

Threat Assessment: Clop Ransomware

unit42.paloaltonetworks.com/clop-ransomware/

Doel Santos

April 13, 2021

By [Doel Santos](#)

April 13, 2021 at 8:00 AM

Category: [Malware](#), [Ransomware](#), [Unit 42](#)

Tags: [Clop](#), [Cybercrime](#), [ransomware threat report](#), [threat assessment](#)



This post is also available in: [日本語 \(Japanese\)](#).

Executive Summary

Unit 42 researchers have observed an uptick in [Clop](#) ransomware activity affecting the wholesale and retail, transportation and logistics, education, manufacturing, engineering, automotive, energy, financial, aerospace, telecommunications, professional and legal services, healthcare and high tech industries in the U.S., Europe, Canada, Asia Pacific and Latin America. Clop also leverages double extortion practices and hosts a leak site, where the number of victims has grown significantly since its launch in March 2020. Clop has been commonly observed being delivered as the final-stage payload of a malicious spam

campaign carried out by the financially motivated actor TA505. This ransomware has also been linked to threat actors behind the recent global zero-day attacks on users of the Acellion File Transfer Appliance (FTA) product.

Due to the surge of this malicious activity, we've created this threat assessment for overall threat awareness. Full visualization of the techniques observed and their relevant courses of action can be viewed in the Unit 42 ATOM Viewer.

Clon Ransomware Overview

Clon ransomware is a variant of a previously known strain called CryptoMix. In 2019, Clon was delivered as the final payload of a phishing campaign associated with the financially motivated actor TA505. The threat actors would send phishing emails that would lead to a macro-enabled document that would drop a loader named Get2. This loader can download different tools used by this group, such as SDBot, FlawedAmmy or FlawedGrace. After the threat actors obtain the initial foothold on the system, they start employing reconnaissance, lateral movement and exfiltration techniques to prepare the ransomware deployment. SDBot has been observed delivering Clon as the final payload.

After the ransomware is executed, Clon appends the .clon extension to the victim's files. We have observed different variants using different extensions, such as “.ClIp”, “.ClIp” and “.C_L_O_P”. Different versions of the ransom note have also been observed after encryption. Depending on the variant, any of these ransom text files could drop: “ClonReadMe.txt”, “README_README.txt”, “ClonReadMe.txt” and “READ_ME_!!!.TXT”.

This ransomware includes various features to avoid detection. Observed Clon samples try to kill several processes and services related to backups and security solutions. It won't execute if it detects it's running in a virtual environment. Clon also leverages Code Signing to evade detection. We observed the use of two signers during our research, as shown below in Figure 1.

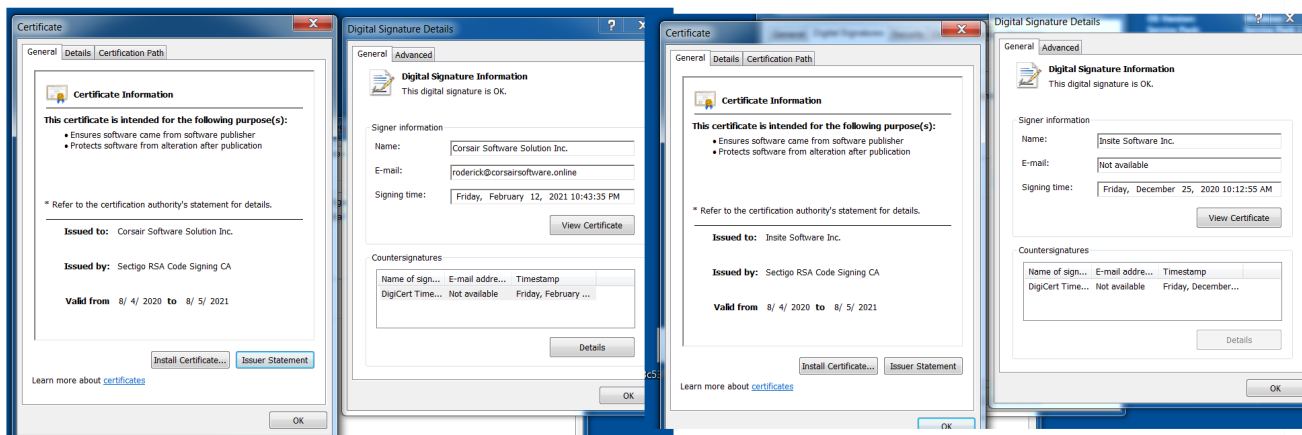


Figure 1. Observed Clon digital signers.

