HC3: Analyst Note
January 04, 2023 TLP:CLEAR Report: 202301041300

Clop Ransomware

Executive Summary

Clop operates under the Ransomware-as-service (RaaS) model, and it was first observed in 2019. Clop was a highly used ransomware in the market and typically targeted organizations with a revenue of $5 million U.S. Dollars (USD) or higher. Since its appearance, HC3 is aware of attacks on the Health and Public Health (HPH) sector. The HPH sector has been recognized as being a highly targeted industry for the Clop ransomware.

Report

Clop ransomware, also written as ClOp, was first observed in February 2019 and the operators have seen very large payouts of up to $500 million USD. Clop is the successor of the CryptoMix ransomware, which is believed to have been developed in Russia and is a popular payload for groups such as FIN11 and other Russian affiliates. Like most ransomware groups, financial gain appears to be their primary goal, which they leverage through the use of the double extortion model. Through this technique the threat actor will encrypt and exfiltrate sensitive information. Sensitive data will be released on their dark web leak site if payment is not made. This model is used so the actor can have additional leverage to help collect a ransom payment.

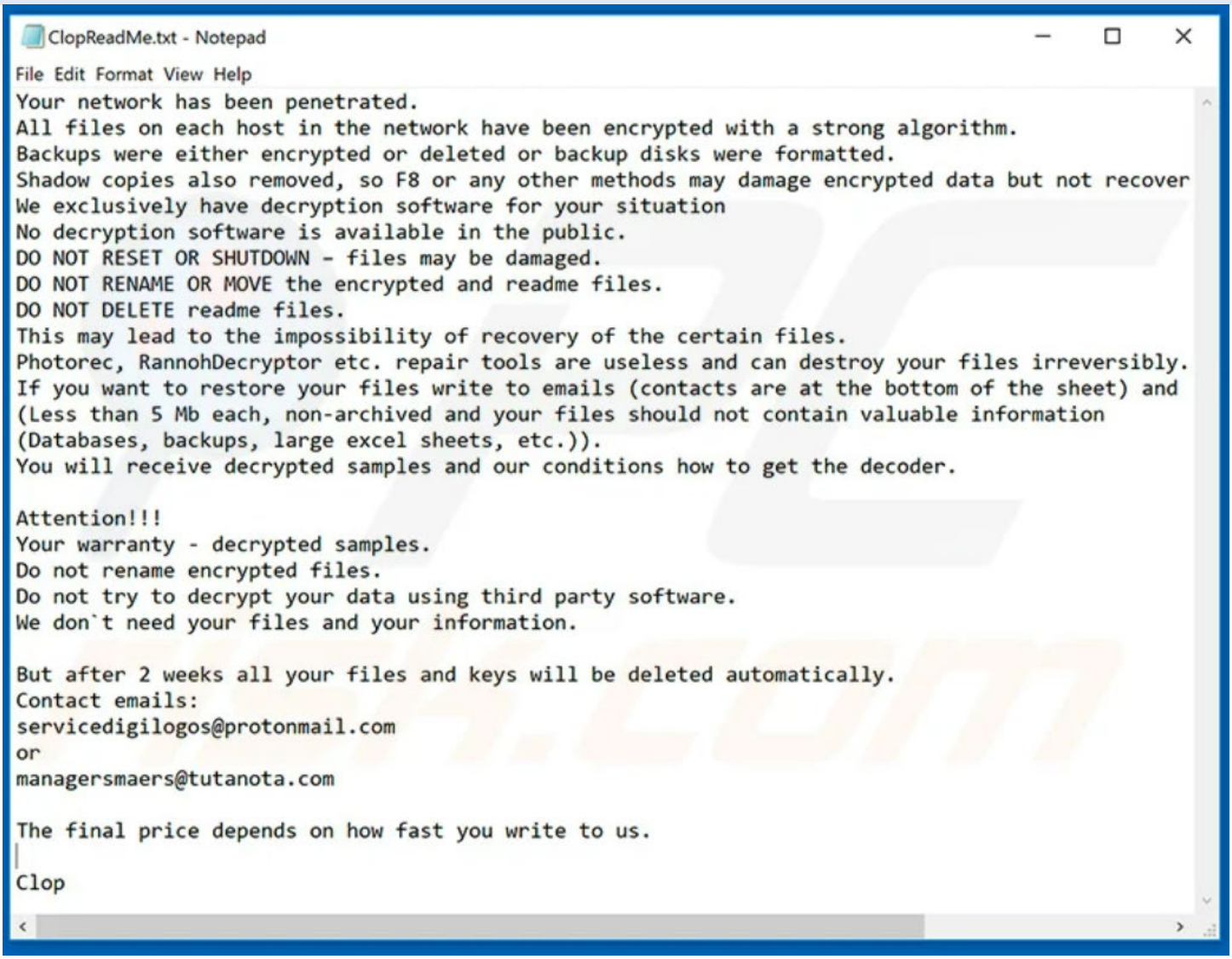
The appearance of Clop ransomware was expected to decline in 2021 after the arrest of six ransomware operators. However, the malware continued to have non-stop activity through 2022. Additionally, it has been observed to be a potential payload from the downloader malware, TrueBot. Clop is designed to have not only have anti-analysis capabilities but also anti-virtual machine analysis to help prevent further investigations in an emulated environment.

