Executive Summary

As an integral department in Cynet’s research team, Orion works around the clock to track threat intelligence resources, analyze payloads, and automate labs to ensure that our customers are protected against the newest ransomware variants. In these monthly reports, Orion reviews the latest trends identified in Bleeping Computer — the most up-to-date website that summarizes the newest ransomware variants — and shares how Cynet detects these threats.

The Week in Ransomware - December 23rd 2022 - Targeting Microsoft Exchange

Reports this week illustrate how threat actors consider Microsoft Exchange as a prime target for gaining initial access to corporate networks to steal data and deploy ransomware.

The Week in Ransomware - December 16th 2022 - Losing Trust

Today’s Week in Ransomware brings you the latest news and stories about the cyberattacks, new tactics, and reports related to ransomware operations.

The Week in Ransomware - December 9th 2022 - Wide Impact

This week has been filled with research reports and news of significant attacks having a wide impact on many organizations.

The Week in Ransomware - December 2nd 2022 - Disrupting Health Care

This week’s big news was the Colombia health system being severely disrupted by a ransomware attack on Keralta, one of the country’s largest healthcare providers.
Cynet 360 AutoXDR™ VS Ransomware
Medusa Locker Ransomware
• Observed since: late 2019
• Ransomware encryption method: AES + RSA
• Ransomware extension: .cipher
• Ransomware note: !-Recovery_instructions-!.html
• Sample hash: 8c0cc36cbaf54c1cc225c95ef8a05f9956317ffdb17e952452e6555a719a927

Cynet 360 AutoXDR™ Detections:

Medusa Locker Overview
Medusa Locker ransomware renames the encrypted files with “.cipher” in the extension:

Once a computer’s files have been encrypted and renamed, Medusa Locker drops a note named “!-Recovery_instructions-!.html”:

The ransomware note contains general information, warnings, and the attacker’s email address:
OBZ Ransomware
- Observed since: Dec 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .OBZ
- Ransomware note: ReadMe.txt
- Sample hash: 4cbd48893182071bbb2086732369b8ca73fb9fb027e63b20a9bc67568ab3521

Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains general information, warnings, and the attacker’s link to TOR:

Once a computer’s files have been encrypted and renamed, the ransomware drops a note named “ReadMe.txt”:
Lucknite Ransomware

- Observed since: June 2021
- Ransomware encryption method: AES + RSA
- Ransomware extension: .lucknite
- Ransomware note: README.txt
- Sample hash: 0f36909d803d00afa7ec5c925651bbf99064318d5e94db7994aa1d2a1815

Upon execution, it immediately encrypts the endpoint and drops the ransomware note.

The ransomware note contains general information, warnings, and the attacker’s wallet number (no decryption guaranteed):
HardBIT 2.0 Ransomware

- Observed since: Dec 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .hardbit2
- Ransomware note: How To Restore Your Files.txt
- Sample hash: a0138b24593483f50e76569856b6c6f77f7676ba37402639ad49ad2f6f2992

Once a computer’s files have been encrypted and renamed, HardBIT drops a note named “How To Restore Your Files.txt.”

Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains general information, warnings, and the attacker’s email address:
Thank you!

December, 2022