Contents

Executive Summary .................................................................................................................................................. 3
Aception ................................................................................................................................................................. 5
Pandora .................................................................................................................................................................. 6
LockBit 2.0 ............................................................................................................................................................ 7
BlackCat ................................................................................................................................................................. 8
Executive Summary

Orion is an integral department in Cynet’s research team that 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 against these threats.

The Week in Ransomware - March 25th 2022 - Critical infrastructure

With the US providing military aid to Ukraine and its sanctions damaging the Russian economy, the US government disclosed this week that there is intelligence that Russia is preparing for potential cyberattacks against US interests.

The Week in Ransomware - March 18th 2022 - Targeting the auto industry

This week, the automotive industry has been under attack, with numerous companies exhibiting signs of breaches or ransomware activity.

The Week in Ransomware - March 4th 2022 - The Conti Leaks

This week’s biggest story is the massive data leak from the Conti ransomware operation, including over 100,000 internal messages between members and source code for the ransomware and TrickBot operation.
Orion Team

Cynet 360 AutoXDR™ VS Ransomware
Acepy Ransomware

- Observed since: March 2022
- Ransomware encryption method: RSA + AES.
- Ransomware extension: .acepy
- Ransomware note: ACEPY_README.txt
- Sample hash: 84BCC4AE912F0378CC5148799B33650FE358820B5F4AD8A38DBD8CEEEE01EB1

Cynt 360 AutoXDR™ Detections:

Acepy Overview

Acepy ransomware renames the encrypted files with .acepy in the extension:

Once a computer’s files have been encrypted and renamed, it drops a note as ACEPY_README.txt.

Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains the attacker information and generic information about the encrypted files.
Pandora Ransomware

- **Observed since:** March 2022
- **Ransomware encryption method:** RSA
- **Ransomware extension:** .pandora
- **Ransomware note:** Restore_My_Files.txt
- **Sample hash:** 2C940A35025DD3847F7C954A282F65E9C2312D2ADA28686F9D1DC7D1C500224

### Pandora Overview

Pandora ransomware renames the encrypted files with .pandora in the extension. Once a computer's files have been encrypted and renamed, it drops a note as Restore_My_Files.txt. Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains warnings, information, and the attacker's contact information (the ransomware couldn't run in the labs properly due to the remediation):

```plaintext
### What happened?
#### !!!!!! Your files are encrypted!!!!

*All your files are protected by strong encryption with RSA-2048.*

*This is not public decryption software.*

*We have successfully stolen your confidential document data, finances, email, employee information, customers, research and development products...*

#### What is the price?

*The price depends on how fast you can write to us.*

*After payment, we will send you the decryption tool which will decrypt all your files.*

#### What should I do?

*There is only one way to get your files back. Contact us, pay and get decryption software.*

*If you decline payment, we will share your data files with the world.*

*You can browse your data breach here:* [http://kidnappedfile.com](http://kidnappedfile.com)

*We will share your files with the world.*

*You should download and install TOR browser first however! (torproject.org)*

#### !!! Decryption Guaranteed !!!

*Free decryption As a guarantee, you can send us up to 3 free decrypted files before payment.*

#### Hi! Contact us!!!

**email:** contact@pandorasway.xyz

#### !!! Warning !!!

*Do not attempt to decrypt your data using third-party software, this may result in permanent data loss.*

*Decryption of your files with the help of a third-party may result in a price increase (they charge as a fee), or you may get locked for a second time.*

*If you choose to use third-party software, expect data loss or re-infestation. It won't work.*

*Attempting to self-decrypt the file will result in the loss of your data.*
LockBit 2.0 Ransomware
- Observed since: Mid 2021
- Ransomware encryption method: AES + RSA
- Ransomware extension: .lockbit
- Ransomware note: Restore-My-Files.txt
- Sample hash: 9FEED0C7FA8C1D3239OE1C168051267DF61F11B048EC6E2A58B6E6F08E083AF

LockBit Overview
LockBit ransomware renames the encrypted files with .lockbit in the extension. Once a computer’s files have been encrypted and renamed, it drops a note as Restore-My-Files.txt.

Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains contact information and warnings:
**BlackCat Ransomware**

- **Observed since**: Early 2022
- **Ransomware encryption method**: AES + RSA
- **Ransomware extension**: .yicrlka
- **Ransomware note**: RECOVER-yicrlka-FILES.txt
- **Sample hash**: 6DD995D896A9A593B2C48D09D60BD8386D8577273F36D08788D83AD8173E68

**Cynet 360 AutoXDR™ Detections:**

![Cynet 360 AutoXDR™ Detections](image)

**BlackCat Overview**

BlackCat ransomware renames the encrypted files with .yicrlka in the extension and once a computer's files have been encrypted and renamed, it drops a note as RECOVER (variant name)-FILES.txt.

Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains instructions and the attacker's webpage address:

```plaintext
> What happened?
Important files on your network were ENCRYPTED and now they have "yicrlka" extension. In order to recover your files you need to follow instructions below.

> Sensitive Data
Sensitive data on your network was DOWNLOADED. If you DON'T WANT your sensitive data to be PUBLISHED you have to act quickly.

Data includes:
- Employees personal data, CIIs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Private financial information including: clients data, bills, budgets, annual reports, bank statements.
- Manufacturing documents including: datagrams, schematics, drawings in solidworks format.
- And more...

> CAUTION
DO NOT MODIFY ENCRYPTED FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.

> What should I do next?
1) Download and install Tor Browser from: https://torproject.org/
```
Thank you!

March, 2022