Ransomware Spotlight: Clop

trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-clop

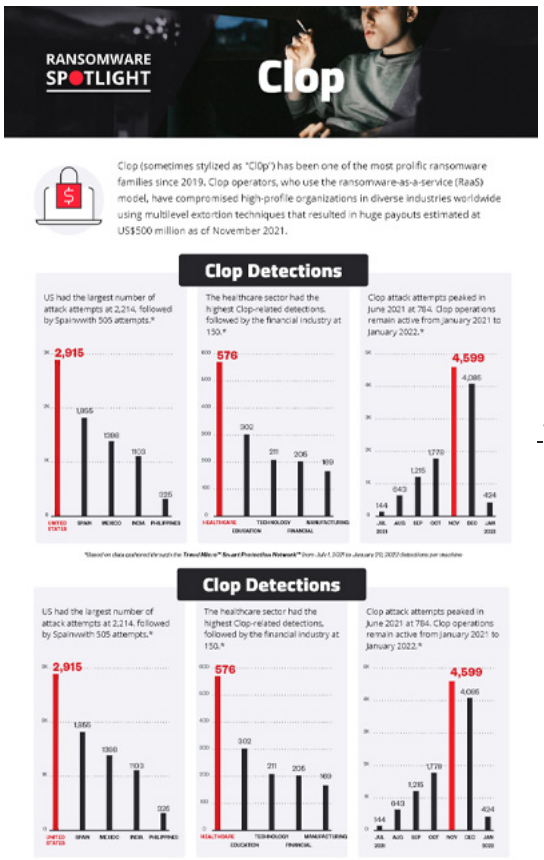
X

RANSOMWARE SPOTLIGHT

Clop

By Trend Micro Research

We take a closer look at the operations of Clop, a prolific ransomware family that has gained notoriety for its high-profile attacks. We review this ransomware group's constantly changing schemes and discuss how companies can shore up defenses against this threat.



View infographic of "Ransomware Spotlight: Clop"

Clop (sometimes stylized as "Cl0p") has been one of the most prolific ransomware families in the past three years. It has gained infamy for compromising high-profile organizations in various industries worldwide using multilevel extortion techniques that resulted in huge payouts estimated at US$500 million as of November 2021. In concerted efforts to dismantle ransomware cartels, a global coalition across five continents that involved law enforcement and private partners led to the arrests in Ukraine of six suspected Clop members in June 2021.

While the arrests in Ukraine might have dealt a big blow to Clop's operations, the group's criminal activities have gone unabated: Our detections of attack attempts showed non-stop malicious activities from January 2021 to January 2022. Reports mentioned that only parts of the ransomware's operations, such as the server infrastructure used by affiliates to disseminate the malware and the channels used to launder cryptocurrency ransom payments that were illegally obtained, were seized and taken down, respectively.

As enterprises ponder on ways to bolster their security defenses in the post-pandemic era, learning more about potential threats is essential to adopting a proactive cybersecurity approach. In this report, we focus the spotlight on the notorious Clop ransomware's operations.

History of Clop

Clop evolved as a variant of the CryptoMix ransomware family. In February 2019, security researchers discovered the use of Clop by the threat group known as TA505 when it launched a large-scale spear-phishing email campaign. Clop is an example of ransomware as a service (RaaS) that is operated by a Russian-speaking group. Additionally, this ransomware used a verified and digitally signed binary, which made it look like a legitimate executable file that could evade security detection.

In 2020, it was reported that FIN11 — a financially motivated hacking group — deployed Clop ransomware and threatened their victims to publish exfiltrated data. FIN11 exploited zero-day vulnerabilities in the legacy file transfer appliance (FTA) of Kiteworks (formerly known as Accellion) to infiltrate the network of the victims. It then aimed to deliver the Clop ransomware as its payload and steal data as well. Researchers also discovered that the group used a specific web shell that was referred to as "DEWMODE" to exfiltrate stolen information from its victims.

Researchers found two groups of malicious actors that have known connections to FIN11 and identified them as UNCA2546 and UNCA2582. These were also the groups responsible for the massive attacks on Kiteworks users.

