Ransomware Spotlight: Clop

Archived: 2026-04-06 00:11:48 UTC

X

An overview of Clop operations

The Clop ransomware appends the ".ClOP" ("Clop" spelled with a small "L") extension to the files it encrypts. Researchers also discovered that Clop targets a victim's entire network instead of just individual computers. This is made possible by hacking into the Active Directory (AD) server before the ransomware infection to determine the system's Group Policy. This allows the ransomware to persist in the endpoints even after incident responders have already cleaned them up.

Previous attacks by the TA505 group saw the delivery of the Clop malware as the final stage of its payloadopen on a new tab in massive phishing campaigns. The malicious actors would send spam emails with HTML attachments that would redirect recipients to a macro-enabled document such as an XLS file used to drop a loader named Get2. This loader facilitates the download of various tools such as SDBOT, FlawedAmmyy, and Cobalt Strike. Once the malicious actors intrude into the system, they proceed to reconnaissance, lateral movement, and exfiltration to set the stage for deployment of the Clop ransomware.

The operators behind Clop coerce their victims by sending out emails in a bid for negotiations. They also resort to more severe threats such as publicizing and auctioning off the stolen information on their data leak site "Cl0p^_-Leaks" if their messages are ignored. They have also gone to the extent of using quadruple extortion techniquesnews- cybercrime-and-digital-threats, which have involved going after top executivesopen on a new tab and customersopen on a new tab to pressure companies into settling the ransom.

Having established itself well in the world of cybercrime, the Clop ransomware gang is deemed as a trendsetter for its ever-changing tactics, techniques, and procedures (TTPs). Indeed, the group's Kiteworks FTA exploits set a new trend as these significantly pulled up the average ransom payments for the first quarter of 2021open on a new tab. A reportopen on a new tab that cited Coveware's findings revealed that the average ransomware payments significantly went up to US$220,298, which is an increase of 43%. It also said that the median ransom payment increased sharply to US$78,398 from US$49,459, which translates to a 60% hike.

Recent Clop activities

The Clop ransomware gang also claimed to have targeted 130 organizations who were victims of the Fortra GoAnywhere MFT vulnerabilitynews article over a month-long period in March 2023. Although Clop ransomware actors did not share specific details on how they exploited the vulnerability, security researcher Florian Hauser published proof-of-concept codenews article on it, while Fortra released an emergency patch shortly after.

Meanwhile, in April 2023, Microsoft attributednews article the exploitation of CVE-2023-27350 to the Clop and LockBit ransomware gangs. CVE-2023-27350 is a vulnerability in the widely used print management software solution PaperCut that was disclosed via Trend Micro's Zero Day Initiative (ZDI),™ as covered in ZDI-23-233. According to Microsoft, the threat actor abused the vulnerability to deploy the Truebot malware and ultimately, the Clop and LockBit ransomware families to steal critical company information.

In May of this year, it was reported that FIN7 (aka Sangria Tempest)news article used the POWERTRASH malware to launch the Lizar toolkit in a series of that started in April 2023. The cybercrime group used the backdoor to take hold of and laterally move within the victim's network and finally, distribute the Clop ransomware on compromised machines.

Since May 2023, the group continuously exploited critical zero-day vulnerabilities in file transfer software MOVEit Transfer and MOVEit Cloud via CVE-2023-24362 and CVE-2023-35036, to compromise a number of private and public organizations from various industries. While the company was able to immediately deploy workarounds, Clop exploited these openings to get into vulnerable systems and networks to exfiltrate sensitive data. Researchers and analysts have notednews article that no ransomware payloads were observed from these attacks, but that the group were focused more on extortion and threatened these high value targets with publishing sensitive and proprietary information. An additional SQL injection security gap still awaiting a CVE assignment and a patch also surfaced in June, which the group exploited.

The number of attacks documented to hold systems and information hostage as a routine are going down, which is common among other ransomware groups in recent months. However, the same techniques and skills are being used to compromise vulnerable systems and networks to steal data or extort companies in exchange for keeping these companies' information confidential.

