Contents

Payt ............................................................................................................................................................................. 5
Hydrox ............................................................................................................................................................................. 6
World2022decoding ......................................................................................................................................................... 7
Medusa ............................................................................................................................................................................ 8
VoidCrypt ....................................................................................................................................................................... 9
Executive Summary

As an integral department of Cynet’s research team, Orion works around the clock to track threat intelligence resources, analyze payloads and automate labs to protect customers 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 - August 26th 2022 - Fighting back
We saw a bit of ransomware drama this week, mostly centered around LockBit, who saw their data leak sites taken down by a DDoS attack after they started leaking the allegedly stolen Entrust data.

The Week in Ransomware - August 19th 2022 - Evolving extortion tactics
Bringing you the latest ransomware news, including new research, tactics, and cyberattacks. We also saw the return of the Blackbyte ransomware operation, who has started to use new extortion tactics.

The Week in Ransomware - August 12th 2022 - Attacking the defenders
It was a very busy week for ransomware news and attacks, especially with the disclosure that Cisco was breached by a threat actor affiliated with the Yanluowang ransomware gang.

The Week in Ransomware - August 5th 2022 - A look at cyber insurance
For the most part, it has been a quiet week on the ransomware front, with a few new reports, product developments, and attacks revealed.
Cynet 360 AutoXDR™ VS Ransomware
Payt Ransomware

- Observed since: Aug 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .Payt
- Ransomware note: ReadthisforDecode.txt
- Sample hash: 3a3c882946ba931c47515463c64389df9d61a90c87d2a0d91ea9268175c7ff8e

Cynet 360 AutoXDR™ Detections:

Payt Overview

Payt ransomware renames the encrypted files with .Payt along with the attacker's email and the host ID in the extension.

Once a computer's files have been encrypted and renamed (in approximately 15 minutes), it drops a note as ReadthisforDecode.txt.

The ransomware note contains general information, warnings and the attacker's email address:
Hydrox Ransomware

- Observed since: Aug 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .hydrox
- Ransomware note: Hydrox Ransomware.txt
- Sample hash: 24d49f947f968c4f654ebfa2d4c0bdd3a8ddf45cfa909dc8b36b57724b14361

Cynet 360 AutoXDR™ Detections:

Hydrox Overview
Hydrox ransomware renames the encrypted files with .hydrox in the extension:

Once a computer's files have been encrypted and renamed, it attempts to drop the ransomware note named Hydrox Ransomware:

Ransomware note contains general information, warnings and no option whatsoever to decrypt the files:

The ransomware also changes the desktop background:
World2022decoding Ransomware

- Observed since: Aug 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .world2022decoding
- Ransomware note: WE CAN RECOVER YOUR DATA.MHT
- Sample hash: 0737ddbd894f37316eee04c6739ac32f0c888535783a1af8c873023bcebb8e8

Cynet 360 AutoXDR™ Detections:

World2022decoding Overview

World2022decoding ransomware renames the encrypted files with .world2022decoding in the extension. Once a computer’s files have been encrypted and renamed, it drops a note named: WE CAN RECOVER YOUR DATA.MHT

Note: the ransomware was unable to encrypt the host and collapsed the machine. Therefore, no encryption was detected.
Cynet 360 AutoXDR™ Detections:

Medusa Locker Ransomware
- Observed since: 2019
- Ransomware encryption method: AES + RSA
- Ransomware extension: .readlockfiles
- Ransomware note: HOW_TO_RECOVER_DATA.html
- Sample hash: e9df120236929887bac3d2a0c6e737c833a306316853d2b3c7b2945d40a0e0a

Medusa Locker Overview
Medusa Locker ransomware renames the encrypted files with .readlockfiles in the extension:

Once a computer's files have been encrypted and renamed, it drops a note as: HOW_TO_RECOVER_DATA.html

Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains general information, warnings and several attacker's links.
VoidCrypt Ransomware

- Observed since: 2020
- Ransomware encryption method: AES + RSA
- Ransomware extension: .dark
- Ransomware note: unlock-info.txt
- Sample hash: 50586ef722c6a5c7b23d7b3a48bcf7003ea458bb1c3e659ddff832be73f5aebeb3d

Once a computer's files have been encrypted and renamed, it drops a note as unlock-info.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:

Orion Team
Thank you!

August, 2022