horizontal line

**Plus971 Cybersecurity**

**Ransomware Attack**

**7th September 2023**

By : Pallavi, Yasir, Daniel, Amatullah, Pranav

**TABLE OF CONTENTS**

[**Objective 1**](#_k4tdwr7kgfyo)

[**Background 1**](#_4c4jf5r08h6l)

[**Overview 1**](#_tcmcll1sqjbp)

[Case Details: 1](#_r1kz8oa5ae2l)

[Analysis Tools Used: 1](#_od0akebegx0v)

[Computer Details: 1](#_67f2gm93iods)

[Image Details: 2](#_vbpxm3a11dtz)

[**Executive Summary 2**](#_hfbwn7sji3wx)

[**Attack Scenario 3**](#_whwqebvfynr6)

[**Timeline of Events 3**](#_b7jdfjnd9kiq)

[**Details of Analysis 5**](#_wwdq7meee1d1)

[**Conclusion 9**](#_tc3mr66ob9)

# 

# Objective

Determine what triggered the Ransomware spread on the imaged computer and the files responsible for the spread.

# Background

This report presents the findings of Plus971 interns ongoing incident response investigation into a “Black cat” Ransomware attack on 2023-05-10 9:40 GST. The forensic analysis is being conducted by Interns of Plus971 Cyber Security.

# Overview

## Case Details:

| Case Number | RANSOMWARE |
| --- | --- |
| Forensic Examiner(s) | Pallavi, Yasir, Daniel, Amatullah, Pranav |
| Date and Time of Attack | 2023-05-10 13:58:23 GST |
| Unique Description | Ransomware Attack |

## Analysis Tools Used:

| **Tool** | **Version Number** | **License Details** |
| --- | --- | --- |
| FTK Imager | 4.7.1 | Freeware |
| Autopsy | 4.20.0 | Free Trial |
| RegRipper | 3.0 | Freeware |

## Computer Details:

| **Attribute** | **Value** | **Value From** |
| --- | --- | --- |
| MAC Address | 80:6E:6F:6E:69:63 | ExeUnique MAC Addresses: (from ntuser.dat) |
| Nation | 244 (United States) | Control Panel\International\Geo  LastWrite time: 2022-05-26 05:25:30Z |
| Operating System | WINDOWS 7 ULTIMATE SERVICE PACK 1 | /img\_CASE RANSOMWARE.E01/vol\_vol2/Windows/System32/license.rtf |
| Timezone | Arabian Standard Time | /img\_CASE RANSOMWARE.E01/vol\_vol2/Windows/System32/config/SYSTEM |

## Image Details:

| File Name | CASE RANSOMWARE.E01 |
| --- | --- |
| Number of image parts | 10 |
| Image Source Size | 61440 MB |
| Sector Size | 512 bytes |
| MD5 Checksum Hash | 19404f45940d23f34d6cf10b78ea9b5f |
| SHA1 checksum Hash | 147d5ed6983a55f502e75117ccf1f388c665b54f |
| Acquisition Started | Wed May 10 14:10:18 2023 |
| Acquisition finished | Wed May 10 14:22:35 2023 |
| Verification Started | Wed May 10 14:22:36 2023 |
| Verification finished | Wed May 10 14:27:02 2023 |
| Hashes Match | YES |
| Tool used for Acquisition | ADI4.5.0.3 |

# Executive Summary

The main objective was to determine what triggered the Ransomware spread on the imaged computer and the files responsible for the spread.

**Key Findings:**

The client's laptop was compromised by the BLACKCAT ransomware.

Data encryption was successful, affecting critical files and documents.

The laptop's system remains uncompromised.

We strongly advise against paying the ransom.

**Recommendations:**

Isolate and preserve the affected laptop.

Conduct a full system scan for residual malware.

Initiate data recovery from clean backups.

Enhance cybersecurity measures and employee training.

Report the incident to relevant authorities.

This summary outlines key findings and provides essential recommendations to address the ransomware attack on the client's laptop, emphasizing data recovery and future prevention measures.

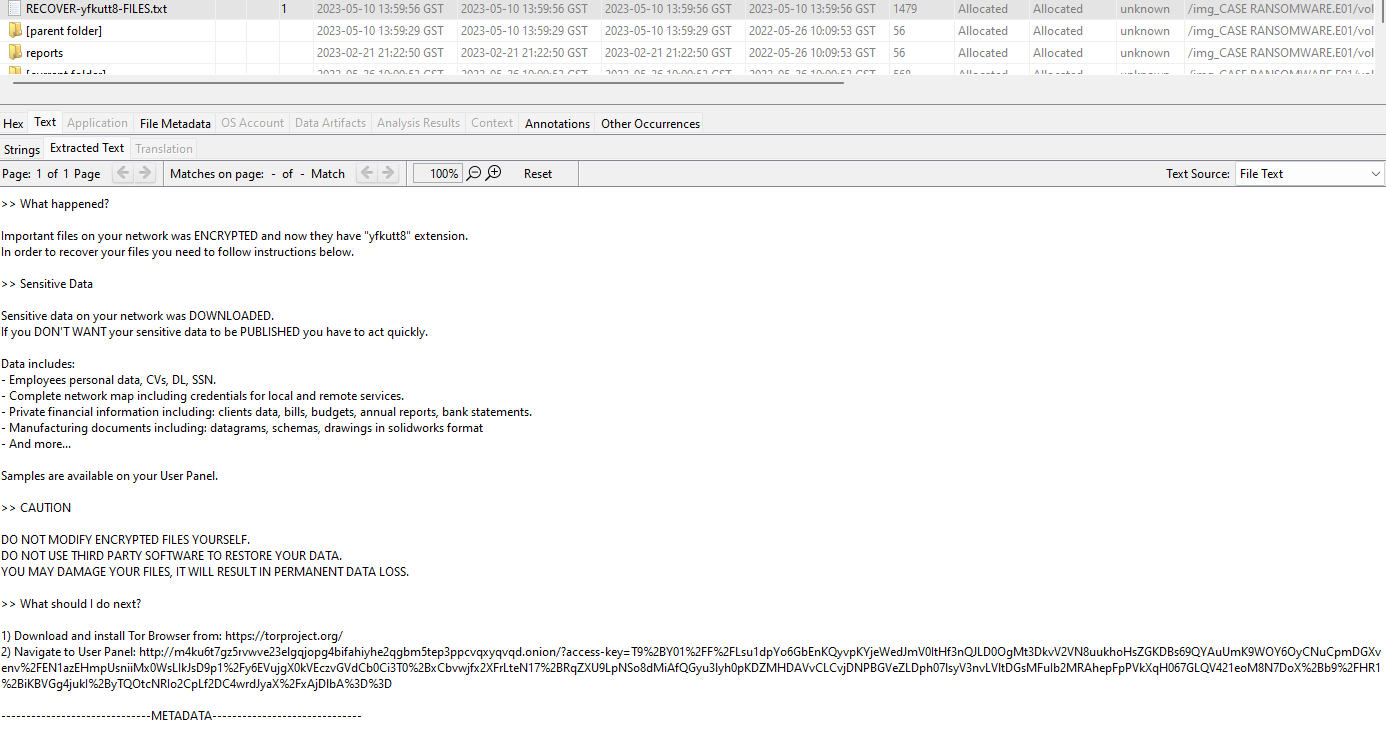
# Attack Scenario

In this scenario, a personal laptop becomes infected with the "BlackCat" ransomware . The ransomware encrypts the user's personal files and displays a ransom note demanding a cryptocurrency payment for decryption. To investigate the infection and potential recovery options, a digital forensics team utilizes the Autopsy tool to analyze the laptop's image. Autopsy assists in identifying the ransomware variant, recovering the ransom note, and providing insights into the attack's execution. This scenario highlights the importance of digital forensics in understanding and responding to ransomware infections on personal computing devices.

# Timeline of Events

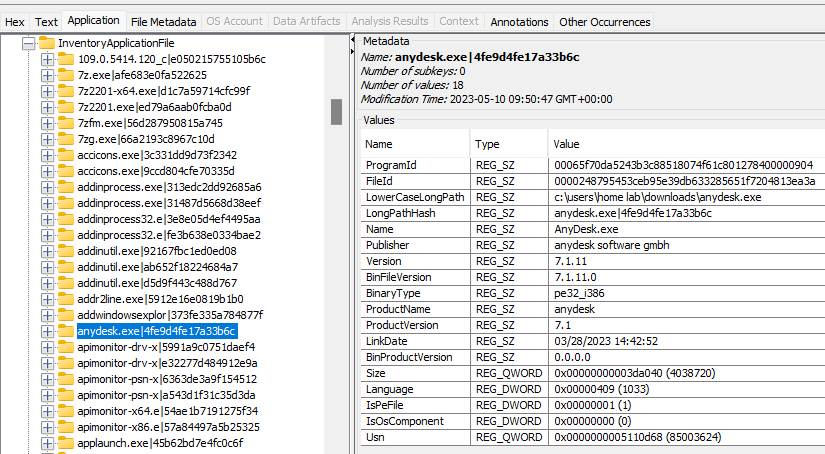
| **EVENT** | **TIME** | **LOCATION** |
| --- | --- | --- |
| Confidential.exe was downloaded | 2023-02-21 12:46:14 GST | /Users/HOME LAB/Downloads/ransomware/forew/continental.exe |
| Fakeransom xml was found that has the command to run the fakeransom.exe file | 2022-07-31 08:24:01 GST | /Windows/System32/Tasks/fakeransom |
| Microsoft Defender Antivirus has removed the history of malware and other potentially unwanted software. | 4/10/2023 1:53:44 PM GMT+4 | Microsoft-Windows-Windows Defender%4Operational.evtx |
| 22 failed logins to user “HOMELAB” | 2023-05-10 09:40:47 Z | /Windows/System32/config/SAM |
| The password to user “HOMELAB” was cracked | 2023-05-10 09:40:50 Z | /Windows/System32/config/SAM |
| AnyDesk was opened | 2023-05-10 09:44:53.162 Z | /$LogFile |
| anydesk access login timestamp was seen before the timestamp of the ransomware note | 2023-05-10 09:50:47 Z | /Windows/AppCompat/Programs/Amcache.hve |
| Folder Libraries\CLSID\_Documents Library\fore - Copy\forew was accessed | 2023-05-10 09:52:27 Z | ShimCache in /img\_CASE RANSOMWARE.E01/vol\_vol2/Users/HOME LAB/AppData/Local/Microsoft/Windows/UsrClass.dat |
| Account “conti” was created | 2023-05-10 09:57:07 Z | /Windows/System32/config/SAM |
| Fakeransom was running during a memory dump | 2023-05-10 13:39:45 GST | /Windows/MEMORY.DMP |
| Offline files service started. | 2023-05-10 1:40:04 PM GMT+4 | /Windows/System32/winevt/Logs/Microsoft-Windows-OfflineFiles%4Operational.evtx |
| SMB BranchCache was disabled. | 2023-05-10 1:40:05 pm GMT+4 | Microsoft-Windows-BranchCacheSMB%4Operational.evtx |
| "Task Scheduler Service" Started 6.1.7600.16385 (win7\_rtm.090713-1255) | 2023-05-10 1:40:08 PM GMT+4 | Windows\Tasks\SchedLgU.txt |
| Network profile changed on an interface. | 2023-05-10 1:40:29 PM GMT+4 | Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall.evtx |
| Remote Desktop Services: Session logon succeeded: | 2023-05-10 1:40:51 PM GMT+4 | Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx |
| Listener RDP-Tcp received a connection | 2023-05-10 1:49:22 PM GMT+4 | Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx |
| Microsoft Defender Antivirus state updated to 7. | 2023-05-10 1:53:44 PM GMT+4 | Microsoft-Windows-Windows Defender%4WHC.evtx |
| Ransomware Deployed | 2023-05-10 1:58:04 PM GMT+4 | /Users/HOME LAB/Documents/RECOVER-yfkutt8-FILES.txt |
| Ransomware attack happened | 2023-05-10 1:58:15 GST | /Users/HOME LAB/Downloads/dnSpy-master.zip.yfkutt8 |

# Details of Analysis

The ransomware text **RECOVER-yfkutt8-FILES.txt** is found in many folders. The text details are as mentioned below.****

The file was created on 2023-05-10 at 1:59PM GST.

From the AmCache hive /Windows/AppCompat/Programs/Amcache.hve, it is found that there was an AnyDesk connection to the affected machine on the same day at 09:50:47 AM. This could be the connection made by the attacker. All the Anydesk logs are encrypted.

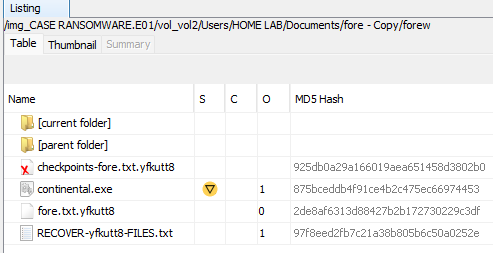


Upon analyzing the ShimCache details from /img\_CASE RANSOMWARE.E01/vol\_vol2/Users/HOME LAB/AppData/Local/Microsoft/Windows/UsrClass.dat, the folder Libraries\CLSID\_Documents Library\fore - Copy\forew( /img\_CASE RANSOMWARE.E01/vol\_vol2/Users/HOME LAB/Documents/fore - Copy/forew/) was accessed at 09:52.

*2023-05-10 09:52:27 | | | | | |Libraries\CLSID\_Documents Library\fore - Copy [Desktop\0\1\3\]*

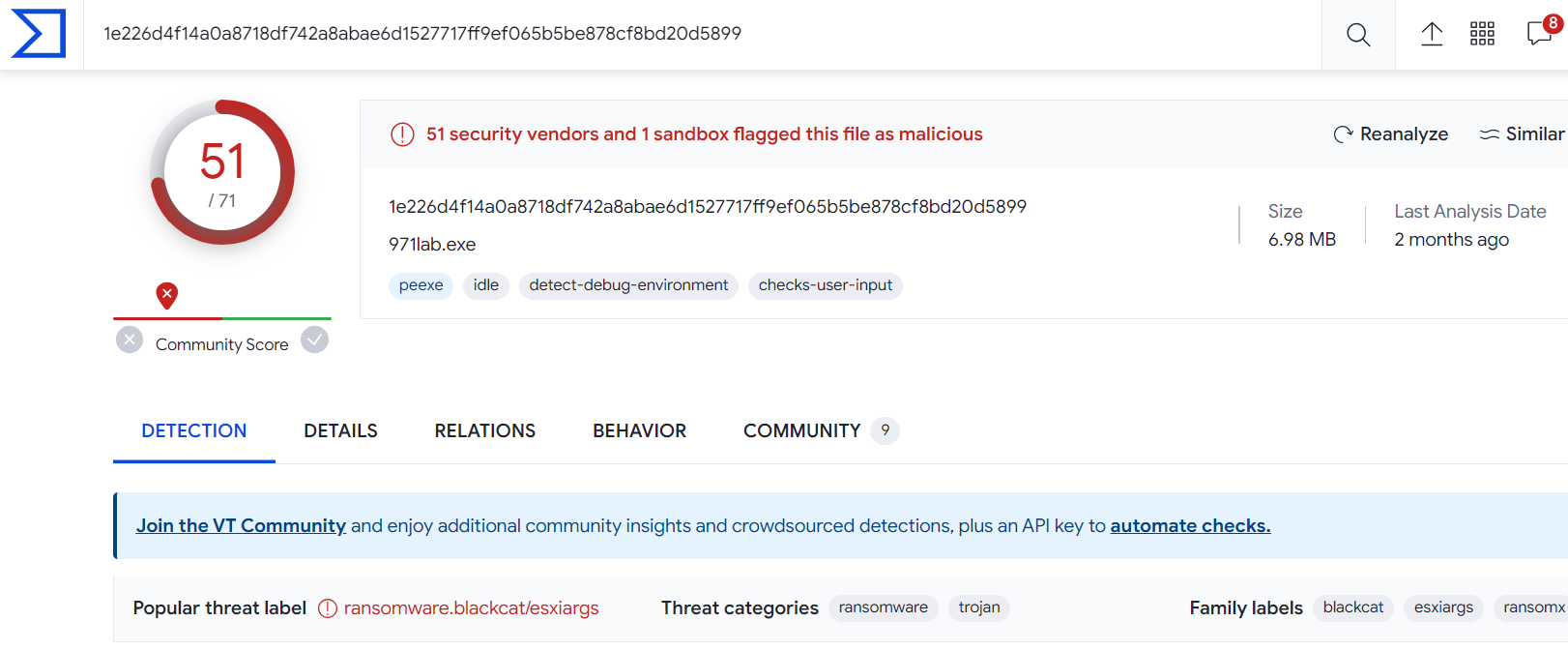
*2023-05-10 09:52:27 | | | | | |Libraries\CLSID\_Documents Library\fore - Copy\forew [Desktop\0\1\3\0\]*

The folder contains following files:



Continental.exe’s hash values:

MD5: 875bceddb4f91ce4b2c475ec66974453  
SHA-256: 1e226d4f14a0a8718df742a8abae6d1527717ff9ef065b5be878cf8bd20d5899

It is a ransomware from blackcat family: ransomware.blackcat/esxiargs

Imports from continental.exe ,Functionality imported from external dynamically linked libraries.

Bcrypt.dll netapi32.dll ws2\_32.dll

Kernel32.dll rstrtmgr.dll user32.dll

Shell32.dll advapi32.dll Userenv.dll

KERNEL32.dll ntdll.dl

Msvcrt.dll ole32.dll

**MITRE ATT&CK Tactics and Techniques for continental.exe**

Execution Defense Evasion Credential Access Discovery Collection

TA0002 TA005 TA006 TA007 TA009

# 

Another suspicious activity was found with the fakeransom.exe file. Upon analyzing the ntuser.dat from Location /img\_CASE RANSOMWARE.E01/vol\_vol2/Users/HOME LAB/NTUSER.DAT

We can view fakeransomware.exe file was downloaded 2022-07-31 04:26:27Z

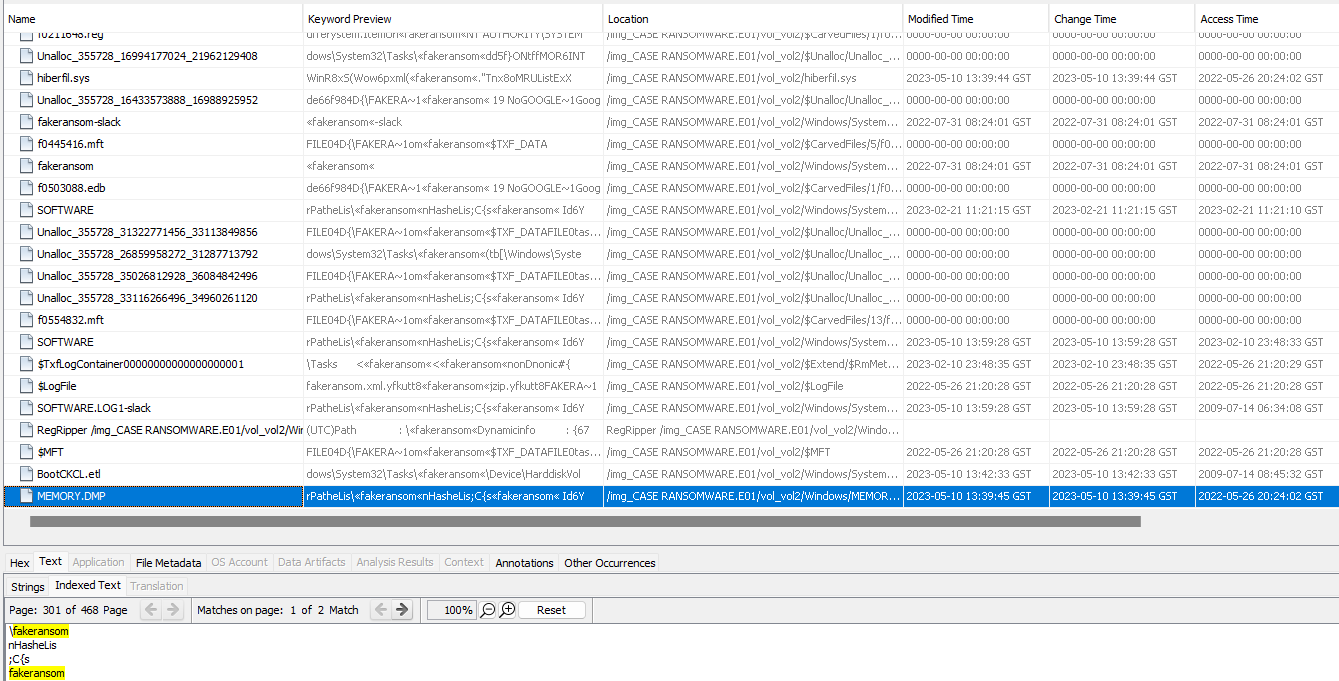
To further analyze this file, the task scheduler logs were searched from the location /img\_CASE RANSOMWARE.E01/vol\_vol2/Windows/System32/Tasks/fakeransom

The xml file shows the date of 2022-07-31T08:24:01.5516253 with the following command:



The file was deleted from the file location given in the above command so it is difficult to determine whether fakeransome.exe was benign or malicious.

There was also evidence that fakeransome was being run at the time as a memory dump seems to have taken place at: 2023-05-10 13:39:45 GST and as we can see in the image below, it was present.



# Conclusion

The forensic investigation has been undertaken with the primary objective of identifying the specific ransomware variant and the strategies and methodologies used by malicious actors. It is crucial to note that the breach was initiated on May 10, 2023, at 9:40 AM GST, persisting until May 10, 2023, at 1:58:15 PM GST. The ransomware responsible for the compromise is believed to be the "esxiargs" from "Blackcat" ransomware family.