Top affected countries and industries

In this section, we discuss Trend Micro™ Smart Protection Network™ (SPN) data on detections of Clop attempts to compromise organizations. Our detections reveal that Türkiye had the largest number of attack attempts at 94 followed by Canada with 80 attempts. The rest of the detections are spread across North America, South America, Asia Pacific, Europe, and the Middle East.

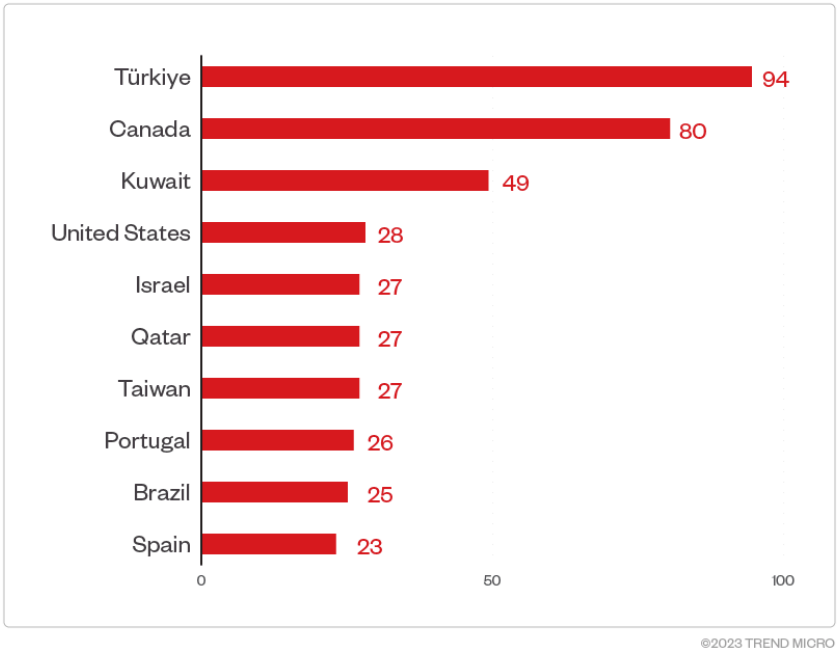
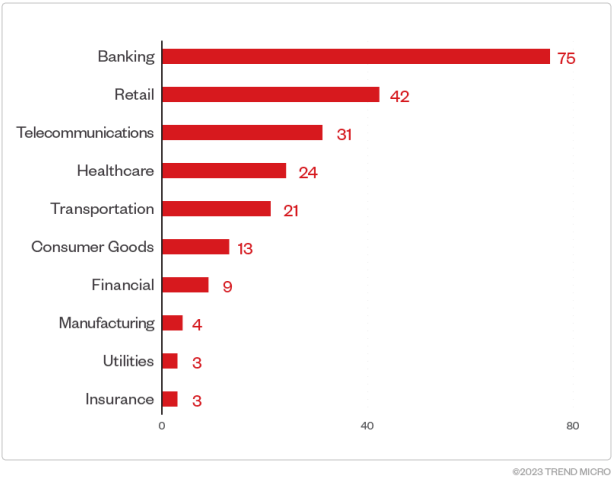


Figure 1. 10 countries with the highest number of attack attempts per machine for the Clop ransomware (January 1, 2023 to May 31, 2023)

While other known RaaS operators claim to avoid the healthcare sector as a target out of humanitarian consideration, our detections reveal that this is not the case for Clop as it is still within the gang's top five targets. The highest number of detections is at 75 in the banking industry, followed by a distant second of 42 detections in the retail sector.



open on a new tab

Figure 2. 10 industries with the highest number of attack attempts per machine for the Clop ransomware (January 1, 2023 to May 31, 2023)
Source: Trend Micro Smart Protection Network infrastructure

By breaking down the detections per month, we are able to determine that 2023 saw a sudden increase in Clop attacks in May of the same year at 245 attack attempts, significantly higher than the detections in prior months. Our detections suggest that Clop deployments were implemented at a steady pace from January to April 2023 before surging in May.

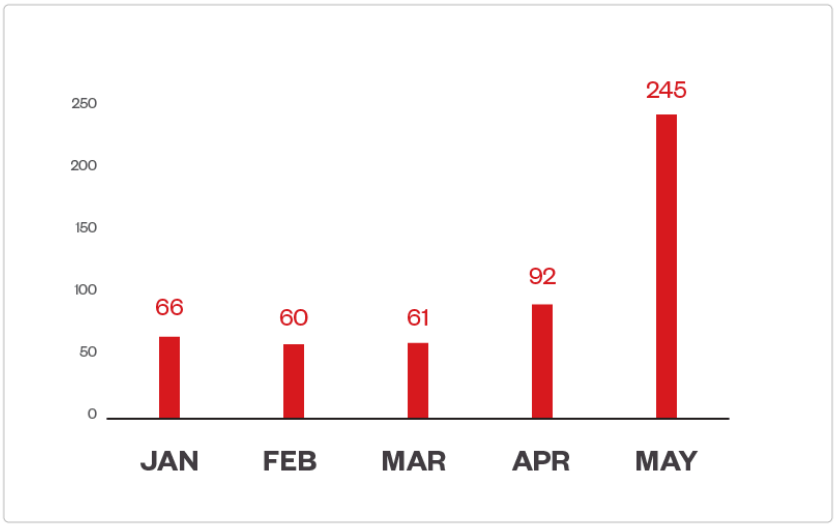
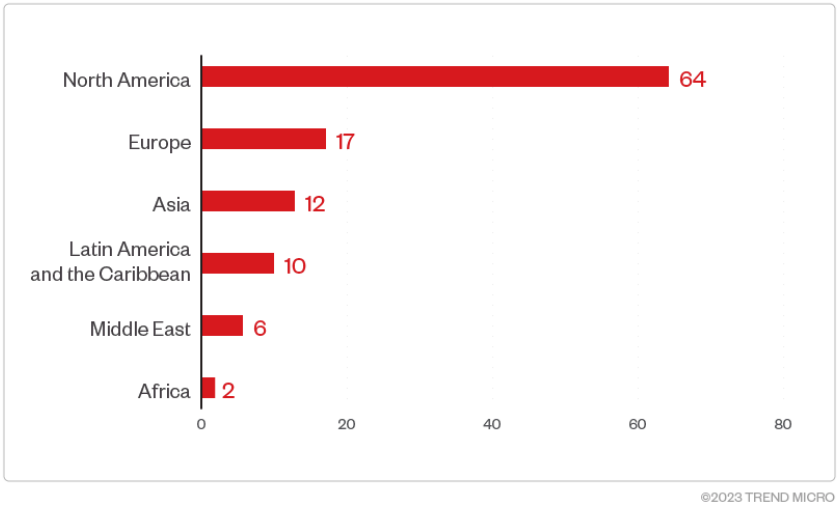


Figure 3. Monthly breakdown of detections per machine for the Clop ransomware (January 1, 2023 to May 31, 2023)
Source: Trend Micro Smart Protection Network infrastructure

Targeted regions and industries according to Clop ransomware's leak site

This section looks at data based on attacks recorded on the Clop ransomware operators' leak site. The following data represents organizations successfully infiltrated by Clop ransomware, which have refused to pay the ransom demand as of writing.

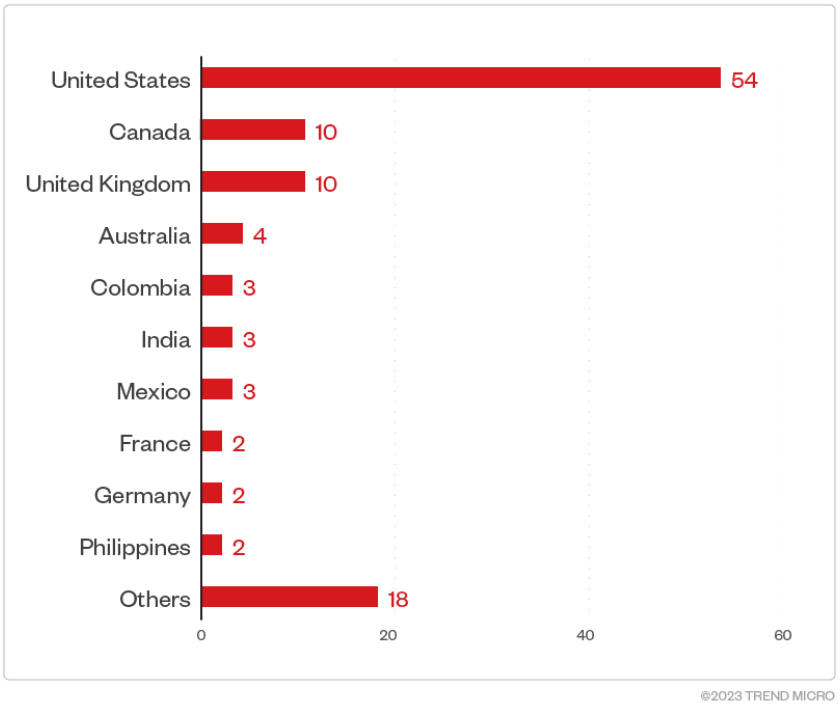
Based on a combination of Trend Micro's open-source intelligence (OSINT) research and investigation of the leak site, Clop ransomware compromised a total of 111 organizations from January to May 2023. Of these, 64 were organizations operating from North America, while 17 were from Europe. Enterprises in Asia, Latin America, the Middle East, and Africa were also compromised.



open on a new tab

Figure 4. The distribution by region of Clop ransomware's victim organization
Source: *Clop ransomware's leak site and Trend Micro's OSINT research (January 2023 – May 2023)*

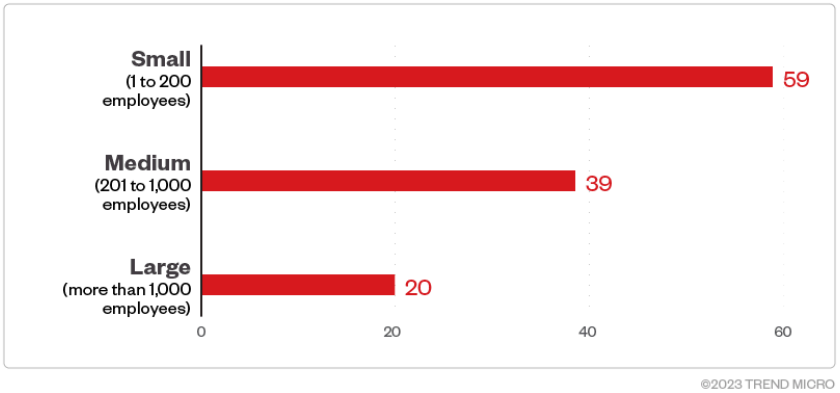
The United States had the most victim organizations with 54 compromised organizations, while 10 enterprises located in the United Kingdom and Canada were also affected. The next four countries most targeted by threat actors behind Clop are Australia, Colombia, India, and Mexico.



open on a new tab

Figure 5. The 10 countries most targeted by the Clop ransomware group
Source: *Clop ransomware's leak site and Trend Micro's OSINT research (January 2023 – May 2023)*

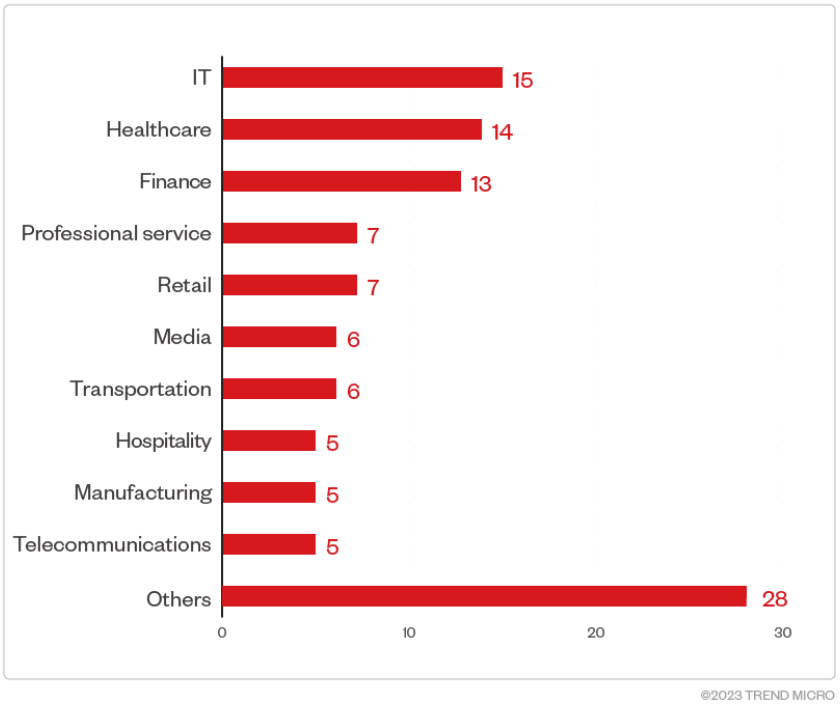
The majority of Clop ransomware victim organizations were large enterprises, followed closely by small- and medium-sized businesses.



open on a new tab

Figure 6. The distribution by organization size of Clop ransomware's victim organizations
Source: *Clop ransomware's leak site and Trend Micro's OSINT research (January 2023 – May 2023)*

Among the identified sectors of Clop ransomware victim organizations, the IT, healthcare, finance, professional services, and retail industries were its top targets.

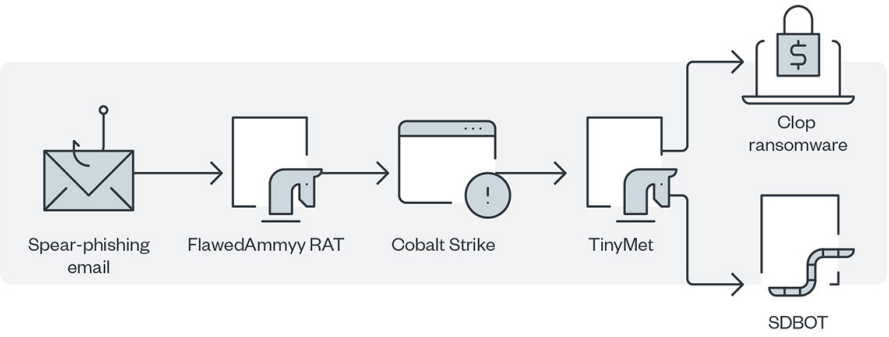


open on a new tab

Figure 7. The 10 industries most targeted by Clop ransomware threat actors
Source: *Clop ransomware's leak site and Trend Micro's OSINT research (January 2023 – May 2023)*

Infection chain and techniques

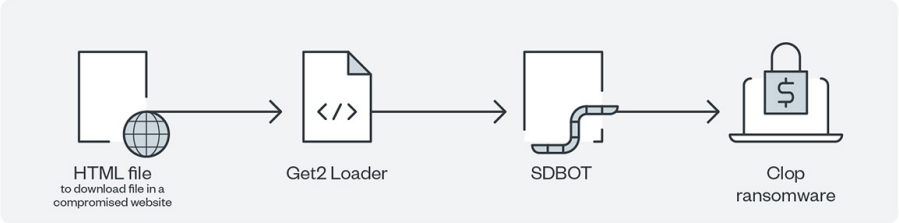
The Clop ransomware that TA505 first distributed evaded detection by using a binary that was digitally signed and verified to make it seem like a legitimate executable file. The group launched a large volume of spear-phishing emails that were sent to the employees of an organization to trigger the infection process. Figure 4 shows the infection chain.