Clop went from being ransomware delivered through malicious spam to being used in targeted campaigns against high-profile companies. In recent events, Clop has been linked to threat actors who have been exploiting Accellion File Transfer Appliance (FTA) vulnerabilities: [CVE-2021-27101](#), [CVE-2021-27102](#), [CVE-2021-27103](#) and [CVE-2021-27104](#). The exploitation of these vulnerabilities led to the compromise of high-profile companies starting in February. Additionally, there has been evidence of an affiliate using a webshell named DEWMODE that was being used to steal data from Accellion FTA devices. Not long after compromise, victims affected by DEWMODE began receiving emails from threat actors announcing the breach with a unique URL per victim to start negotiation efforts. If ignored, the threat actors would reach out again with an ultimatum of releasing the data to “Clop^_- Leaks”.

Clop didn't have a leak site when it was first sighted back in February 2019. It was in March 2020 when the threat actors decided to launch a leak site titled, “Clop^_- Leaks” (Figure 2). This website is a Tor-based blog site, where victims who don't pay the ransom or ignore threats have their confidential data publicly exposed. The threat actors behind Clop also leverage a variety of extortion techniques, such as targeting workstations of top executives, “doxxing” employees and advertising their breaches to reporters.

The screenshot shows a dark-themed website with the following elements:

- Navigation:** A top bar with the title ">_ CLOP^_- LEAKS" and two menu items: "HOME" and "HOW TO DOWNLOAD?".
- Updates List:** A vertical list of entries, each consisting of a redacted name followed by "FILES PARTX PUBLISHED". The parts listed are PART6, PART2, PART5, PART9, PART1, PART4, PART8, PART8, PART4, PART3, PART7, PART7, PART4, and PART2.
- Main Text Area:**
 - Starts with "====" and "ATTENTION!!!".
 - Contains a warning: "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."
 - Followed by another "====" and the heading "Imagine a situation".
 - Contains a detailed scenario: "You are the owner of a large business, you have a company revenue of 1 million - 100 billion and more. Thousands or hundreds of thousands of employees, large staff of IT specialists. Everything is good for you, you make a profit, commercial success! Your colleagues call you at night and tell you that all the servers and workstations of your company are not working! All files are encrypted without the ability to decrypt, the company stopped, can not serve customers! All your employees can't even log in to a Windows account on a computer! One hour of company downtime costs you thousands or hundreds of thousands dollars. Your actions? Imagine a problem? Do you feel goosebumps on body? If you feel - then presented, if you did not feel go-count in numbers, attract a consultant".
 - Section "From personal experience we can tell you:" with text: "All companies have security holes, regardless of size infrastructure, the number of IT specialists, the number of antivirus and monitoring systems. A very small percentage of companies that are really at the highest level of security. At the same time, companies with 100+ thousand servers and computers allow primitive erred in administration Which allow one person to destroy your business in 5 hours of work but you have been building it many years. This is exactly moment when you got the call at night! This is exactly what we been doing for many years!".
 - Text: "Now take a deep breath through your nose breathe out..."
 - Section "We can help you avoid this situation!" with text: "We can't guarantee that no one will hack you! But we can guarantee you that your specialists will close the holes that contribute to penetration and distribution Invest in the knowledge of your network administrators or suffer losses from not knowing they them! We can offer you instructions.txt - 250000\$ in BTC. E-mail: unlock@support-box.com OR unlock@support-iron.com. If you are interested in detailed logs and files of any companies, we have - write to us".

Figure 2. Clop leak site and sample instructions delivered by Clop operators detailing how to improve security posture and close security holes – for a price.

More information on ransomware and victimology can be found in the [2021 Unit 42 Ransomware Threat Report](#).

Courses of Action

This section documents relevant tactics, techniques and procedures (TTPs) used with Clop and maps them directly to Palo Alto Networks product(s) and service(s). It also further instructs customers on how to ensure their devices are configured correctly.

Product / Service	Course of Action
Initial Access, Exfiltration, Defense Evasion, Execution	
Exploit Public-Facing Application [T1190], Exfiltration Over C2 Channel [T1041], Spearphishing Attachment [T1566.001], Code Signing [T1553.002], Windows Command Shell [T1059.003]	
NGFW	Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone
Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist	
Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources Exists	
Set up File Blocking	
Threat Prevention [†]	Ensure a Vulnerability Protection Profile is set to block attacks against critical and high vulnerabilities, and set to default on medium, low and informational vulnerabilities
Ensure a secure Vulnerability Protection Profile is applied to all security rules allowing traffic	
Ensure that antivirus profiles are set to block on all decoders except 'imap' and 'pop3'	
Ensure a secure antivirus profile is applied to all relevant security policies	
Ensure an anti-spyware profile is configured to block on all spyware severity levels, categories and threats	
Ensure DNS sinkholing is configured on all anti-spyware profiles in use	

Ensure passive DNS monitoring is set to enabled on all anti-spyware profiles in use	
Ensure a secure anti-spyware profile is applied to all security policies permitting traffic to the internet	
DNS Security†	Enable DNS Security in Anti-Spyware profile
URL Filtering†	Ensure that URL Filtering is used
Ensure that URL Filtering uses the action of 'block' or 'override' on the <enterprise approved value> URL categories	
Ensure that access to every URL is logged	
Ensure all HTTP Header Logging options are enabled	
Ensure secure URL Filtering is enabled for all security policies allowing traffic to the internet	
WildFire†	Ensure that WildFire file size upload limits are maximized
Ensure forwarding is enabled for all applications and file types in WildFire file blocking profiles	
Ensure a WildFire Analysis profile is enabled for all security policies	
Ensure forwarding of decrypted content to WildFire is enabled	
Ensure all WildFire session information settings are enabled	
Ensure alerts are enabled for malicious files detected by WildFire	
Ensure 'WildFire Update Schedule' is set to download and install updates every minute	
Cortex XSOAR	Deploy XSOAR Playbook - Isolate Endpoint - Generic
Deploy XSOAR Playbook - Block IP	
Deploy XSOAR Playbook - Block URL	

Deploy XSOAR Playbook - Hunting and Threat Detection Playbook	
Deploy XSOAR Playbook - PAN-OS Query Logs for Indicators	
Deploy XSOAR Playbook - Phishing Investigation - Generic V2	
Deploy XSOAR Playbook - Endpoint Malware Investigation	
Cortex XDR	Enable Anti-Exploit Protection
Enable Anti-Malware Protection	
Discovery	
File and Directory Discovery [T1083], Process Discovery [T1057]	
Cortex XDR	Look for the following BIOC alerts to detect activity*: Cortex XDR Analytics - Multiple Discovery Commands
Impact	
Data Encrypted for Impact [T1486], Inhibit System Recovery [T1490], Service Stop [T1489]	
Cortex XSOAR	Deploy XSOAR Playbook - Ransomware Manual
Cortex XDR	Look for the following BIOC alerts to detect activity*: Manipulation of Volume Shadow Copy configuration Cortex XDR Agent - Behavioral Threat Detected

Table 1. Courses of Action for Clop ransomware.
*These analytic detectors will trigger automatically for Cortex XDR Pro customers.

Conclusion

Clop ransomware is a high-profile ransomware family that has compromised industries globally. Organizations should be aware of SDBot, used by TA505, and how it can lead to the deployment of Clop ransomware. Like many other current ransomware families, Clop hosts a leak site to create additional pressure and shame victims into paying the ransom.

Indicators associated with this Threat Assessment are available on [GitHub](#), have been published to the [Unit 42 TAXII](#) feed and are viewable via the ATOM Viewer.

In addition to the above courses of action, AutoFocus customers can review additional activity by using the tag [Clop](#).

Additional Resources

Palo Alto Networks has shared our findings, including file samples and indicators of compromise, in this report with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. For more information on the Cyber Threat Alliance, visit www.cyberthreatalliance.org.

**Get updates from
Palo Alto
Networks!**

Sign up to receive the latest news, cyber threat intelligence and research from us

By submitting this form, you agree to our [Terms of Use](#) and acknowledge our [Privacy Statement](#).