Clop was written to target Windows systems, and some reporting samples showcase that it is a Win32 executable written in C++. The executable packet is compressed, which helps hide its functionality. The ransomware encrypts files with an RSA 1024-bit public key with RC4 that uses 117 bytes of the public key. Phishing emails have been a primary initial access vector for Clop, but reports have shown that it also exploits the following Common Vulnerabilities and Exposures (CVE): CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, CVE-2021-27104, and CVE-2021-35211.

Once a network has been compromised, they have been observed to use remote desktop protocols and deploying Cobalt Strike to aid in lateral movement. Finally, after encryption is complete, the victim will be able to access a dropped **README.TXT**, and the encrypted file's extension will be changed to 'Clop'. In the ransom note, it states that the Shadow Volume Copies have been deleted and the decryption key is only available from the group, along with claiming that all the files will be deleted after two weeks have passed.

HC3: Analyst Note

January 04, 2023 TLP:CLEAR Report: 202301041300



Source: pcrisk

Analyst Comment

The Clop ransomware has been around since 2019, and even though the organization had several members arrested, its activity appeared to be uninterrupted. However, the gang has had difficulties getting victims to payout on a ransom which has reportedly lead to a change in their tactics that directly impacts the HPH sector. The group has been infecting files that are disguised to look like medical documents, submitting them to facilities, and then requesting a medical appointment in hopes of those malicious documents being opened and reviewed beforehand. These attacks have a higher chance of working due to conditions from COVID-19 expansion in the telehealth environment.

Outside of the techniques addressed in this report, HC3 continues to see the following attack vectors frequently associated with ransomware:

- Phishing
- Remote Desktop Protocol Compromises and credential abuse

- Compromises of exploilted vulnerabilities, such as VPN servers
- Compromises in other known vulnerabilities

The following sources contain indicators of compromise:

- Ransomware Spotlight: Clop - Security News (trendmicro.com)
- Clop Ransomware - AlienVault - Open Threat Exchange
- https://sequretek.com/wp-content/uploads/2018/10/Sequretek-Advisory-Clop-Ransomware_.pdf

References

Davis, Jessica. "Clop ransomware group targeting provider-patient trust by infecting medical images". SCmagazine. Dec 20, 2022. https://www.scmagazine.com/analysis/ransomware/clop-ransomware-group-targeting-provider-patient-trust-by-infecting-medical-images

"CLOP Poses Ongoing Risk to HPH Organizations". HC3. March 23, 2021. 202103231400_Analyst_Note_CLOP_TLP_WHITE (hhs.gov)

"Threat Thursday: CryptoMix Clop Ransomware". Blackberry. July 15, 2021. https://blogs.blackberry.com/en/2021/07/threat-thursday-cryptomix-clop-ransomware

"New Ransom Payment Schemes Targets Executives, Telemedicine". Krebsonsecurity. Dec 08, 2022. New Ransom Payment Schemes Target Executives, Telemedicine – Krebs on Security

Paganini, PierLuigi. "TrueBot Infections were Observed in Clop Ransomware Attacks". Securityaffairs. Dec 12, 2022. TrueBot infections were observed in Clop ransomware attacks Security Affairs

Toulas, Bill. "Clop Ransomware uses TrueBot malware for access to networks". Bleepingcomputer. Dec 11, 2022. Clop ransomware uses TrueBot malware for access to networks (bleepingcomputer.com)

"Ransom.CryptoMix". Malwarebytes. Ransom.Cryptomix (malwarebytes.com)

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback