HC3: Analyst Note
November 21, 2022 TLP:CLEAR Report: 202211211700

Lorenz Ransomware

Executive Summary
Lorenz is human-operated ransomware that has been in operation for approximately two years. In that time, HC3 is aware of the compromise of healthcare and public sector targets. It is used to target larger organizations in what is called "big-game hunting", and publishes data publicly as part of pressuring victims in the extortion process. Lorenz is known to target organizations globally using customized code, and can demand hundreds of thousands of dollars in ransoms.

Report
Lorenz ransomware was first observed in February of 2021. Lorenz is believed to be related to sZ40 ransomware (first observed in October 2020) and ThunderCrypt ransomware (first observed in May of 2017). One of the indications of the similarities is the use of encryptors – Lorenz uses the same encryptor as ThunderCrypt, which could indicate operations by the same group, or a purchase or theft of code.

Lorenz is human-operated ransomware, run by operators known to be customize their executable code, tailoring it for their targets. This implies that they may maintain persistent access for reconaissance purposes for some extended period of time prior to ransomware deployment. They often follow the pattern of initial access, followed by reconaissance and lateral movement, ultimately seeking a Windows domain controller in search of administrator credentials.

Some research suggests the ransomware code is written in C++ using Microsoft Visual Studio 2015. Upon execution, Lorenz has been observed executing a file named ScreenCon.exe possibly from a compromised domain controller. Lorenz has also been observed creating a mutual exclusion object (mutex) called "wolf" as it executes, which allows multiple program threads to share resources. Specifically, wolf is intended to prevent multiple instances of Lorenz running concurrently. Lorenz has also been observed sending the name of the compromised system to a command-and-control server prior to encryption, in some cases via the TCP port 55. Files are encrypted in blocks of 48 bytes and are given the file extension ".Lorenz.sz40". Lorenz leverages a combination of RSA and AES-128 in CBC mode to encrypt files. Each encrypted file has a password generated at random and an encryption key generated with the CryptDeriveKey function. In one case, they were identified exploiting a vulnerability in the Mitel Service Appliance component of MiVoice Connect (CVE-2022-29499).

Lorenz ransom demands range from $500,000 to $700,000. It's only known to attack enterprise targets (as opposed to private users). Furthermore, it's known to target larger organizations in what is known as "big game hunting". Most of its victims appear to be English-speaking organizations. Lorenz runs a data leak site; however, their leaking process is non-typical. Upon becoming frustrated with a victim's unwillingness to pay, they first make the stolen data available for sale to other threat actors or competitors. If the victim continues to fail to pay, they will next release password protected RAR archives containing the victim data. Finally, if they fail to monetize the data – if the victim does not pay and the data does not sell, they will release the password for the full archives, so they will be publicly available for anyone to access. They have also been known to sell access to the victim network as well.

Analyst Comment
Relatively little is known about Lorenz as compared to many other ransomware operators. Several of the technical indicators previously identified could be used for detection, defense and mitigation, including

filenames, port numbers and tactics.

Furthermore, HC3 continues to see the following four categories of attack vectors frequently associated with ransomware operators:

- Phishing
- Compromise of known vulnerabilities
- Compromise of remote-access technologies, especially VPNs and RDP
- Distributed attacks, especially supply chain and Managed Service Provider compromise

Finally, the following source includes indicators of compromise:

- https://www.tesorion.nl/en/posts/lorenz-ransomware-analysis-and-a-free-decryptor/

References

Meet Lorenz — A new ransomware gang targeting the enterprise
https://www.bleepingcomputer.com/news/security/meet-lorenz-a-new-ransomware-gang-targeting-the-enterprise/

Lorenz ransomware: analysis and a free decryptor
https://www.tesorion.nl/en/posts/lorenz-ransomware-analysis-and-a-free-decryptor/

NoMoreRansomware: Lorenz
https://www.nomoreransom.org/en/decryption-tools.html#Lorenz

ID Ransomware: Lorenz (Russian)
https://id-ransomware.blogspot.com/2020/10/sz40-ransomware.html

Free decrypter available for Lorenz ransomware
https://therecord.media/free-decrypter-available-for-lorenz-ransomware/

This company was hit with ransomware, but didn't have to pay up. Here's how they did it
https://www.zdnet.com/article/this-company-was-hit-with-ransomware-but-didnt-have-to-pay-up-heres-how-they-did-it/

Chiseling In: Lorenz Ransomware Group Cracks MiVoice And Calls Back For Free
https://arcticwolf.com/resources/blog/lorenz-ransomware-chiseling-in/

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