Ransomware Roundup - Cl0p | FortiGuard Labs

By Shunichi Imano, James Slaughter

Published: 2023-07-21 · Archived: 2026-04-05 23:47:40 UTC

On a bi-weekly basis, FortiGuard Labs gathers data on ransomware variants of interest that have been gaining traction within our datasets and the OSINT community. The Ransomware Roundup report aims to provide readers with brief insights into the evolving ransomware landscape and the Fortinet solutions that protect against those variants.

This edition of the Ransomware Roundup covers the Cl0p ransomware.

Affected platforms: Microsoft Windows, Linux
Impacted parties: Microsoft Windows, Linux Users
Impact: Encrypts and exfiltrates victims' files and demands ransom for file decryption and not to leak stolen files
Severity level: High

Recently, the Cl0p ransomware group received a lot of media attention for compromising a large number of organizations by exploiting a recently-unpatched vulnerability in MOVEit Transfer (CVE-2023-34362), a managed file transfer (MFT) solution. Although there is no evidence that the threat actor used the encryptor in this particular incident, the group exfiltrated data from victims and threatened them with ransom in exchange for not exposing the stolen information.

This blog provides insights into the Cl0p ransomware group's activities over the past several years.

Note that FortiGuard Labs released an Outbreak Alert for the MOVEit Transfer incident. Please refer to "Progress MOVEit Transfer SQL Injection Vulnerability" for additional information.

What is Cl0p?

The history of Cl0p ransomware goes back to early 2019 and is typically associated with financially motivated threat actor FIN11 (also known as TA505 and Snakefly), who is known to target organizations in North America and Europe. The Cl0p ransomware appears to be a descendent (or variant) of another ransomware, "CryptoMix", which also has an association with FIN11. And CryptoMix is reportedly a hybrid of the ransomware variants "CryptXXX" and "CryptoWall". However, that claim has not yet been independently verified by FortiGuard Labs.

Typically, FIN11 unleashes Cl0p ransomware on a victim's network to encrypt files after stealing information. However, the ransom note dropped by an older Cl0p ransomware variant, shown below, shows no evidence of FIN11 having exploited victim data, at least during the early period of Cl0p ransomware activity. It is estimated that they only began exfiltrating victim information around the time the leak site described later in this report was set up.

Figure 1: Files encrypted by an earlier version of the Cl0p ransomware

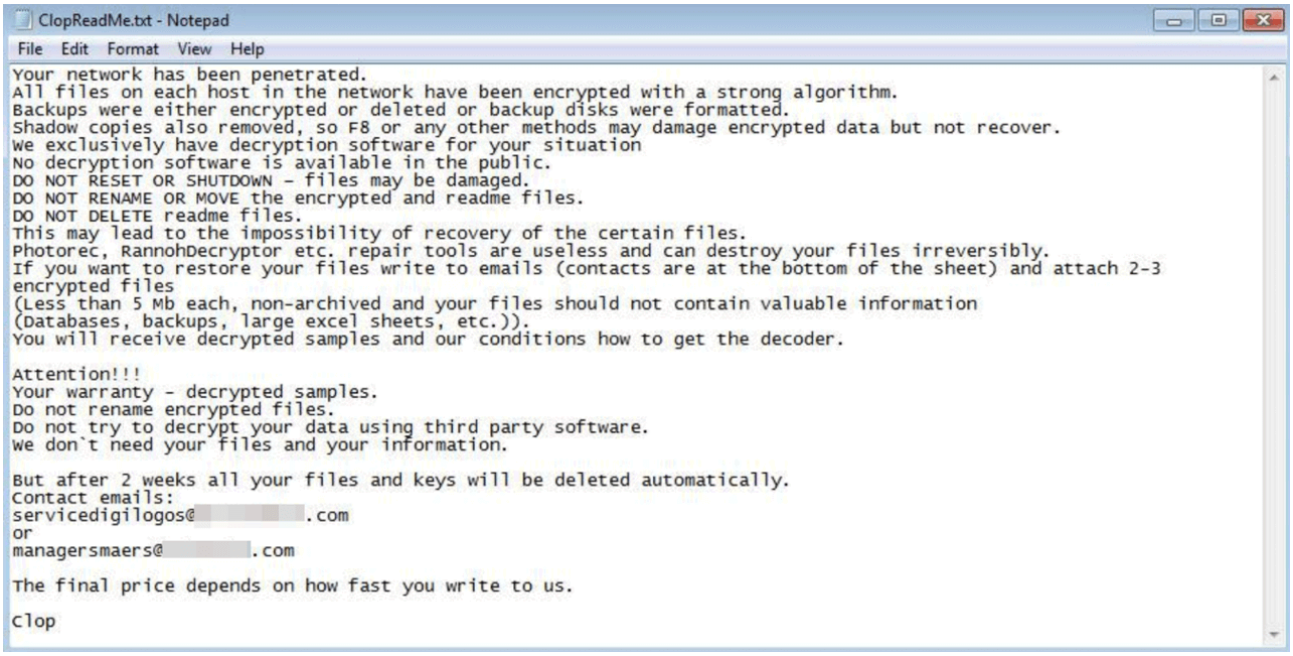

Figure 2: Ransomware note dropped by an earlier version of the Cl0p ransomware

At some stage in its operations, the FIN11 group revised its strategy of deploying ransomware and shifted to purely exfiltrating information from victims for extortion. In fact, there is no evidence that the Cl0p ransomware was deployed when the MOVEit Transfer vulnerability was recently exploited.

Deployed Cl0p ransomware variants append a new file extension to the files it encrypts. Typical file extensions include, but are not limited to, “.Clop”, “.Cl0p”, “.C_L_O_P”, “.C_I_0P” and “.Cllp”. Cl0p ransomware ransom notes are labeled “ClopReadMe.txt”, “README_README.txt” and “!!!_READ_!!!.RTF”.

The Cl0p threat actor is also associated with the use of the Cobalt Strike post-exploitation tool, web shells such as DEWMODE and LEMURLOOT, SDBot, and the FlawedAmmyy remote access trojan (RAT). FIN11 is also known to use spear-phishing to target victims.

FIN11 recently leveraged the MOVEit Transfer SQL injection vulnerability (CVE-2023-34362) to gain initial entry to victim networks. This was not the first time the group has exploited vulnerabilities. According to a report published by the Health Sector Cybersecurity Coordination Center (HC3), the following vulnerabilities have been potentially exploited by this group:

- PaperCut MF/NG improper access control vulnerability (CVE-2023-27350, CVE-2023-27351)
- Accellion File Transfer Appliance vulnerabilities (CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, CVE-2021-27104)
- Windows Netlogon elevation of privilege vulnerability (aka. ZeroLogon) (CVE-2020-1472)
- Fortra GoAnywhere Managed File Transfer (MFT) Remote Code Execution (RCE) vulnerability (CVE-2023-0669)
- SolarWinds Serv-U remote memory escape vulnerability (CVE-2021-35211)
- F5.BIG-IP iControl REST authentication bypass vulnerability (CVE-2022-1388)
- Apache Log4J Remote Code Execution (RCE) vulnerability (CVE-2021-44228)

While earlier Cl0p ransomware variants only include an attacker's contact email addresses, the ransom group subsequently set up a data leak site on TOR in 2020 called "CL0P^_-LEAKS" to post information stolen from victims.

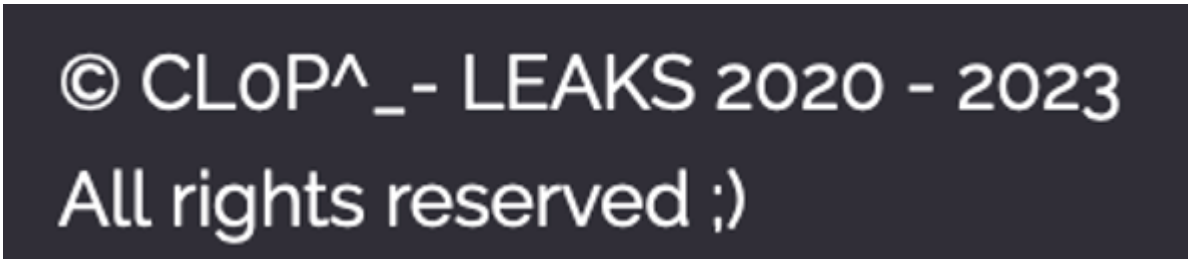

Figure 3: Duration of activity of the data leak site listed on the Cl0p ransomware TOR site.

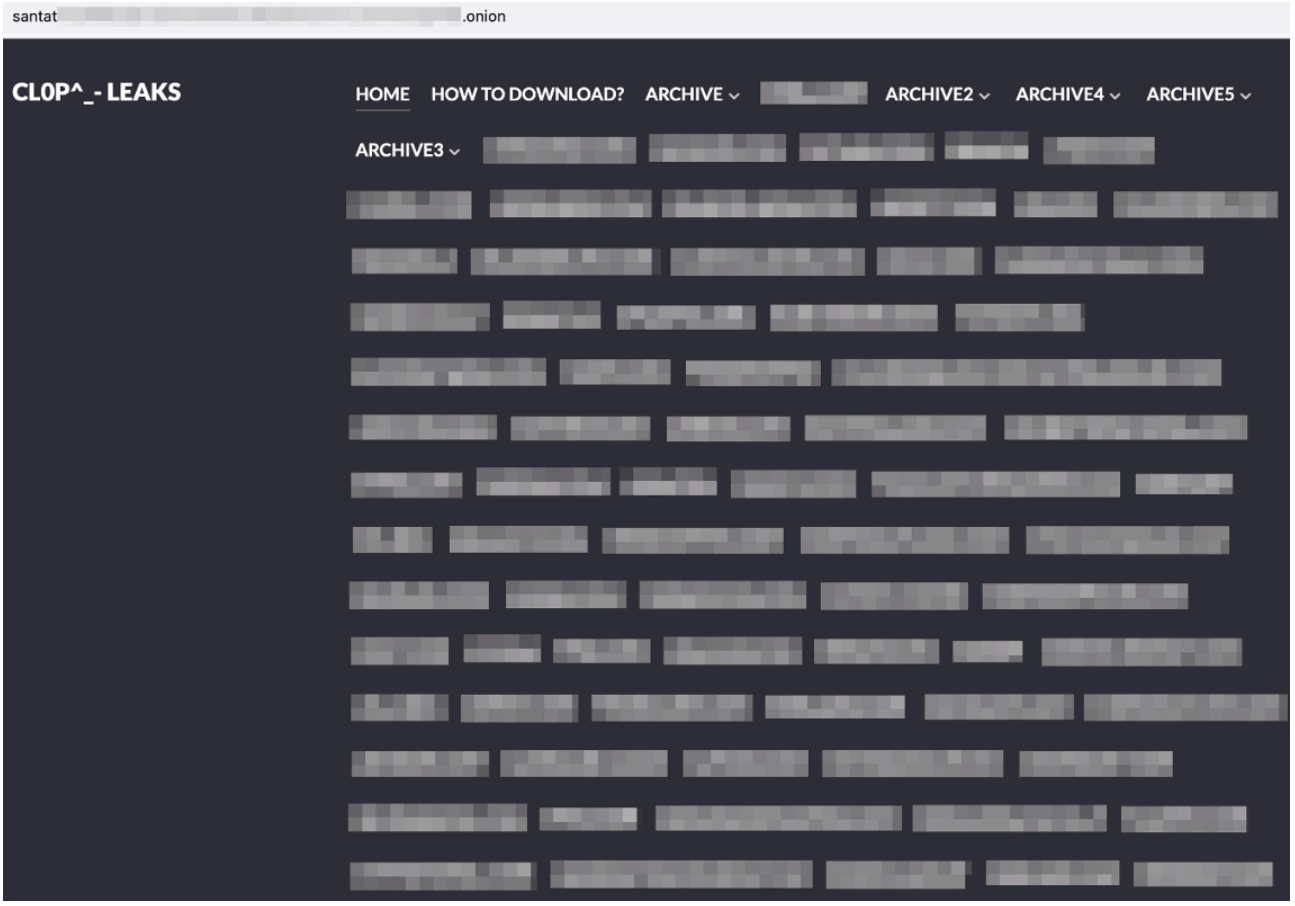

Figure 4: Main page of the Cl0p ransomware TOR site

On the TOR site, the ransomware group also states that its primary motivation is financial gain and that it is not politically motivated in its choice of victims.