The operators behind Clop made their first attempt at using the double extortion scheme in April 2020 when they publicized the data of a pharmaceutical company on their leak site. Clop's dedicated leak site hosts its list of victims, which has markedly grown since its launch. Over time, the gang's extortion tactics have become more sophisticated and thus more destructive.

In November 2021, security researchers detected malicious activity by Clop operators that exploited a SolarWinds Serv-U vulnerability to breach corporate networks and deliver the Clop ransomware as a payload. The Serv-U Managed File Transfer and Serv-U Secure FTP remote code execution (RCE) vulnerability, tracked as CVE-2021-35211, allowed RCE on the vulnerable server with elevated privileges.

A maritime services giant with headquarters in Singapore also fell prey to Clop. In November 2021, it was reported that Clop breached its IT systems to steal classified proprietary commercial information and employee data that included bank account details, payroll information, passports, email addresses, and internal correspondence, among others.

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 payload 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 techniques, which have involved going after top executives and customers 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 2021. A report 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.

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 the US had the largest number of attack attempts at 2,214 followed by Spain at a distant second with 505 attempts. The rest of the detections are spread across North America, South America, Asia Pacific, Europe, and the Middle East.

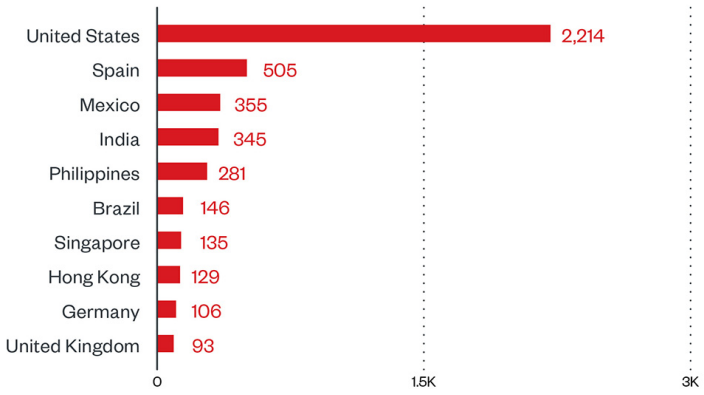


Figure 1. 10 countries with the highest number of attack attempts per machine for the Clop ransomware (January 1, 2021 to January 31, 2022)

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 this sector received the highest number of detections at 959, followed by the financial industry at 150. Figure 2 shows the breakdown of detections according to industry.

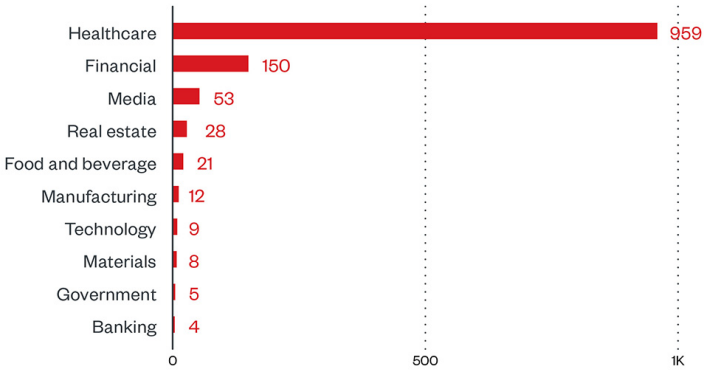


Figure 2. 10 industries with the highest number of attack attempts per machine for the Clop ransomware (January 1, 2021 to January 31, 2022)
Source: Trend Micro Smart Protection Network infrastructure

By breaking down the detections per month, we are able to determine that 2021 saw the peak of Clop attacks in June of the same year at 784 attack attempts. March also saw a steep rise in attempts at 663, which was significantly higher than the detections in prior months. Our detections suggest that Clop operations have remained robust as numbers consistently straddled the 300 to 400 range from July 2021 to January 2022.