open on a new tab

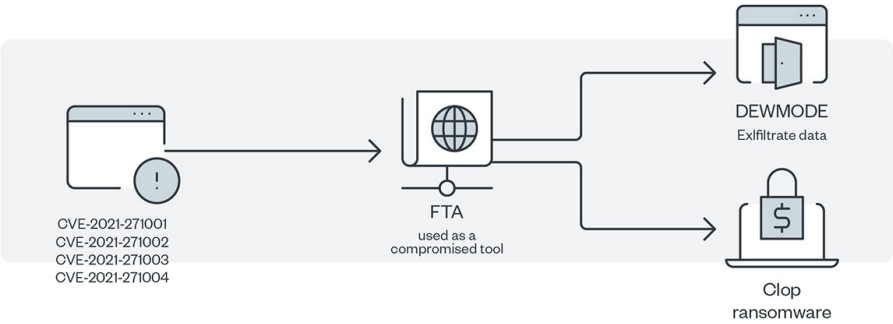
Figure 8. The first infection chain of TA505

In January 2020, TA505 changed the flow of infection by using SDBOT alone to collect and exfiltrate data to the command-and-control (C&C;) server. Figure 9 shows the modified infection chain.



open on a new tab

Figure 9. The modified infection chain of TA505



open on a new tab

Figure 10. The infection chain of FIN11

Figure 10 shows the infection chain of FIN11's exploit of the multiple zero-day vulnerabilities in Kiteworks' FTA so that it could install a newly discovered web shell, DEWMODE. FIN11 then used this same web shell to exfiltrate data from the FTA and deliver the Clop ransomware as a payload.

Initial Access

The threat actors behind the Clop ransomware use an established network of affiliates to gain initial access and send a large volume of spear-phishing emails to employees of an organization to induce infection. The malicious actors use a compromised RDP to penetrate the system either by attempting to brute-force passwords or by exploiting some known vulnerabilities. The following are the Kiteworks FTA zero-day exploitsopen on a new tab that they used in early 2021:

- CVE-2021-27101 – SQL injection via a crafted host header
- CVE-2021-27102 – Operating system command execution via a local web service call
- CVE-2021-27103 – SSRF via a crafted POST request
- CVE-2021-27104 – Operating system command execution via a crafted POST request

The ransomware group was reported to have exploited the SolarWinds Serv-U product vulnerability tagged as CVE-2021-35211.

Discovery

Clop's ransomware toolkit contained several malware types to harvest information:

- FlawedAmmyy remote access trojan (RAT) collects information and attempts to communicate with the C&C; server to enable the download of additional malware components.
- After getting through the AD server, it will download an additional hacking tool, Cobalt Strike.
- SDBOT, another RAT, propagates the infection in many ways, including exploiting vulnerabilities and dropping copies of itself in removable drives and network shares. It is also capable of propagating when shared through peer-to-peer (P2P) networks. Malicious actors use SDBOT as a backdoor to enable other commands and functions to be executed in the compromised computer.

Lateral Movement, Discovery, and Defense Evasion

At this stage, the malware scans for the workgroup information of the machine to distinguish personal machines from enterprise ones. If the workgroup is the default by value, the malware will stop malicious behavior and delete itself. If the AD server domain is returned, a machine gets classified as a corporate machine. The malware attempts to hack the AD server using Server Message Block (SMB) vulnerabilitiesopen on a new tab and using the added downloaded hacking tool

Cobalt Strike. Cobalt Strike is a known tool for post-exploitation that has been previously connected to other ransomware families. Meanwhile, TinyMet is used to connect the reverse shell to the C&C; server. The AD server admin account is used to propagate the Clop ransomware to internal network machines. As for SDBOT, it uses application shimming to preserve the continuity of the attack and to avoid detection.

Exfiltration

One attack was observed as using DEWMODE to exfiltrate stolen data.

Impact

The ransomware payload that terminates various Windows services and processes proceeds to its encryption routine.

Additional insights

In the course of monitoring the Clop ransomware group's activity over the years, we observed that it follows a distinct attack chain or flow: As the attacks on both Accellion FTA and GoAnywhere, as well as the more recent incidents involving the MOVEit zero-day vulnerability show, the ransomware group focuses on finding zero-day vulnerabilities on third-party file transfer applications.

Based on its recent activity, the Clop ransomware group prefers abusing these vulnerabilities to gain initial access, exfiltrate data, and fultimately, deliver its ransomware payload.