> *WE GOT A LOT OF EMAILS ABOUT GOVERNMENT DATA, WE DON'T HAVE ANY GOVERNMENT DATA AND ANYTHING DIRECTLY RESIDING ON EXPOSED AND BAD PROTECTED NOT ENCRYPTED FILE TRANSFER WE STILL DO THE POLITE THING AND DELETE ALL. ALL MEDIA SPEAKING ABOUT THIS ARE DO WHAT ALWAYS THEY DO. PROVIDE LITTLE TRUTH IN A BIG LIE. WE ALSO WANT TO REMIND ALL COMPANY THAT IF YOU PUT DATA ON INTERNET WHERE DATA IS NOT PROTECT DO NOT BLAME US FOR PENETRATION TESTING SERVICE. WE ARE ONLY FINANCIAL MOTIVATED AND DO NOT CARE ANYTHING ABOUT POLITICS.*

Figure 5: Financial statement made by the Cl0p threat actor

The group also claims that it intends to attack commercial pharmaceutical companies, but not hospitals and social institutions.

> **ATTENTION!!!**
> **We have never attacked hospitals, orphanages, nursing homes, charitable foundations, and we will not.**
> **Commercial pharmaceutical organizations are not eligible for this list;**
> **they are the only ones who benefit from the current pandemic.**
> **If an attack mistakenly occurs on one of the foregoing organizations, we will provide the decryptor for free, apologize and help fix the vulnerabilities.**

Figure 6: Cl0p's statement on TOR for not attacking certain industry sectors

DEAR COMPANIES.

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.
STEP 2 - EMAIL OUR TEAM UNLOCK@ COM OR UNLOCK@ COM
STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE

STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE
STEP 2 - IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU
STEP 3 - OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE
STEP 4 - YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING
STEP 5 - YOU HAVE 3 DAY TO DISCUSS PRICE AND IF NO AGREEMENT YOU CUSTOM PAGE WILL BE CREATED
STEP 6 - AFTER 7 DAYS ALL YOU DATA WILL START TO BE PUBLICATION
STEP 7 - YOU CHAT WILL CLOSE AFTER 10 NOT PRODUCTIVE DAY AND DATA WILL BE PUBLISH

WHAT WARRANTY? OUR TEAM HAS BEEN AROUND FOR MANY YEARS. WE HAVE NOT EVEN ONE TIME NOT DO AS WE PROMISE. WHEN WE SAY DATA IS DELETE IT IS CAUSE WE SHOW VIDEO PROOF. WE HAVE NO USE FOR FEW MEASLE DOLLARS TO DECEIVE YOU.

CALL TODAY BEFORE YOUR COMPANY NAME IS PUBLISH HERE.

Figure 7: Message to the Cl0p victims in regards with MOVEit Transfer vulnerability (CVE-2023-34362)

Prevalence

As of July 15th, 2023, Fortinet's FortiRecon service listed 419 victim organizations on the Cl0p ransomware data leak site.

Figure 8: The number of ransomware victims on the Cl0p data leak site per FortiRecon

According to data collected through Fortinet's FortiRecon service, the Cl0p ransomware group preyed on several industry sectors between January and June 2023, with business services leading the way, followed by software and finance. When victim organizations are classified by country, the United States is in first place by a significant margin. By region, nearly three-quarters of victims are located in North America and Europe.