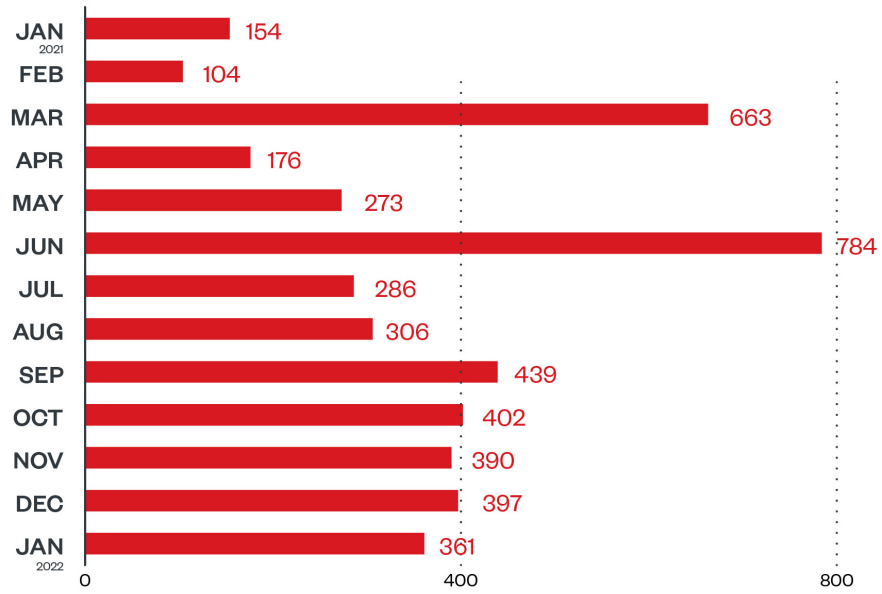


Figure 3. Monthly breakdown of detections per machine for the Clop ransomware (January 1, 2021 to January 31, 2022)
Source: Trend Micro Smart Protection Network infrastructure

We also looked into Clop's leak site to gain insights into the operators' successful attacks from December 16, 2021 to January 15, 2022. During this period, only two organizations — both small businesses — were successfully compromised by Clop operators. One organization belongs to the legal sector, while the other belongs to the fashion and apparel sector. Both organizations are based in North America, and as observed in the aforementioned period, have yet to pay ransom.

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.

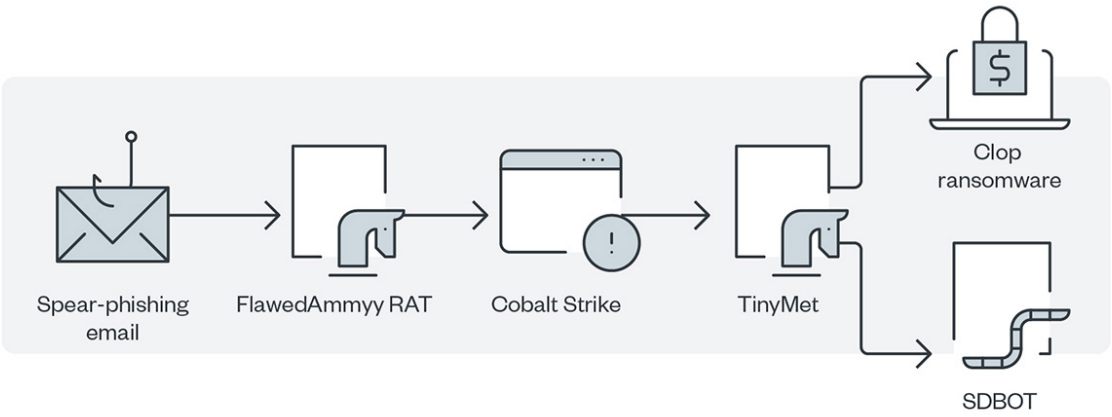


Figure 4. The first infection chain of TA505

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 5 shows the modified infection chain.

