cynet

Orion Team

Monthly Ransomware Activity

Written by: Maor Huli

April, 2022

Orion Team

Contents

©ALL RIGHTS RESERVED TO CYNET 2022 WWW.CYNET.COM

Orion Team

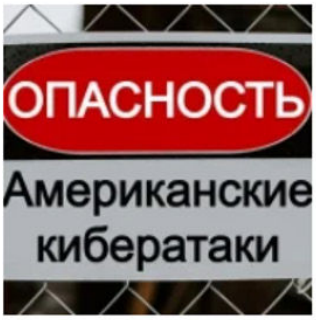
Executive Summary

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 indentified 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 - April 29th 2022 - New operations emerge

This week we have discovered numerous new ransomware operations that have begun operating, with one appearing to be a rebrand of previous operations.

LAWRENCE ABRAMS APRIL 29, 2022 06:29 PM 0



The Week in Ransomware - April 15th 2022 - Encrypting Russia

While countries worldwide have been the frequent target of ransomware attacks, Russia and CIS countries have been avoided by threat actors. The tables have turned with the NB65 hacking group modifying the leaked Conti ransomware to use in attacks on Russian entities.

LAWRENCE ABRAMS APRIL 15, 2022 05:19 PM 0

The Week in Ransomware - April 1st 2022 - 'I can fight with a keyboard'

While ransomware is still conducting attacks and all companies must stay alert, ransomware news has been relatively slow this week. However, there were still some interesting stories that we outline below.

LAWRENCE ABRAMS APRIL 01, 2022 07:07 PM 0

©ALL RIGHTS RESERVED TO CYNET 2022 WWW.CYNET.COM

Orion Team

Cynet 360 AutoXDR™ VS Ransomware

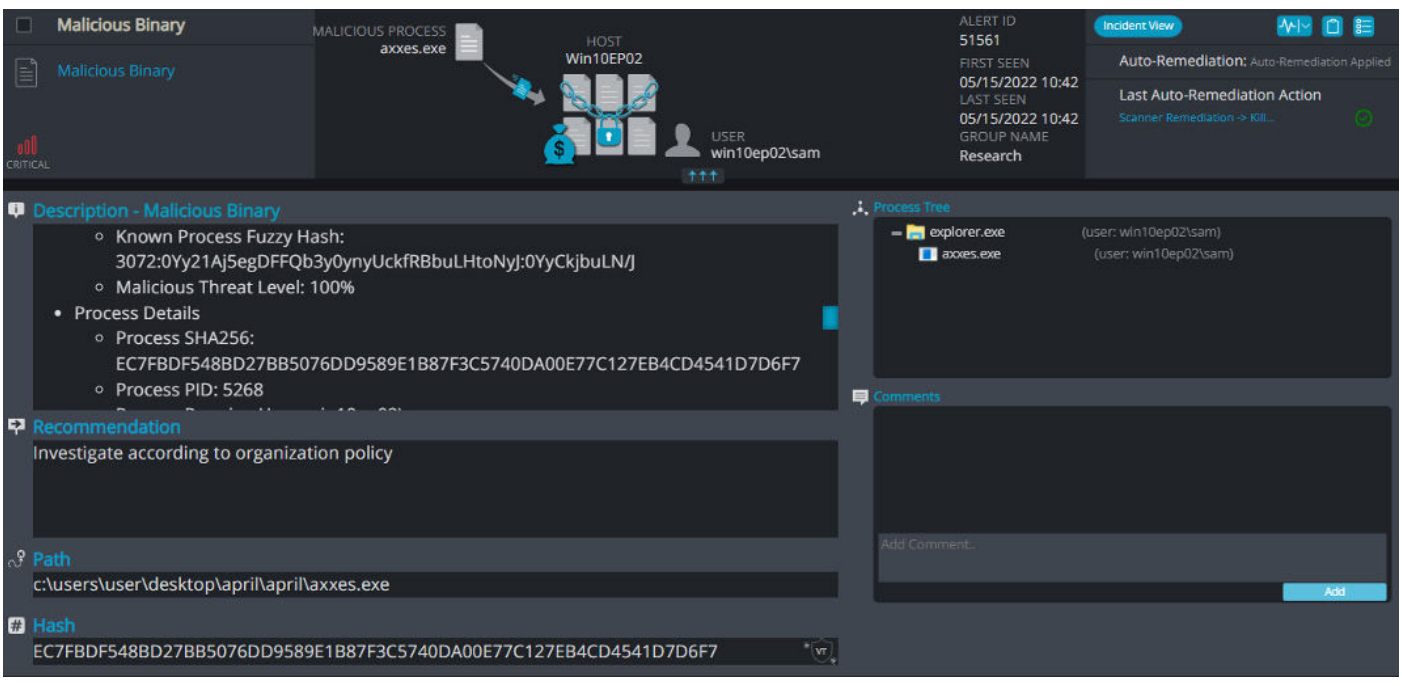
©ALL RIGHTS RESERVED TO CYNET 2022 WWW.CYNET.COM

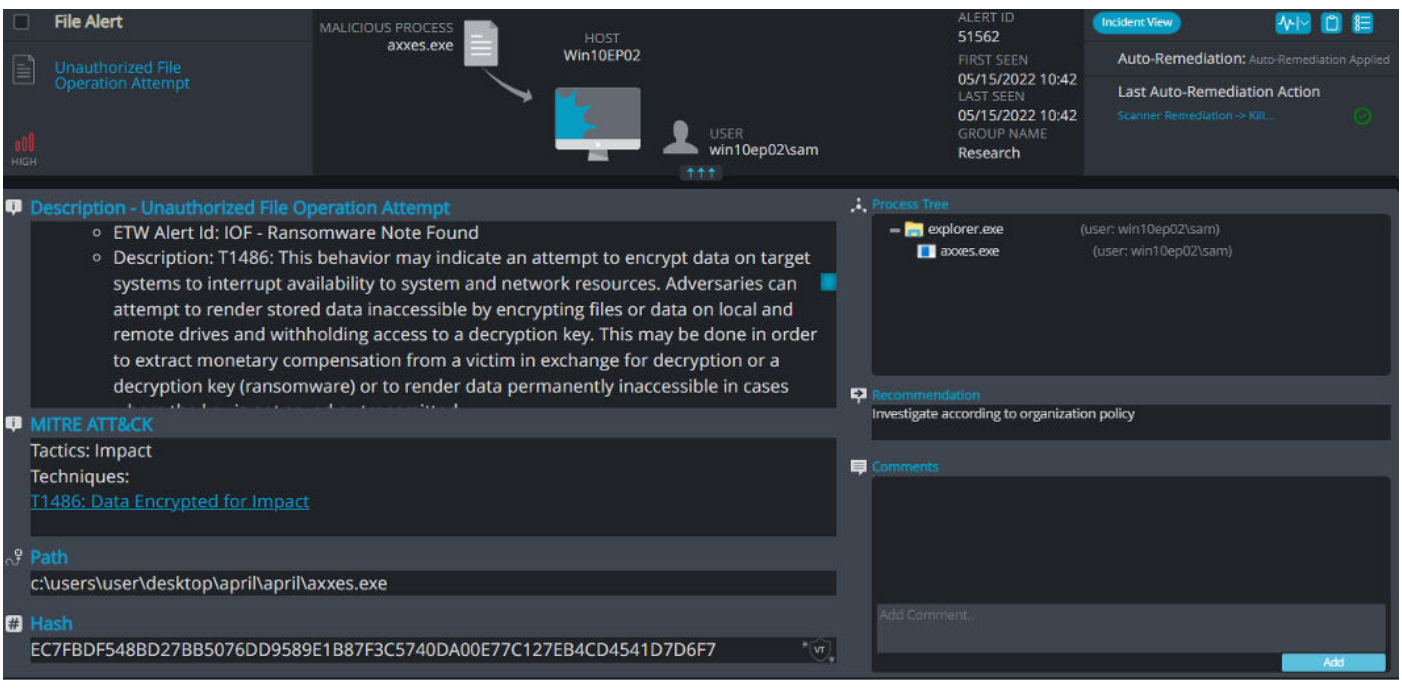
Orion Team

Axxes Ransomware

- Observed since: April 2022
- Ransomware encryption method: RSA + AES.
- Ransomware extension: .axxes
- Ransomware note: RESTORE_FILES_INFO.txt
- Sample hash: ec7fbdf548bd27bb5076dd9589e1b87f3c5740da00e77c127eb4cd4541d7d6f7

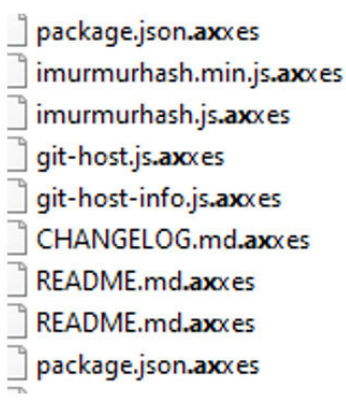
Cynet 360 AutoXDR™ Detections:



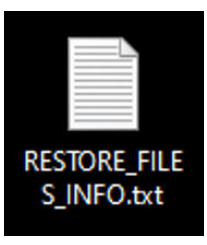


Axxes Overview

Axxes ransomware renames the encrypted files with .axxes in the extension:



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



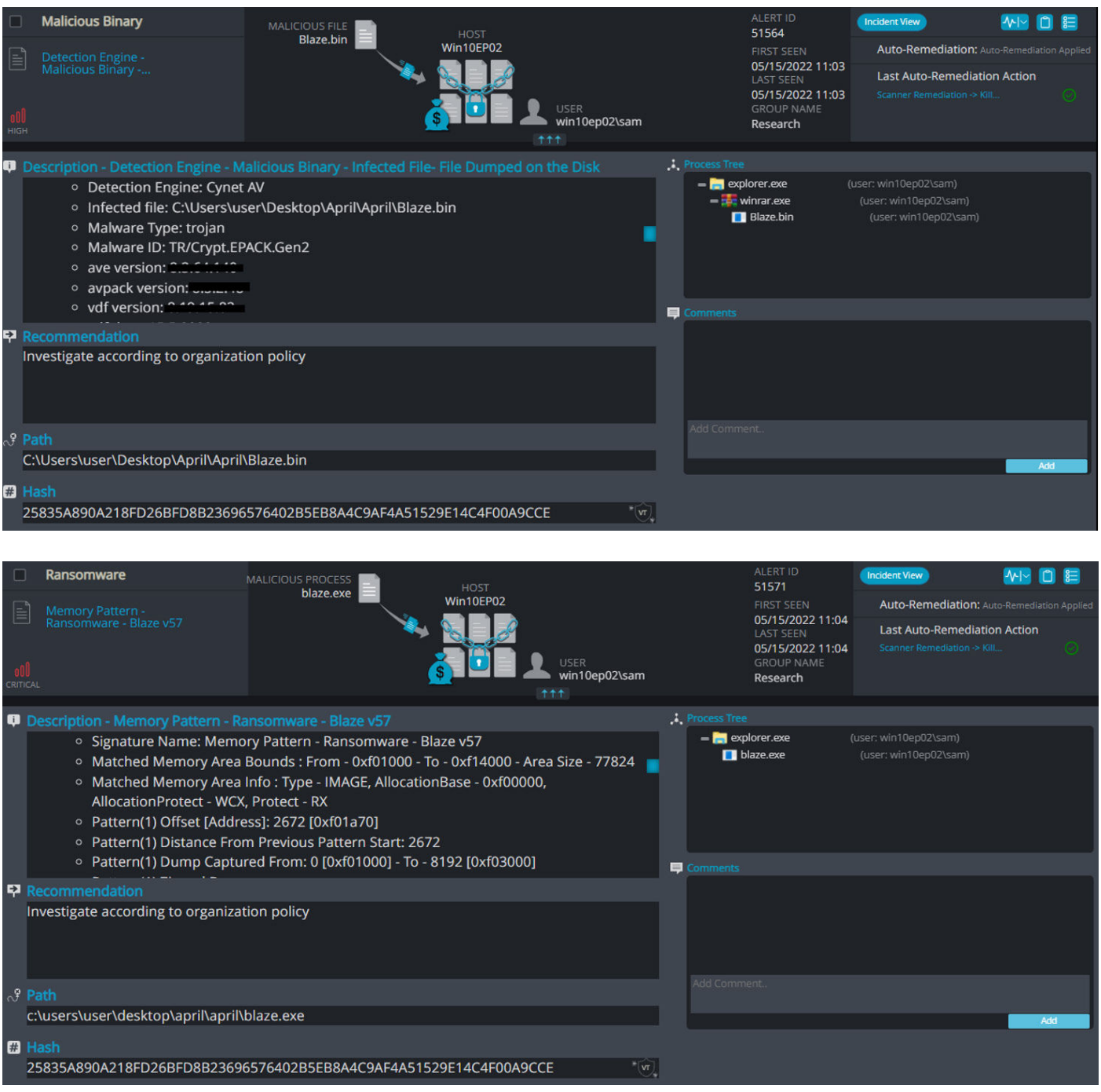
Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains only the encryption key:

Orion Team

Blaze Ransomware

- Observed since: December 2021
- Ransomware encryption method: RSA.
- Ransomware extension: .blaze
- Ransomware note: How To Decrypt.txt
- Sample hash: 25835a890a218fd26bfd8b23696576402b5eb8a4c9af4a51529e14c4f00a9cce

Cynet 360 AutoXDR™ Detections:

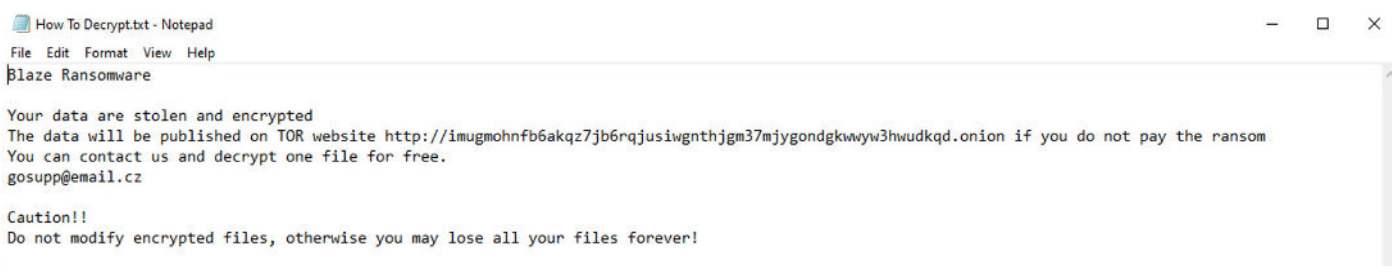


Blaze Overview

Blaze ransomware renames the encrypted files with .blaze in the extension:

Once a computer's files have been encrypted and renamed, it drops a note as How To Decrypt.txt:

Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains general information and the attacker's contact information:

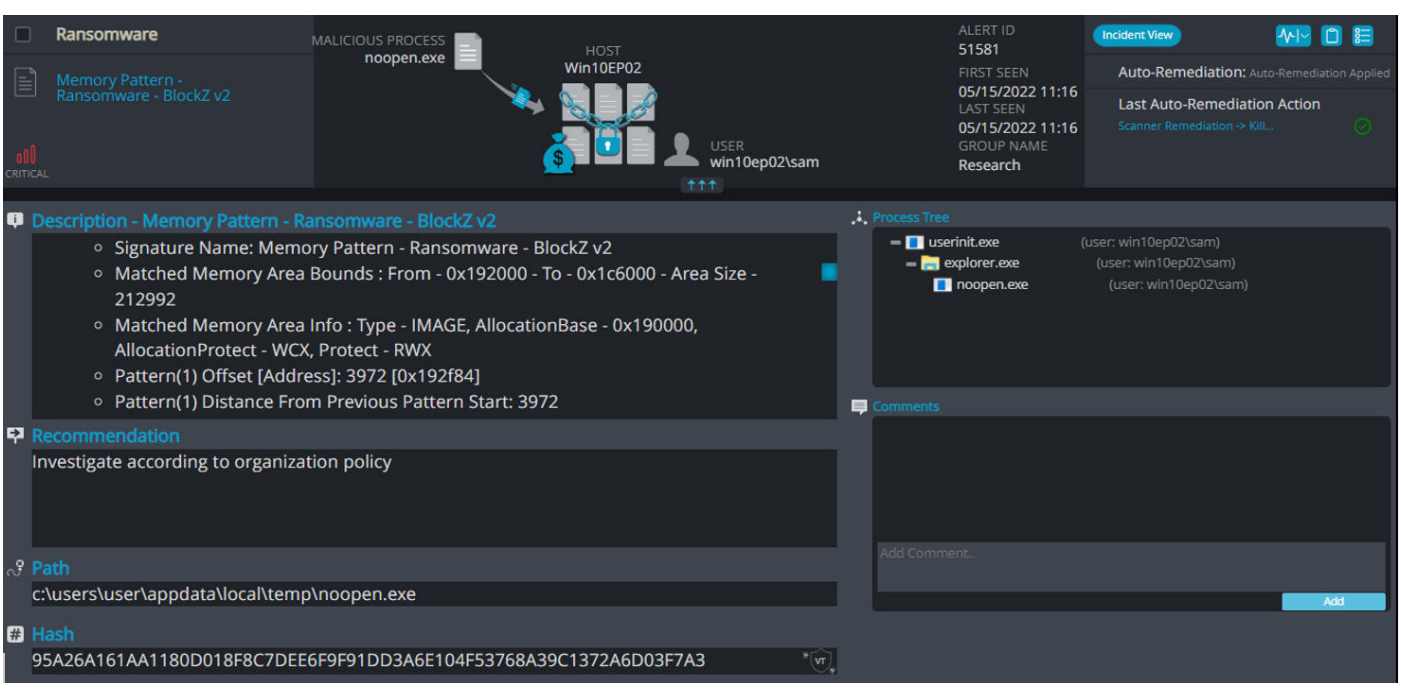


Orion Team

BlockZ Ransomware

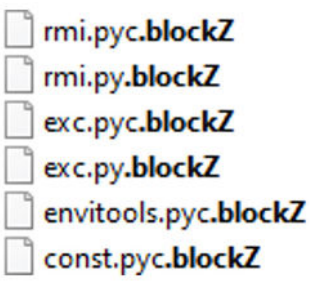
- Observed since: April 2022
- Ransomware encryption method: AES + RSA.
- Ransomware extension: .blockZ
- Ransomware note: How To Restore Your Files.txt
- Sample hash: 856d9e698f240a21db57f404fea33ee65cd0458f31a9d0fca7044962204484c9

Cynet 360 AutoXDR™ Detections:



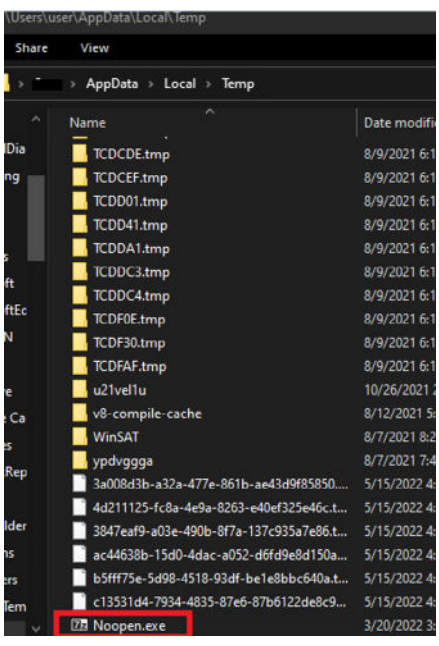
BlockZ Overview

BlockZ ransomware renames the encrypted files with .blockZ in the extension:

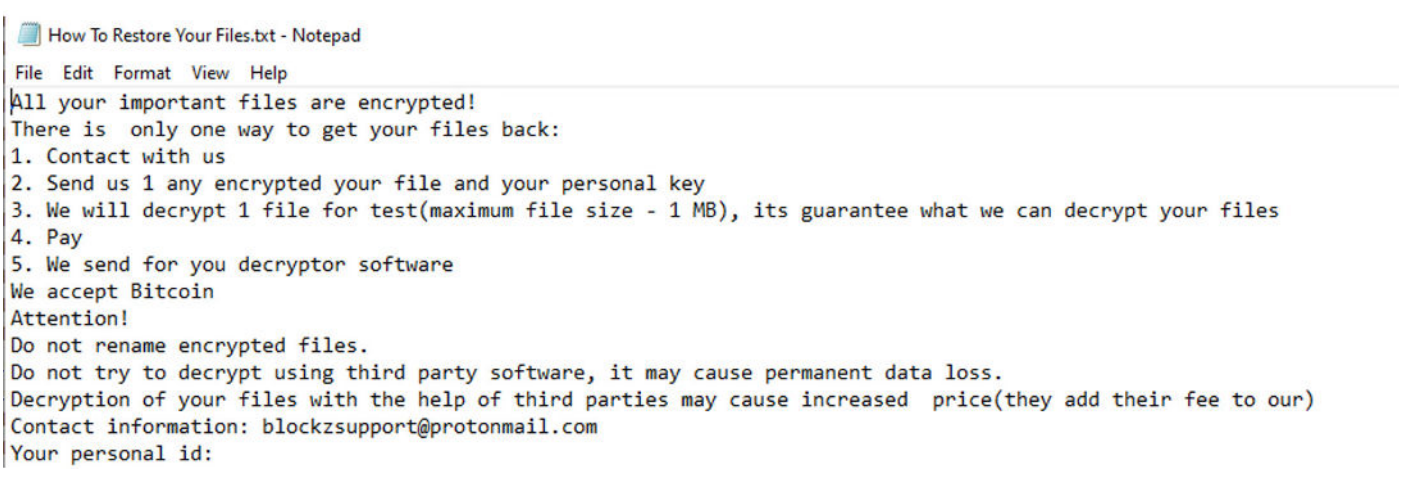


Once a computer's files have been encrypted and renamed, it drops a note as How To Restore Your Files.txt:

Upon execution, it first drop a file in the path "c:\users*user\appdata\local\temp\" with the name of Noopen.exe:



Once executed the dropped file it changes the process name to schtasks.exe and it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains contact information, warnings, and decryption test for 1 file:

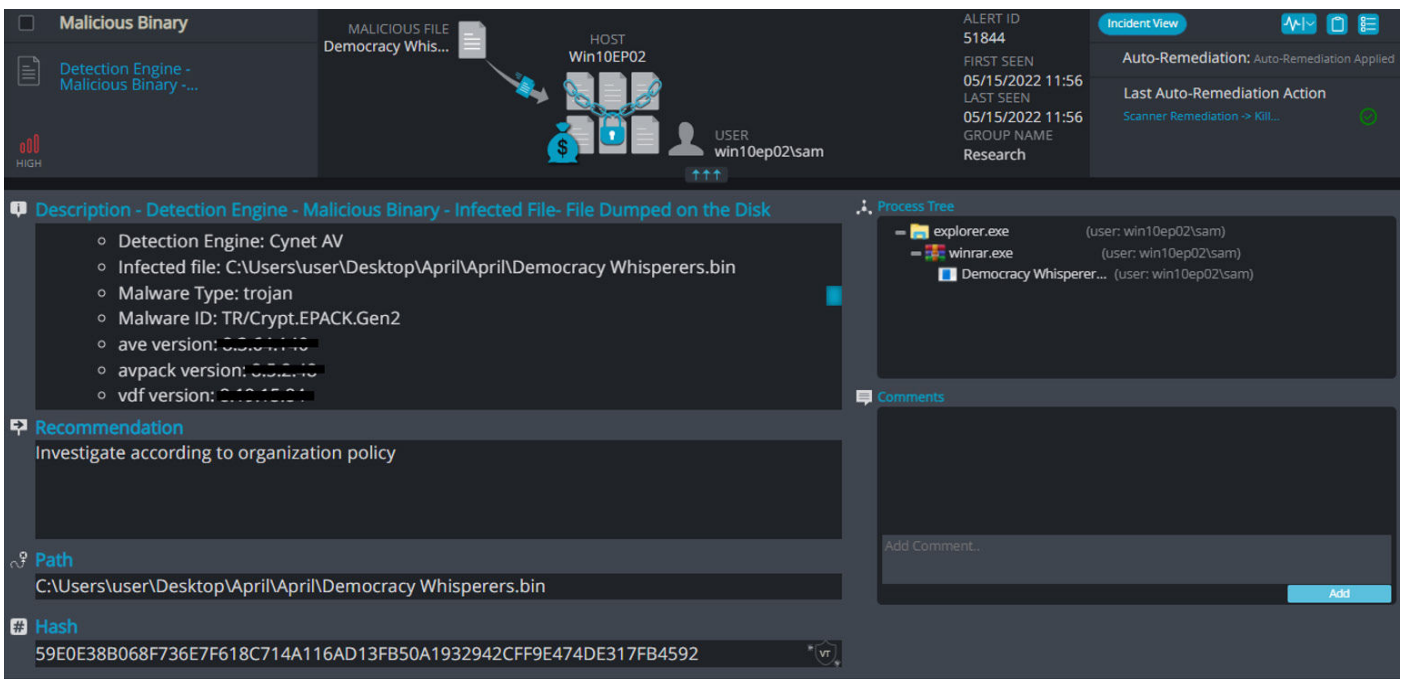


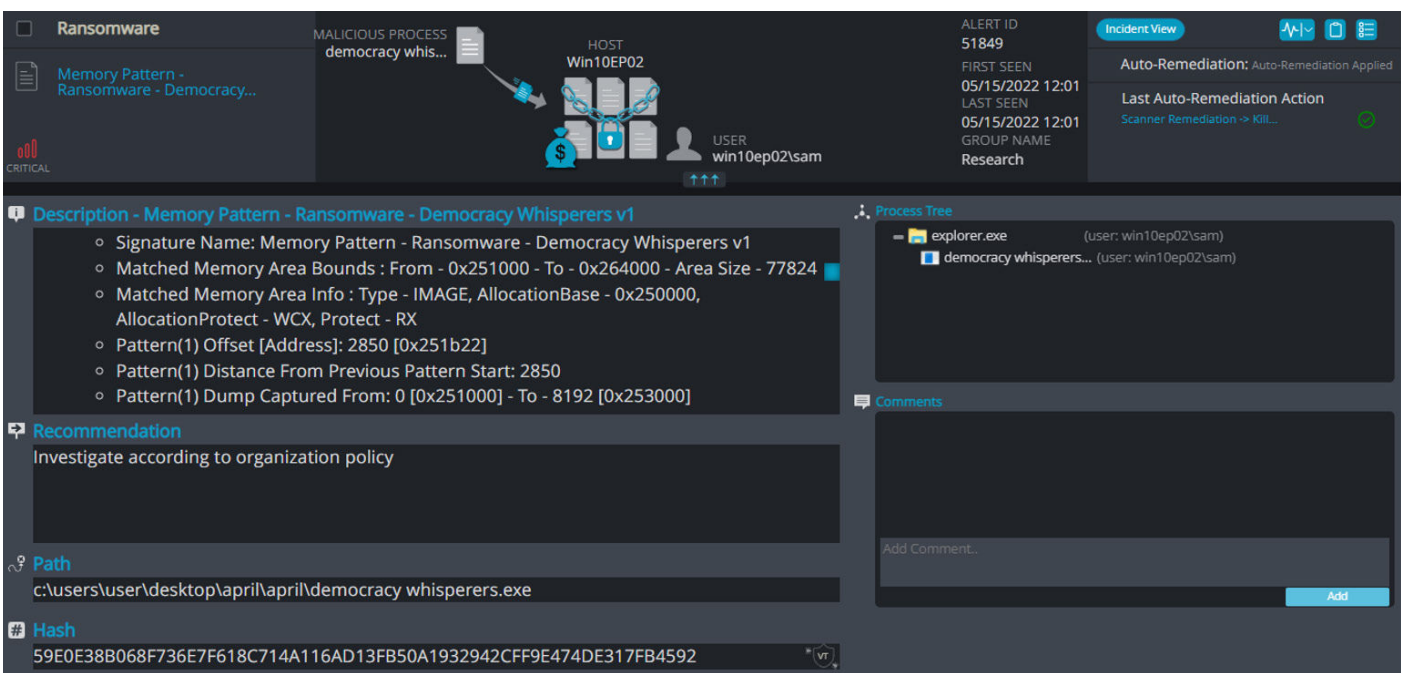
Orion Team

DemocracyWhisperers Ransomware

- Observed since: April 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .democ
- Ransomware note: Restore Files.txt
- Sample hash: 59e0e38b068f736e7f618c714a116ad13fb50a1932942cff9e474de317fb4592

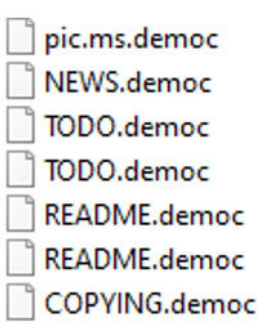
Cynet 360 AutoXDR™ Detections:



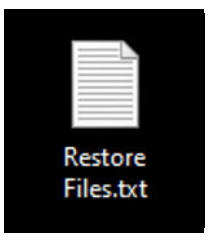


DemocracyWhisperers Overview

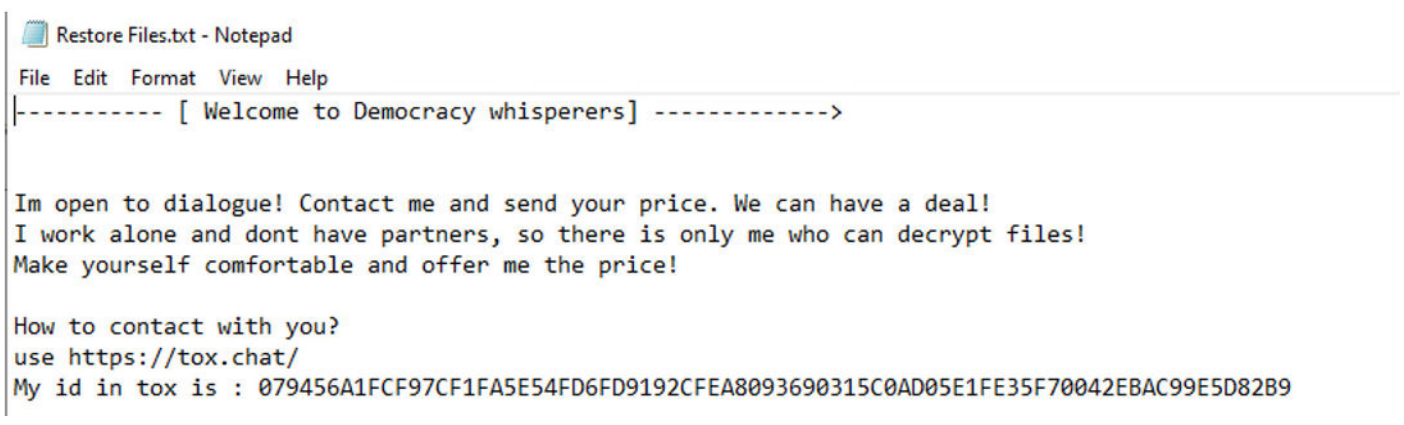
DemocracyWhisperers ransomware renames the encrypted files with .democ in the extension:



Once a computer's files have been encrypted and renamed, it drops a note as Restore Files.txt:



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



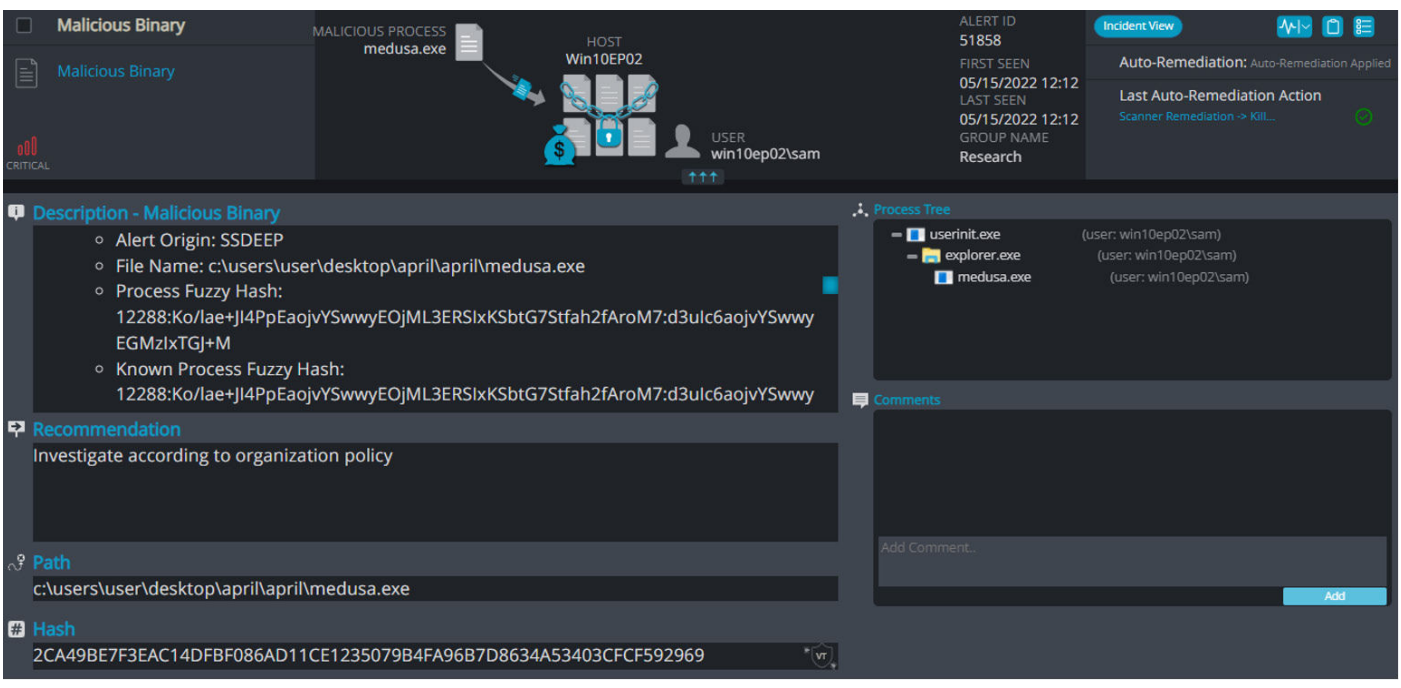
©ALL RIGHTS RESERVED TO CYNET 2022 WWW.CYNET.COM

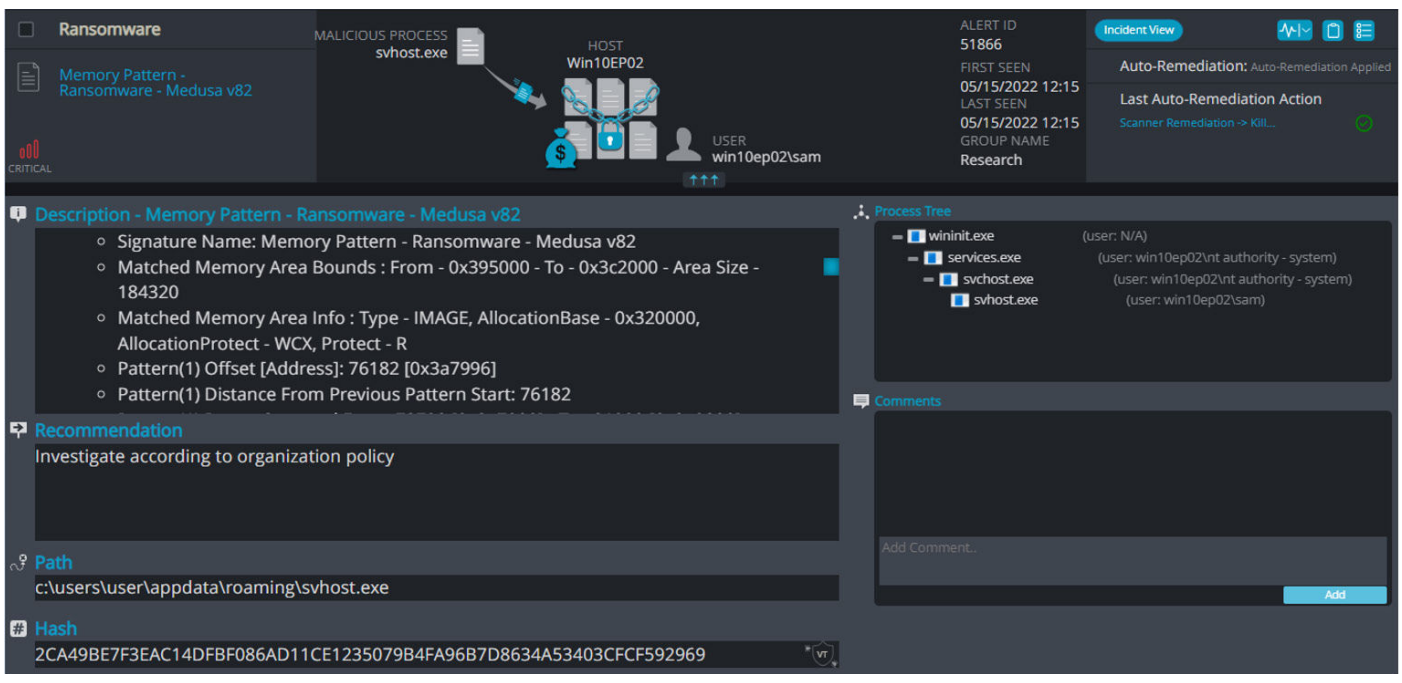
Orion Team

Medusa Ransomware

- Observed since: Late 2019
- Ransomware encryption method: AES + RSA
- Ransomware extension: .stopfiles
- Ransomware note: Recovery_instructions.html
- Sample hash: 2ca49be7f3eac14dfbf086ad11ce1235079b4fa96b7d8634a53403cfcf592969

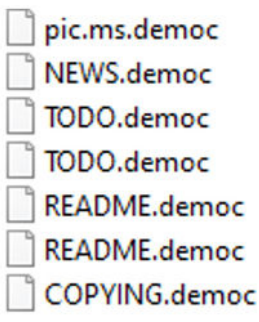
Cynet 360 AutoXDR™ Detections:





Medusa Overview

Medusa ransomware renames the encrypted files with .stopfiles in the extension:



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

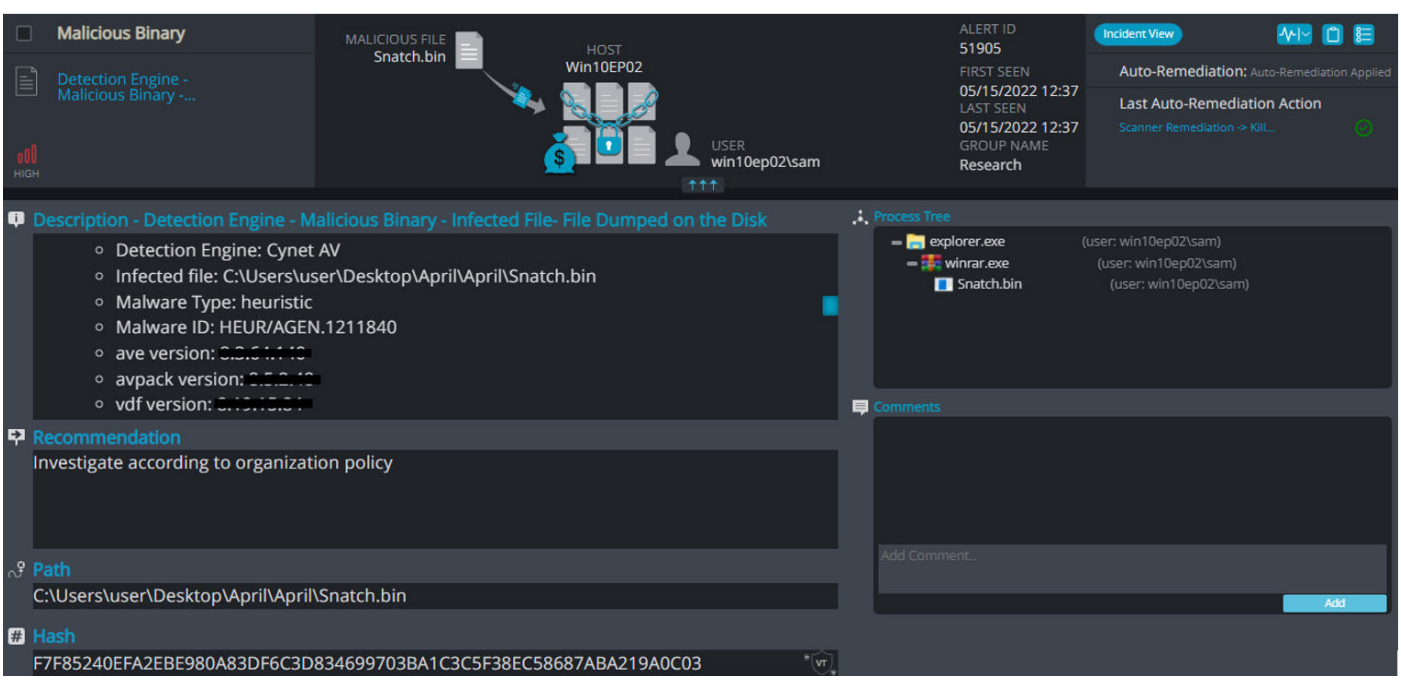
Upon execution, it inject itself to svchost and it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains instructions and the attacker's contact info:

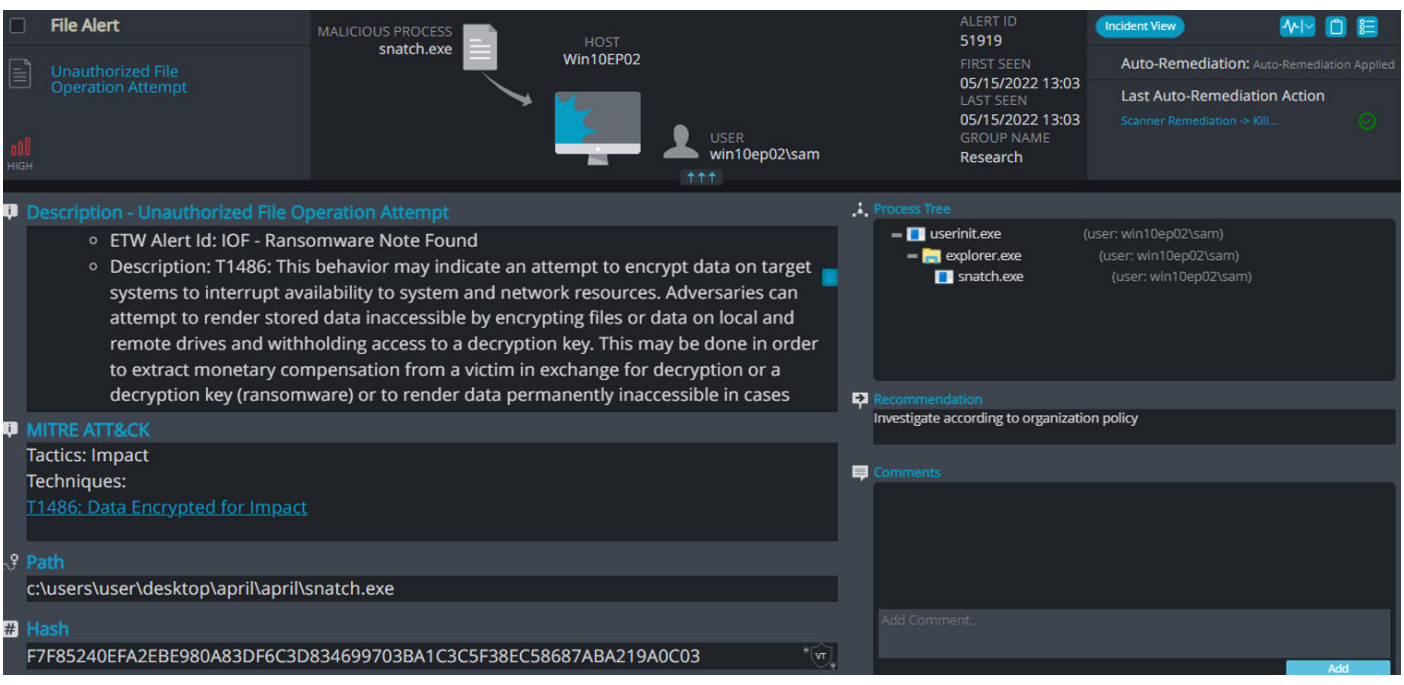
Orion Team

Snatch Ransomware

- Observed since: December 2018
- Ransomware encryption method: AES + RSA
- Ransomware extension: .sdhvqq
- Ransomware note: HOW TO RESTORE YOUR FILES.TXT
- Sample hash: 25835a890a218fd26bfd8b23696576402b5eb8a4c9af4a51529e14c4f00a9cce

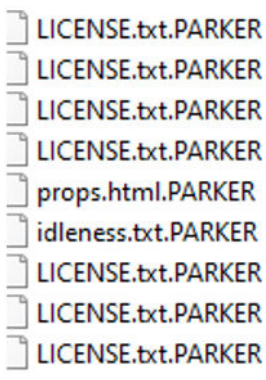
Cynet 360 AutoXDR™ Detections:



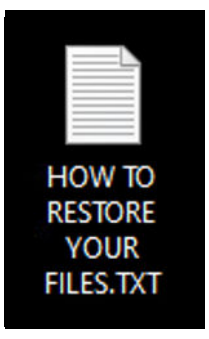


Snatch Overview

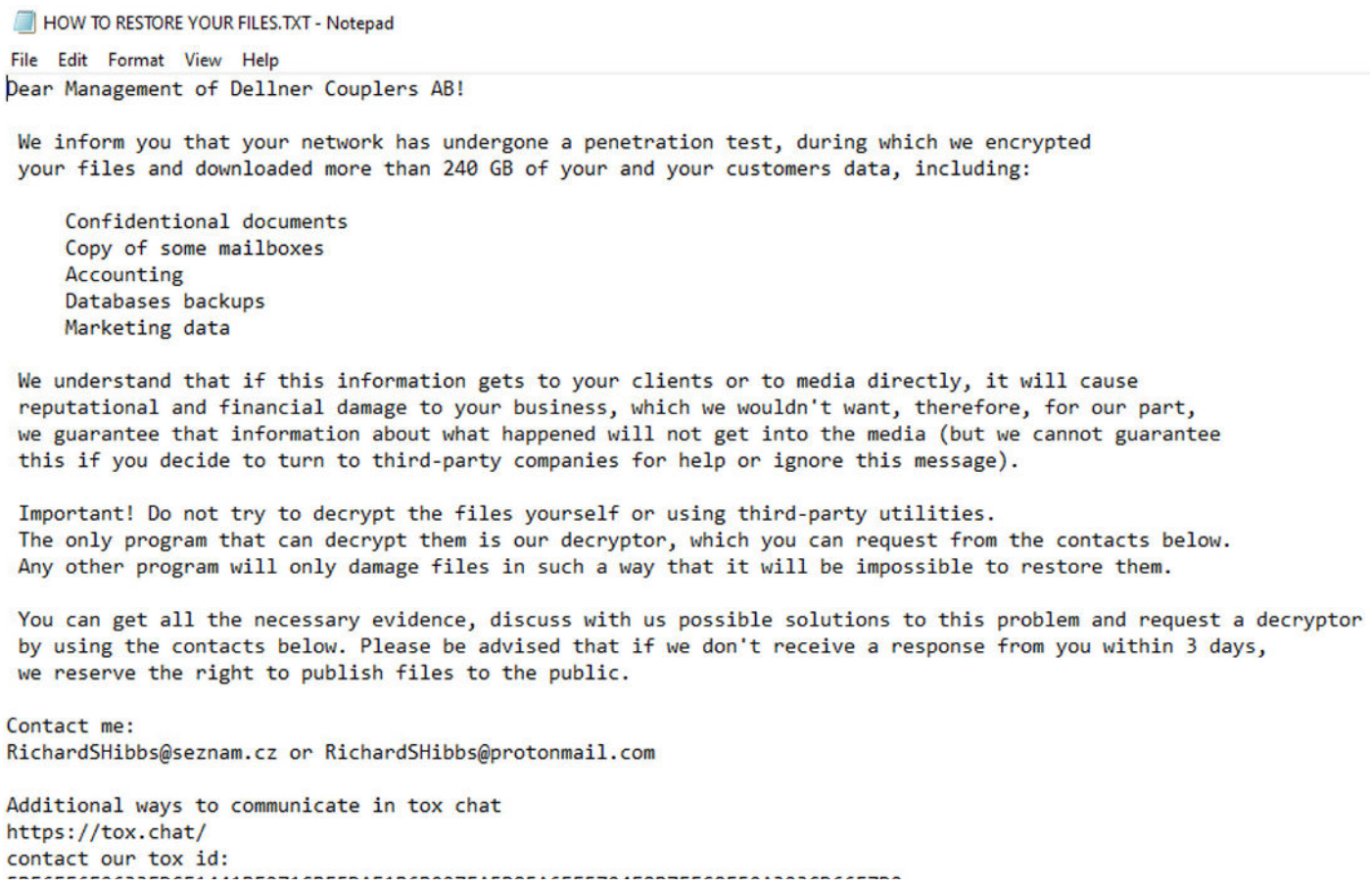
Snatch ransomware renames the encrypted files with .sdhvqq in the extension:



Once a computer's files have been encrypted and renamed, it drops a note as HOW TO RESTORE YOUR FILES.TXT:



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

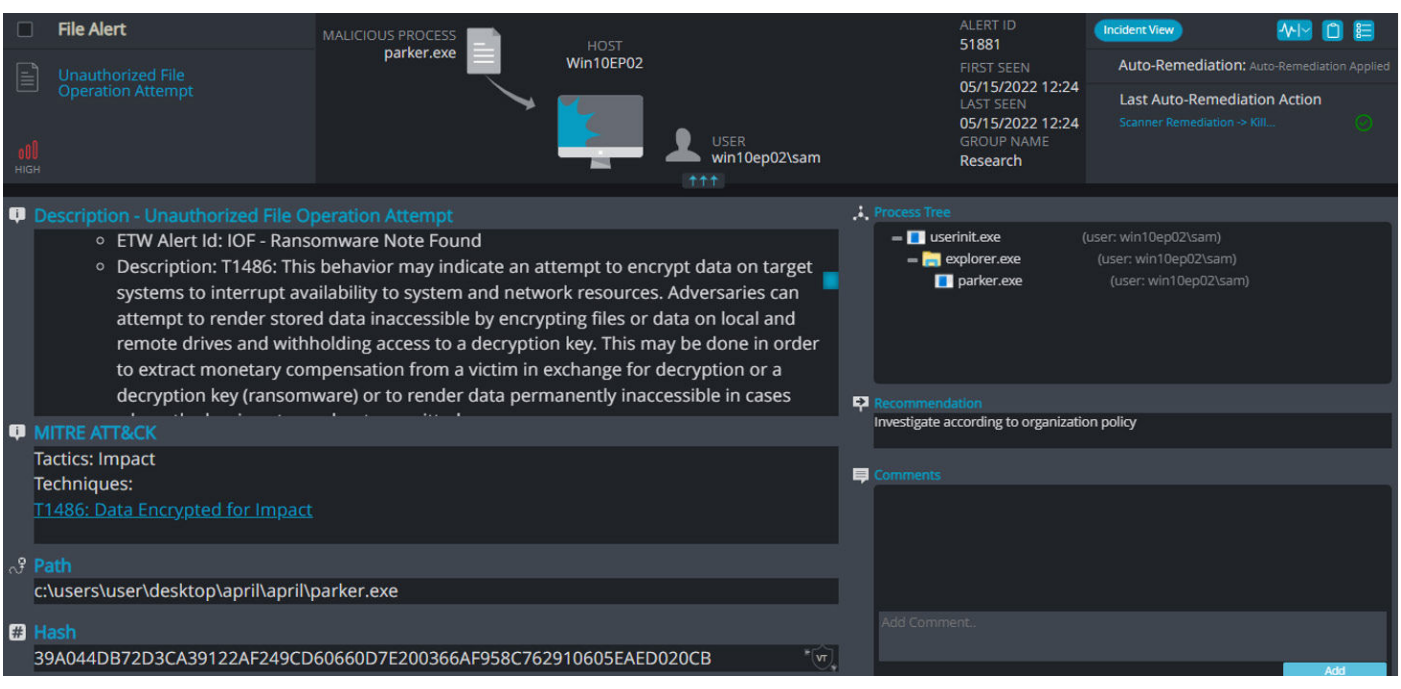


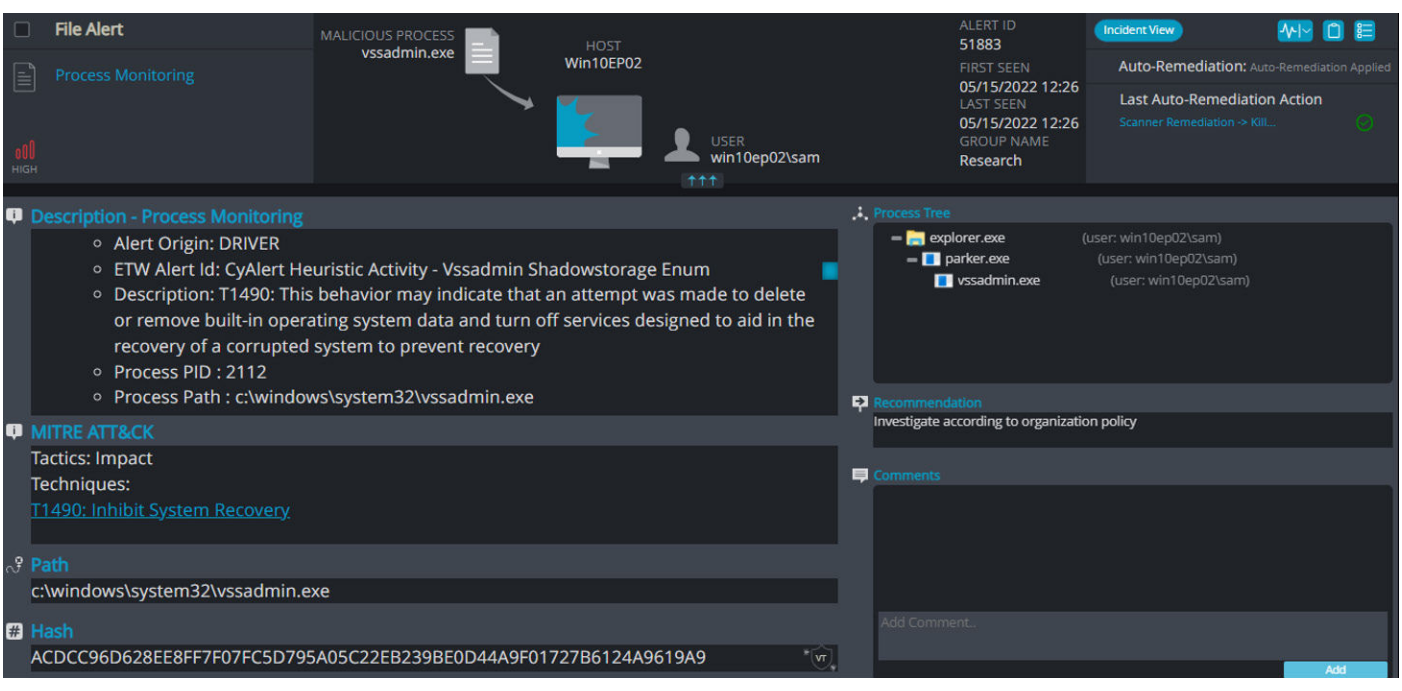
Orion Team

Parker Ransomware

- Observed since: April 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .PARKER
- Ransomware note: RESTORE_FILES_INFO.txt
- Sample hash: 39a044db72d3ca39122af249cd60660d7e200366af958c762910605eaed020cb

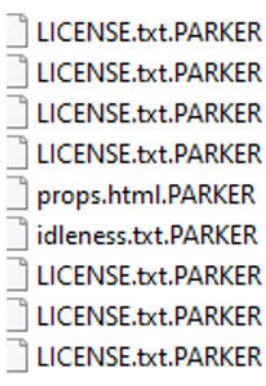
Cynet 360 AutoXDR™ Detections:



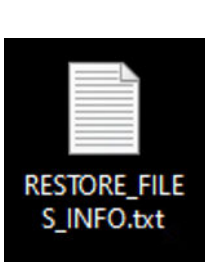


Parker Overview

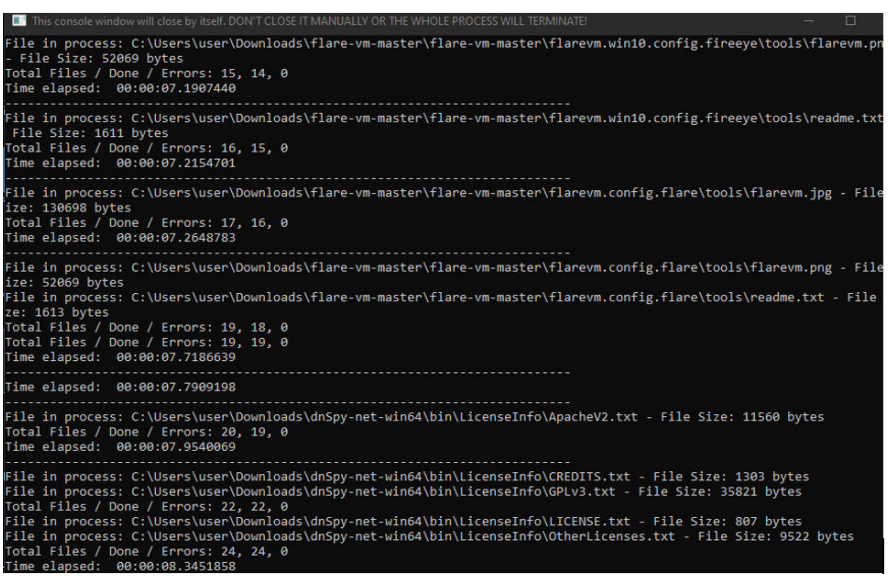
Parker ransomware renames the encrypted files with .PARKER in the extension:



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



Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains instructions, threats for data publication, and the attacker's contact info:



RESTORE_FILES_INFO.txt - Notepad

File Edit Format View Help

```
------------------
| What happened? |
------------------

Your network was ATTACKED, your computers and servers were LOCKED,
Your private data was DOWNLOADED:
 - Contracts
 - Customers data
 - Finance
 - HR
 - Databases
 - And more other...

----------------------
| What does it mean? |
----------------------

It means that soon mass media, your partners and clients WILL KNOW about your PROBLEM.

--------------------------
| How it can be avoided? |
--------------------------

In order to avoid this issue,
you are to COME IN TOUCH WITH US no later than within 3 DAYS and conclude the data recovery and breach fixing AGREEMENT.

-----------------------------------------
| What if I do not contact you in 3 days? |
-----------------------------------------

If you do not contact us in the next 3 DAYS we will begin DATA publication.

It is your RIGHT, but in this case all your data will be published for public USAGE.

------------------------------
| I do not fear your threats! |
------------------------------

That is not the threat, but the algorithm of our actions.
If you have hundreds of millions of UNWANTED dollars, there is nothing to FEAR for you.
That is the EXACT AMOUNT of money you will spend for recovery and payouts because of PUBLICATION.
You are exposing yourself to huge penalties with lawsuits and government if we both don't find an agreement.
We have seen it before cases with multi million costs in fines and lawsuits,
not to mention the company reputation and losing clients trust and the medias calling non-stop for answers.

--------------------------
| You have convinced me! |
--------------------------

Then you need to CONTACT US, there is few ways to DO that.

                    ---Secure method---

   a) Download a qTOX client: https://tox.chat/download.html
   b) Install the qTOX client and register account
   c) Add our qTOX ID: 671263E7BC06103C77146A5ABB802A63F53A42B4C4766329A5F04D2660C99A3611635CC36B3A
or qTOX ID: BC6934E2991F5498BDF5D852F10EB4F7E1459693A2C1EF11026EE5A259BBA3593769D766A275
   d) Write us extension of your encrypted files .PARKER

Our LIVE SUPPORT is ready to ASSIST YOU on this chat.
```


©ALL RIGHTS RESERVED TO CYNET 2022 WWW.CYNET.COM

cynet

Thank you!

April, 2022