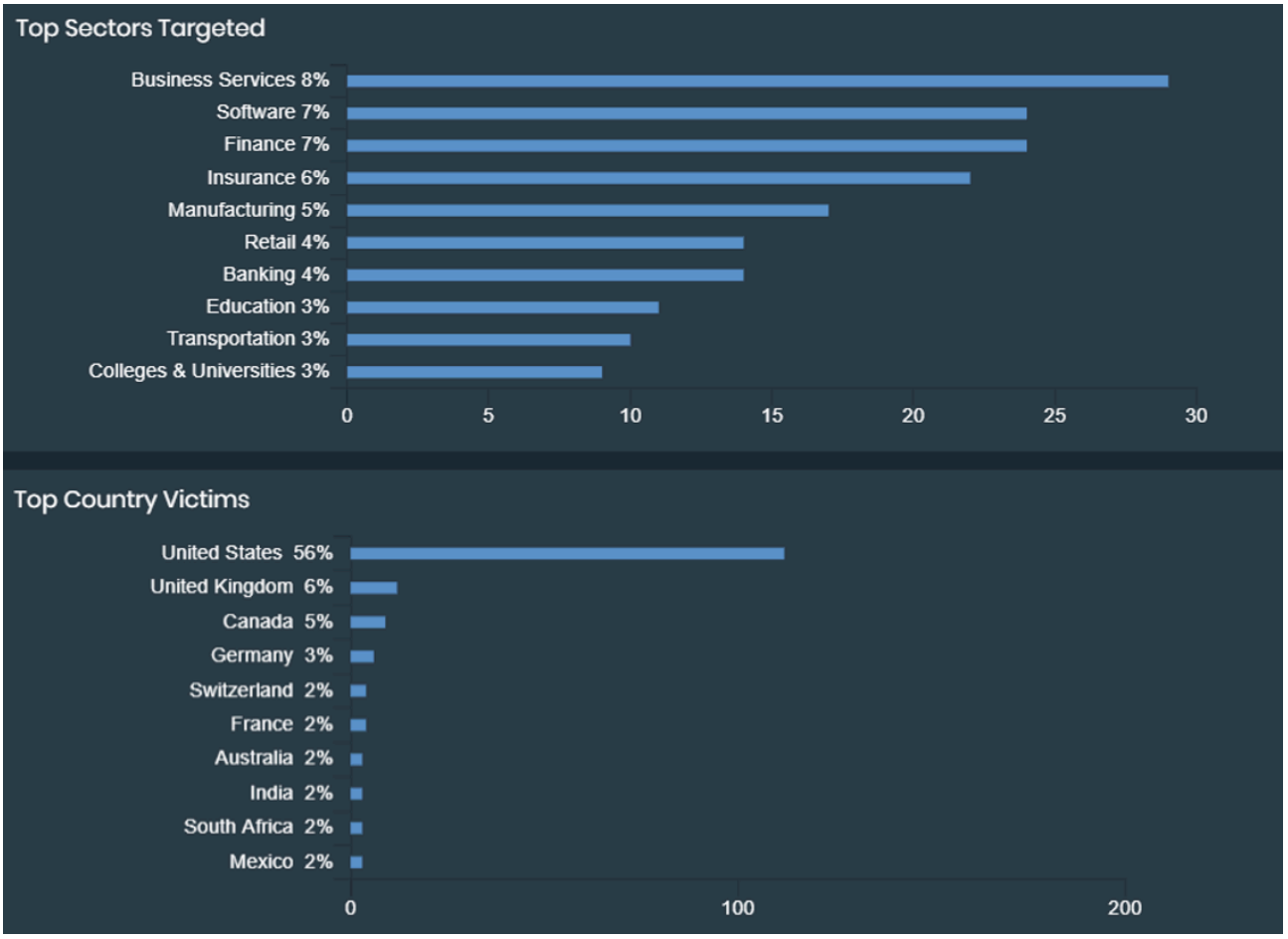

Figure 9: Top industry sectors and Cl0p ransomware victims locations in the first half of 2023 per FortiRecon

The FortiRecon data below indicates that the Cl0p ransomware has been more active in 2023 than 2022 and 2021. The inactivity of the ransomware group from May to July 2021 could be attributed to the arrest of some Cl0p ransomware operators in June 2021, though we cannot verify this.

Figure 10: The number of Cl0p ransomware victims in 2021, 2022 and 2023 per FortiRecon

Looking closely at the prevalence of Cl0p ransomware in the United States during the first half of 2023, Cl0p ranked third behind LockBit and Blackcat (ALPHV) ransomware.

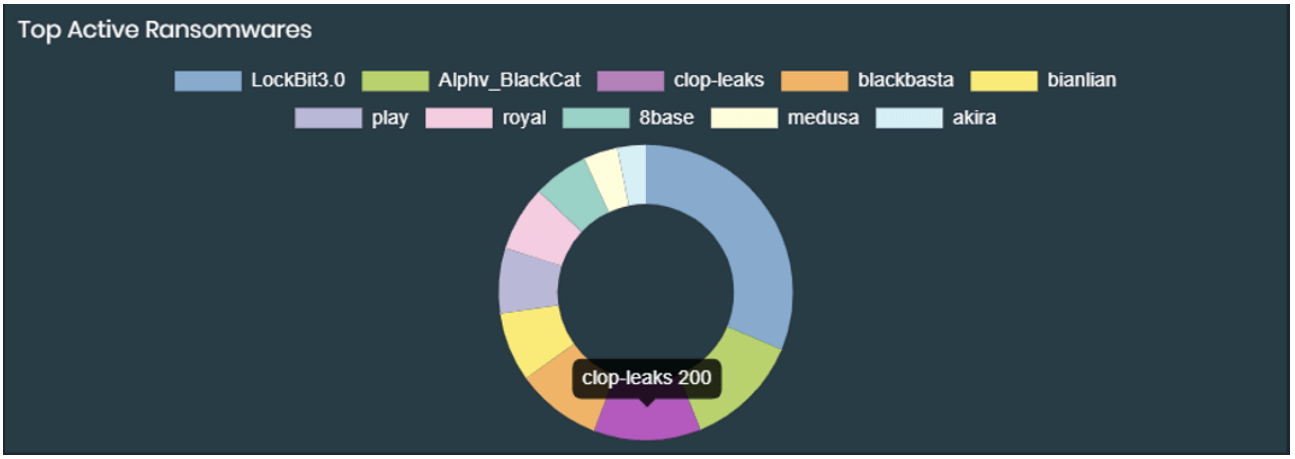

Figure 11: Cl0p ransomware ranking in the United States in the first half of 2023 per FortiRecon

Conclusion

The Cl0p ransomware has been around since early 2019, and its developers are still one of the most active ransomware threat actors today. While they seem to have largely shifted from "exfiltrating and encrypting data and extorting money" to simply "exfiltrating data and extorting money," affected organizations are just as impacted as before. As the group is known to exploit high-severity vulnerabilities, including the recently disclosed MOVEit Transfer vulnerability, patch management is critical to preventing attacks by the group.

IOCs

Note that a large number of Cl0p ransomware samples exist due to the high prevalence of the ransomware over the past several years. Because of this, this section only contains a small number of samples from the ransomware family.

SHA2	**Note**
3320f11728458d01eef62e10e48897ec1c2277c1fe1aa2d471a16b4dccfc1207	Cl0p ransomware
d0cde86d47219e9c56b717f55dcdb01b0566344c13aa671613598cab427345b9	Cl0p ransomware
d36766cbc149d7f79654d2810ffe2fd3b1a6487fe3aff6ff010e664b60493cf0	Cl0p ransomware
1687eda911c5129f3189d7e1ad31430856d7732fe870eb49971298367b98189c	Cl0p ransomware

f1b8c7b2d20040f1dd9728de9808925fdcf035a1a289d42f63e5faa967f50664	Cl0p ransomware
343cb2d5900f5fe4abd5442a4a18541753fbb6ca5ff4ee7f2c312ed96e413335	Cl0p ransomware
968307a367471e25bef58b0d4687ab4fdf34539bbfb603b5b19ae99d4d0c0340	Cl0p ransomware
09d6dab9b70a74f61c41eaa485b37de9a40c86b6d2eae7413db11b4e6a8256ef	Cl0p ransomware for Linux

Protection

FortiGuard Labs has the following AV signatures in place for the Cl0p ransomware samples listed in the IOC section:

- W32/Filecoder_cl0p.A!tr.ransom
- W32/Filecoder.7742!tr.ransom
- W32/HydraCrypt.S!tr.ransom
- W32/HydraCrypt.P!tr.ransom
- W32/Encoder.Q!tr.ransom
- ELF/Filecoder_cl0p.A!tr.ransom
- Malicious_Behavior.SB

Additionally, the following AV signatures are available for Cl0p ransomware samples:

