-data specialist Fugro
- the University of Colorado

After we reported on the Singtel breach earlier this month, the Clop gang contacted us and stated that they stole 73 GB of data as part of their attack. When BleepingComputer asked how they gained access to Singtel's data, Clop refused to share that information.

BleepingComputer has learned from sources that the American Bureau of Shipping (ABS), who Clop listed as Eagle.org, received a ransom note via email.

Details about Accellion attacks revealed

A coordinated announcement from Accellion and Mandiant today sheds light on how the attacks against the Accellion FTA devices took place.

In its press release, Accellion says there were 300 customers using its legacy, 20-years old File Transfer Appliance (FTA). Of these customers, less than 100 were victims of the attacks from Clop and FIN11, and that less “than 25 appear to have suffered significant data theft.

Accellion patched the vulnerabilities and continues its mitigations efforts. The company “strongly recommends that FTA customers migrate to Kiteworks” - an enterprise content firewall platform that has a different code base, features a security architecture, and includes a segregated, secure devops process.

Incident responders at FireEye Mandiant investigated these attacks for some of their customers and highlighted the collaboration between Clop ransomware and the FIN11 gang in this campaign.

Both groups have worked together before. Last year, FIN11 joined the ransomware business and started to encrypt the networks of their victims using Clop.

Mandiant has been tracking the recent exploitation of Accellion FTA using multiple zero-days as UNC2546. The following vulnerabilities have been discovered:

- 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

The researchers distinguish this activity from the extortion campaign, which they track as UNC2582. However, they did notice overlaps between the two and previous operations attributed to FIN11.

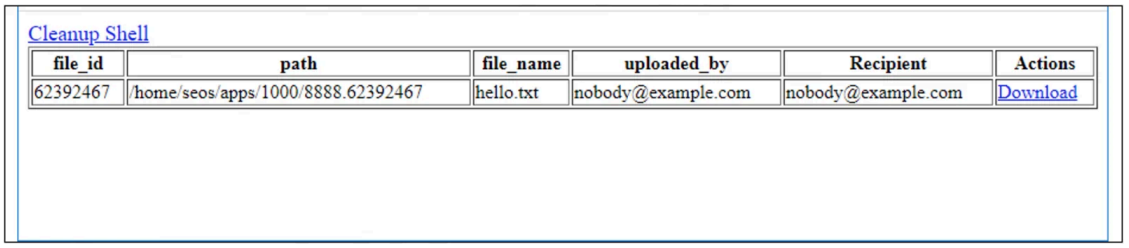
New DEWMODE webshell planted on Accellion devices

While investigating the incidents, the researchers observed that the intruders used a previously undocumented webshell that they called DEWMODE.

“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”

The researchers reconstructed the compromise of Accellion FTAs using system logs from the breached devices, trailing the initial entry, the deployment of DEWMODE, and the follow-up interaction.

The attacker used the SQL injection vulnerability to gain access and then followed with requests to additional resources. Once they obtained the necessary access level, the hackers wrote the DEWMODE web shell to the system.


Cleanup Shell

file_id	path	file_name	uploaded_by	Recipient	Actions
62392467	/home/seos/apps/1000/8888.62392467	hello.txt	nobody@example.com	nobody@example.com	Download

The role of the webshell was to extract a list of available files from a MySQL database on the FTA and to list them on an HTML page along with the accompanying metadata (file ID, path, filename, uploader, and recipient).

A blog post from Mandiant today explains all the technical aspects regarding the use of the web shell and how the hackers gained access to their targets.

The intruders stole the data via DEWMODE but did not encrypt the compromised systems. In late January, though, victims started to get extortion emails from someone threatening to publish the stolen data on Clop ransomware’s leak site.

If the victim did not respond to the initial threats, other emails followed with the clear intention to force payment.

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!

The researchers note that the first emails are delivered to a smaller set of recipients from a free email account that appears to be unique for each victim.

Lack of a reply from the victim led to the hackers sending out additional emails, "to a much larger number of recipients from hundreds or thousands of different email accounts and using varied SMTP infrastructure," Mandiant says.

"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" - Mandiant

Analyzing the extortion emails, the researchers found that some of the IP addresses and email accounts had been used by FIN11 in phishing operations between August and December 2020.

Furthermore, some of the targets compromised through Accellion's FTA had been compromised by FIN11 in the past, linking the group to this set of intrusions.

Another connection is an IP address used to communicate with DEWMODE web shell, which is assigned to Fortunix Networks L.P., a network that FIN11 uses frequently for one of their malware downloaders tracked as FRIENDSPEAK.

Mandiant says that the connection between FIN11 and UNC2546 in the Accellion breaches are "compelling" but the the relationship is still under assessment, which explains why the researchers are tracking the threats separately.

A reason is that the infection vector and foothold attributed to UNC2546 are different from what has been attributed to FIN11. Moreover, the uncategorized actor did not move laterally across the network, something that FIN11 does.

Based on this, Mandiant considers that they have insufficient evidence for attributing the attacks 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," the researchers say.