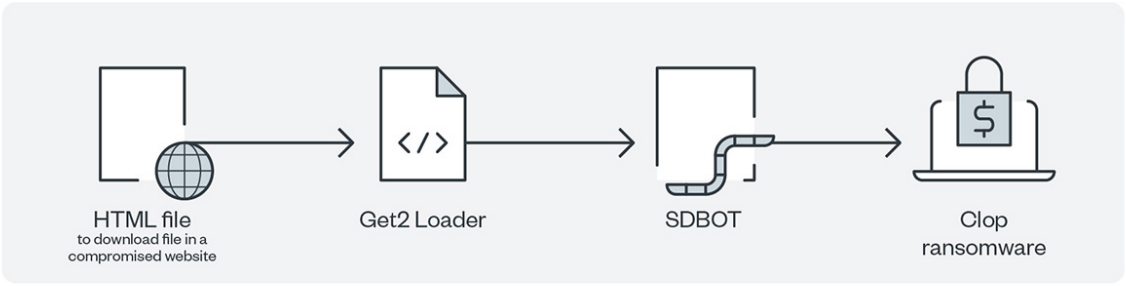


Figure 5. The modified infection chain of TA505

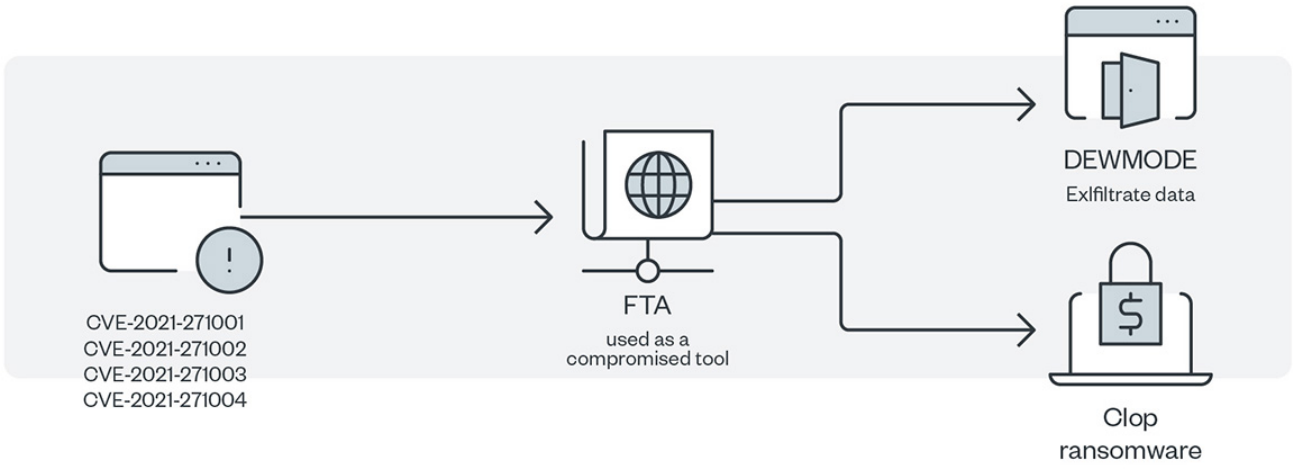


Figure 6. The infection chain of FIN11

Figure 6 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 exploits 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) vulnerabilities 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.

MITRE tactics and techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral Movement	Collection

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• CVE-2021-35211* **T1078** - Valid accounts *Have been reported to make used of compromised accounts to access victims via RDP*	**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 execution flow *UAC bypass*	**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 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*	**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 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*	**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*

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	Exfiltration

Initial Entry	Execution	Discovery	Privilege Escalation	Lateral Movement	Command and Control	Defense Evasion	Exfiltration
• Phishing emails • Exploits: ◦ CVE-2021-27101 ◦ CVE-2021-27102 ◦ CVE-2021-27103 ◦ CVE-2021-27104 ◦ CVE-2021-35211	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	DEWMODE

Recommendations

Despite last year's arrests of alleged members of the Clop ransomware cartel in Ukraine, 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 Micro Vision One™ provides multilayered protection and behavior detection, which helps block questionable behavior and tools early on before the ransomware can do irreversible damage to the system.
- Trend Micro Cloud One™ Workload Security 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 Inspector 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™ 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)

The IOCs for this article can be found here. Actual indicators might vary per attack.

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.