In some cases, Clop delivers its payload using tools and malware in its arsenal. Recently, however, the ransomware group appears to be focusing on data breach and extortion.

In January 2020, TA505 changed the flow of infection by using SDBOT alone to collect and exfiltrate data to the command-and-control (C&C;) server. Figure 9 shows the modified infection chain.

MITRE tactics and techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral Movement	Collection
T1566.001 - Phishing: Spear-phishing attachment *Arrives via phishing emails that have Get2 Loader, which will download the SDBot and FlawedAmmy RAT* **T1190** - Exploit public-facing application *Arrives via any the following exploits:• CVE-2021-27101• CVE-2021-27102• CVE-2021-27103• CVE-2021-27104•*	**T1106** - Native API *Uses native API to execute various commands/routines* **T1059** - Command and scripting interpreter *Uses various scripting interpreters like PowerShell, Windows command shell and Visual Basic (macro in documents)* **T1204** - User execution*User execution is needed to carry out the payload from the spear-phishing link/attachments*	**T1547** - Boot or logon autostart execution *Creates registry run entries to execute the ransomware as a service* **T1543.003** - Create or modify system process: Windows service *Creates a service to execute the ransomware*	**T1484.001** - Domain Policy modification: Group Policy modification *Uses stolen credentials to access the AD servers to gain administrator privilege and attack other machines within the network* **T1068** - Exploitation for privilege escalation *Makes use of CVE-2021-27102 to escalate privilege* **T1574** - Hijack	**T1036.001** - Masquerading: invalid code signature *Makes use of the following digital signatures:• DVERI• FADO• TOV* **T1562.001** - Impair defenses: disable or modify tools *Disables security-related software by terminating them* **T1140** - Deobfuscate/Decode files or information *The tool used for exfiltration has a part of its malware trace removal, and it drops a base-64 encoded file.* **T1070.004** - Indicator removal on host: file deletion *Deletes traces of*	**T1083** - File and directory discovery *Searches for specific files and the directory related to its encryption* **T1018** - Remote system discovery *Makes use of tools for network scans* **T1057** - Process discovery *Discovers certain processes for process termination* **T1082** - System information discovery *Identifies*	**T1570** - Lateral tool transfer *Can make use of RDP to transfer the ransomware or tools within the network* **T1021.002** - Remote services: SMB/Windows admin shares *Drops a copy of the payload to the compromised AD and then create a service on the target machine to execute the copy of the payload*	**T1005** - Data from local system *Might make use of RDP to manually search for valuable files or information*

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral Movement	Collection
CVE-2021-35211• CVE-2023-34362• CVE-2023-27350• CVE-2023-0669• CVE-2023-27351 **T1078** - Valid accounts *Have been reported to make used of compromised accounts to access victims via RDP*			execution flow *UAC bypass*	*itself in the infected machine* **T1055.001** - Process injection: DLL injection *To deliver other tools and payload, a tool has the capability to inject its downloaded payload.* **T1202** - Indirect command execution *A startup script runs just before the system gets to the login screen via startup registry.* **T1070.001** - Indicator removal on host: clear Windows event logs *Clears the Event Viewer log files*	*keyboard layout and other system information* **T1012** - Query registry *Queries certain registries as part of its routine* **T1063** - Security software discovery *Discovers security software for reconnaissance and termination*		

Summary of malware, tools, and exploits used

Security teams can watch out for the presence of the following malware tools and exploits that are typically used in Clop attacks:

Initial Entry	Execution	Discovery	Privilege Escalation	Lateral Movement	Command and Control	Defense Evasion

• Phishing emails
• Exploits:
  ◦ CVE-2021-27101
  ◦ CVE-2021-27102
  ◦ CVE-2021-27103
  ◦ CVE-2021-27104
  ◦ CVE-2021-35211
  ◦ CVE-2023-34362
  ◦ CVE-2023-27350
	• Get2 Loader	• FlawedAmmyy RAT
		• SDBOT
			• CVE-2021-27102	• RDP
				• Cobalt Strike
					• TinyMet	• SDBOT
						  ◦ Uses application shimming to maintain continuity of the attack and to avoid detection
						• Active Directory Server Admin Account
						  ◦ New account creation to propagate the payload throughout the network

Initial Entry	Execution	Discovery	Privilege Escalation	Lateral Movement	Command and Control	Defense Evasion
◦ CVE-2023-0669 ◦ CVE-2023-27351						

Recommendations

Despite arrests of alleged members of the Clop ransomware cartel in Ukraine in 2021, our detections of this ransomware indicate that the group is still a potential threat and might strike anytime. Moreover, the operators behind Clop are known to regularly change their TTPs, which means that expecting them to sharpen the proverbial saw is par for the course. It is therefore best to stay vigilant and armed with the knowledge that ransomware operators are always waiting for a chance to pounce on their next victim.

To protect systems against similar threats, organizations can establish security frameworks that allocate resources systematically for establishing a strong defense strategy against ransomware.

Here are some best practices that organizations can consider:

Audit and inventory

- Take an inventory of assets and data.
- Identify authorized and unauthorized devices and software.
- Make an audit of event and incident logs.

Configure and monitor

- Manage hardware and software configurations.
- Grant admin privileges and access only when necessary to an employee's role.
- Monitor network ports, protocols, and services.
- Activate security configurations on network infrastructure devices such as firewalls and routers.
- Establish a software allowlist that only executes legitimate applications.

Patch and update

- Conduct regular vulnerability assessments.
- Perform patching or virtual patching for operating systems and applications.
- Update software and applications to their latest versions.
- To prevent attacks like the Kiteworks FTA exploits, update to and patch the latest version of the FTA to clear the zero-day vulnerabilities that were released by the malicious actors and dedicated to the attack signatures.

Protect and recover

- Implement data protection, backup, and recovery measures.
- Enable multifactor authentication (MFA).

Secure and defend

- Employ sandbox analysis to block malicious emails.
- Deploy the latest versions of security solutions to all layers of the system, including email, endpoint, web, and network.
- Detect early signs of an attack such as the presence of suspicious tools in the system.
- Use advanced detection technologies such as those powered by AI and machine learning.

Train and test

- Regularly train and assess employees on security skills.
- Conduct red-team exercises and penetration tests.

A multilayered approach can help organizations guard the possible entry points into the system (endpoint, email, web, and network). Security solutions that detect malicious components and suspicious behavior could also help protect enterprises.

- Trend Vision One™products enables security teams to continuously identify the attack surface, including known, unknown, managed, and unmanaged cyber assets. It automatically prioritizes risks, including vulnerabilities, for remediation, taking into account critical factors such as the likelihood and impact of potential attacks. Vision One offers comprehensive prevention, detection, and response capabilities backed by AI, advanced threat research, and intelligence. This leads to faster mean time to detect, respond, and remediate, improving the overall security posture and effectiveness.
- Trend Micro Cloud One™ Workload Securityproducts protects systems against both known and unknown threats that exploit vulnerabilities. This protection is made possible through techniques such as virtual patching and machine learning.
- Trend Micro™ Deep Discovery™ Email Inspectorproducts employs custom sandboxing and advanced analysis techniques to effectively block malicious emails, including phishing emails that can serve as entry points for ransomware.
- Trend Micro Apex One™products offers next-level automated threat detection and response against advanced concerns such as fileless threats and ransomware, ensuring the protection of endpoints.

Indicators of Compromise (IOCs)

HIDE

Like it? Add this infographic to your site:

1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

We Recommend

-
-
-
-

- The Industrialization of Botnets: Automation and Scale as a New Threat Infrastructurenews article
- Complexity and Visibility Gaps in Power Automatenews article
- Cracking the Isolation: Novel Docker Desktop VM Escape Techniques Under WSL2news article
- Azure Control Plane Threat Detection With TrendAI Vision One™news article
- The AI-fication of Cyberthreats: Trend Micro Security Predictions for 2026predictions
- Ransomware Spotlight: DragonForcenews article
- Stay Ahead of AI Threats: Secure LLM Applications With Trend Vision Onenews article
- The Road to Agentic AI: Navigating Architecture, Threats, and Solutionsnews article

---