Contents

CrySpheRe .................................................................................................................................................................................... 3
Inlock .............................................................................................................................................................................................. 6
Anon_by .......................................................................................................................................................................................... 7
Faust ............................................................................................................................................................................................. 8
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 - November 18th 2022 - Rising Operations

There have been some interesting developments in ransomware this week, with the arrest of a cybercrime ring leader and reports shedding light on two new, but up-and-coming, ransomware operations.

Lawrence Abrams  November 18, 2022  05:13 PM  0

The Week in Ransomware - November 11th 2022 - LockBit feeling the heat

This 'Week in Ransomware' covers the last two weeks of ransomware news, with new information on attacks, arrests, data wipers, and reports shared by cybersecurity firms and researchers.

Lawrence Abrams  November 11, 2022  05:25 PM  0
CrySpheRe Ransomware

- Observed since: Nov 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .CrySpheRe
- Ransomware note: КАК РАСШИФРОВАТЬ ФАЙЛЫ.txt
- Sample hash: 9680ddca296d16b58ceb38130de58509df73eaafbf928d84b4a5d52c843c0a63

Cynet 360 AutoXDR™ Detections:

CrySpheRe Overview

CrySpheRe ransomware renames the encrypted files with .CrySpheRe in the extension:

Once a computer's files have been encrypted and renamed, it drops a note as “KA RASCHIFROVATь ФАЙЛЫ.txt” (No Russian Language in the machine):

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

- Observed since: Nov 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .inlock
- Ransomware note: READ_IT .txt
- Sample hash: 96e48ea92e40ebe25e26aa769b3cbe77fdef718d1846a92f6d3bb900932ebd

Cyrenet 360 AutoXDR™ Detections:

Inlock Overview

Inlock ransomware renames the encrypted files with .inlock in the extension:

Once a computer’s files have been encrypted and renamed, it drops a note named *READ_IT*.txt*:

The ransomware note contains general information, and warnings, seemingly in Spanish:

After Translation:

The attacker says the decryption key will be sent once the payment arrives.

YOUR COMPUTER HAS BEEN ENCRYPTED!!!

We are very sorry, but you have been the target of a cyber-attack.

All your personal data has been encrypted. Can I contact you to negotiate the ransom.

Once the payment arrives, I will send you the key to decrypt all the files.

I hope you don’t have anything of great value :(
Anon_by Ransomware

- Observed since: Nov 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .anon_by
- Ransomware note: anon_by.txt
- Sample hash: 057824bbb1dca42df1af0cacde596f8a5d3bb09a71dbbee5d2b4816b533ae35

Once a computer’s files have been encrypted and renamed, it drops a note named “anon_by.txt”:

Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains vague general information, as well as the attacker’s tags:

Translated:

you are attacked

The official anonymous IRC community, based on volunteering against unsupervised countries, etc.

© 2022 CYNET. All Rights Reserved

www.cy.net
Faust Ransomware

- Observed since: Nov 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .faust
- Ransomware note info.txt | .hta
- Sample hash: 0385dd2419adf0fe1a1e5d5ed28aaecbceb141103f0785e1b7079d94c9e4722e

Once a computer's files have been encrypted and renamed, it drops a note named “info.txt”:

And opens the note as a .hta file:

Upon execution, it immediately encrypts the endpoint. Then, after a while (approximately 15 minutes), it drops the ransomware note. The ransomware note contains general information and the attacker's contact information:

The .hta file contains additional information, along with the general information in the text file. It also contains information on a free decryption option, how to buy bitcoins, and generic warnings:
Thank you!

November, 2022