- W32/Ransom_Win32_CLOP.SMK
- W32/Ransom_Win32_CLOP.SME
- W32/Ransom_Win32_CLOP.SM
- W32/Ransom_Win32_CLOP.RK!tr
- W32/Ransom_Win32_CLOP.NW
- W32/Ransom_Win32_CLOP.AA
- W32/Ransom_Clop.PW!tr
- W32/Ransom.CLOP!tr
- W32/Filecoder_cl0p!tr.ransom
- W32/Clop.GWKF!tr.ransom
- W32/Clop.407E!tr.ransom
- W32/Clop.2D9D!tr.ransom
- W32/Clop.2794!tr.ransom
- Linux/Filecoder_Cl0p.A!tr

FortiGuard Labs has put the following IPS signatures in place for the vulnerabilities reportedly exploited by the Cl0p ransomware threat actor:

- Progress.MOVEit.Transfer.Unrestricted.File.Upload (CVE-2023-34362)
- PaperCut.NG.SetupCompleted.Authentication.Bypass (CVE-2023-27350 and CVE-2023-27351)
- Fortra.GoAnywhere.MFT.LicenseResponseServlet.Command.Injection (CVE-2023-0669)
- Accellion.FTA.Remote.OS.command.Execution (CVE-2021-27102)
- MS.Windows.Server.Netlogon.Elevation.of.Privilege (CVE-2020-1472)
- SolarWinds.Serv-U.FTP.Unauthorized.User.Creation (CVE-2021-35211)
- F5.BIG-IP.iControl.REST.Authentication.Bypass (CVE-2022-1388)
- Apache.Log4j.Error.Log.Remote.Code.Execution (CVE-2021-44228)

FortiGuard Labs Guidance

Due to the ease of disruption, damage to daily operations, potential impact to an organization's reputation, and the unwanted destruction or release of personally identifiable information (PII), etc., it is vital to keep all AV and IPS signatures up to date.

Since the majority of ransomware is generally delivered via phishing, organizations should consider leveraging Fortinet solutions designed to train users to understand and detect phishing threats:

The FortiPhish Phishing Simulation Service uses real-world simulations to help organizations test user awareness and vigilance to phishing threats and to train and reinforce proper practices when users encounter targeted phishing attacks.

Fortinet's FREE NSE training: NSE 1 – Information Security Awareness includes a module on internet threats designed to help end users learn how to identify and protect themselves from various types of phishing attacks and can be easily added to internal training programs.

Organizations also need to make foundational changes to the frequency, location, and security of their data backups to effectively deal with the evolving and rapidly expanding risk of ransomware. When coupled with digital supply chain compromise and a workforce telecommuting into the network, there is a real risk that attacks can come from anywhere. Organizations are encouraged to implement cloud-based security solutions, such as SASE, to protect off-network devices, advanced endpoint security, such as EDR (endpoint detection and response) solutions that can disrupt malware mid-attack, and Zero Trust Access and network segmentation strategies that restrict access to applications and resources based on policy and context. These solutions are proven to minimize risk and reduce the impact of a successful ransomware attack.

By operating these solutions as part of the industry's only fully integrated Security Fabric, organizations can also take advantage of native synergy and automation across your security ecosystem, Fortinet also provides an extensive portfolio of technology and human-based as-a-service offerings that can be deployed independently or as part of the Fortinet Security Fabric. These services are powered by advanced AI-enabled technologies and our global FortiGuard team of seasoned cybersecurity experts.

Best Practices Include Not Paying a Ransom

Organizations such as CISA, NCSC, the FBI, and HHS caution ransomware victims against paying a ransom partly because payment does not guarantee that files will be recovered. According to a U.S. Department of

Treasury's Office of Foreign Assets Control (OFAC) advisory, ransom payments may also embolden adversaries to target additional organizations, encourage other criminal actors to distribute ransomware, and/or fund illicit activities that could potentially be illegal. For organizations and individuals affected by ransomware, the FBI has a Ransomware Complaint page where victims can submit samples of ransomware activity via their Internet Crimes Complaint Center (IC3).

How Fortinet Can Help

FortiGuard Labs' Emergency Incident Response Service provides rapid and effective response when an incident is detected. And our Incident Readiness Subscription Service provides tools and guidance to help you better prepare for a cyber incident through readiness assessments, IR playbook development, and IR playbook testing (tabletop exercises).

Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard AI-powered security services portfolio.
