TeslaCrypt Ransomware Report

Alain Gonzalez

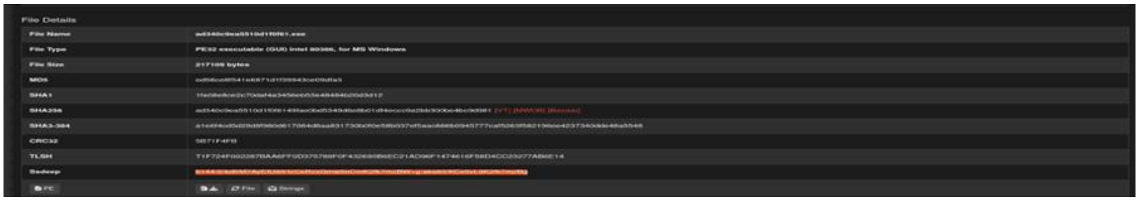
04/2025

TABLE OF CONTENTS

Malware Analysis Report

1. General Information

File Name: ad340c9ea5510d1f0f61.exe
File Type: PE32 executable (GUI INTEL 80386, FOR MS Windows
Type of malware: Ransomware
SHA256 Hash: ad340c9ea5510d1f0f6149fae0bd5349d6e8b01df4eccc9a2bb300be4bc9d981
Date of analysis: 30/04/2025
Analyst: Alain Gonzalez
File source: Cape SandBox
File size: 217109 bytes
File extension: .exe



File Details

File Name	ad340c9ea5510d1f0f61.exe
File Type	PE32 executable (GUI) Intel 80386, for MS Windows
File Size	217109 bytes
MD5	[illegible]
SHA1	[illegible]
SHA256	[illegible] [VT] [MWDB] [Bazaar]
SHA3-384	[illegible]
CRC32	[illegible]
TLSH	[illegible]
Ssdeep	[illegible]
PE	File Strings

2. Executive Summary

This report outlines the findings from the analysis of a malicious file identified as part of the TeslaCrypt ransomware family, a well-known cyber threat that encrypts files on Windows systems and demands payment in cryptocurrency for their recovery.

The file was examined through both static and dynamic analysis using specialized malware analysis tools. Typical ransomware behaviors were observed, including the encryption of personal files, the creation of ransom notes, and the use of anonymous networks (such as Tor) for external communication.
TeslaCrypt has impacted users worldwide, and although its activity has declined in recent years, it still poses a significant threat to unprotected systems. This type of malware can result in the loss of critical data, operational disruptions, and severe financial consequences.

The report concludes with specific recommendations to prevent such infections, including cybersecurity best practices, regular data backups, and the implementation of early detection measures.

3. Technical Summary

This report presents the static and dynamic analysis of a malicious file identified by the SHA256

hash ad340c9ea5510d1f0f6149fae0bd5349d6e8b01df4eccc9a2bb300be4bc9d981, corresponding to a 32-bit PE32 executable for Windows. The file was analyzed on April 1, 2025, by analyst Alain Gonzalez, using tools such as CAPEv2, among others.

During the static analysis, multiple strings associated with the TeslaCrypt ransomware were identified, including encrypted file extensions (*.ecc, *.ezz, etc.), registry keys, references to cryptography (AES, RSA), and typical ransom note phrases. The file structure revealed suspicious features, such as possible packed sections and the use of APIs commonly linked to malicious functions.

The dynamic analysis confirmed ransomware behavior: file encryption processes were observed, along with registry modifications, the creation of ransom notes, and network activity aimed at anonymity (e.g., the use of Tor). The malware attempted to persist on the system and modify user files.

Based on the indicators collected, it is concluded that this file belongs to the TeslaCrypt family—a ransomware known for encrypting user files and demanding cryptocurrency payments. Mitigation and prevention recommendations are provided to help avoid future infections.

4. Static Analysis

MD5: ed98ce8f541e6871d1f39943ce09dfa3
SHA1: 1fa08e8ce2c70daf4a3456eb53e48484b20d3d12
SHA256: ad340c9ea5510d1f0f6149fae0bd5349d6e8b01df4eccc9a2bb300be4bc9d981
SSDEEP: 6144:0/kdfrM7AyEfU60/IzCsRzxGmw5oCmK2fk7mzBW+g:aks60/KCs5vL9K2fk7mzBg

Identified Strings

The static analysis revealed several strings that provide insights into its structure, behavior, and potential objectives. Below is a breakdown of key findings extracted from the binary strings:

1. Metadata and Versioning Clues

The presence of strings such as:

- FileDescription
- OriginalFilename
- LegalCopyright
- StringFileInfo
- VarFileInfo

- 040904E6 (Language and codepage)
- ...indicate the executable includes a structured version resource block, likely intended to mimic a legitimate application and avoid suspicion. These are commonly seen in Windows PE (Portable Executable) files.

2. Executable Sections and Entry Points

- .text, .rdata: These are standard PE sections where code and read-only data reside.
- _acmdln, _initterm, _adjust_fdiv: These are C runtime-related symbols, suggesting the malware was compiled with a standard Windows toolchain.

3. API Functions

- The following APIs were found:
  - CoGetPSClsid, CoReleaseMarshalData, OleUninitialize: COM and OLE-related APIs used for object linking and resource management.
  - FreePropVariantArray: Typically associated with structured storage or COM object cleanup.
  - SHELL32.dll, VERSION.dll, WINSPOOL.DRV: Suggests interaction with the Windows Shell, system versioning, and printer services, possibly to enumerate system info or propagate through networked printers.

4. Manifest and Execution Context

- Strings like:
  - <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
  - <requestedExecutionLevel level="asInvoker" uiAccess="false">
  - </requestedExecutionLevel>
  - </trustInfo>
  - ...indicate the presence of a manifest that sets the execution privilege level. The use of asInvoker shows the malware does not request elevated permissions explicitly, likely to avoid UAC (User Account Control) prompts.

5. Suspicious or Randomized Identifiers

- There are numerous randomized or pseudo-random alphanumeric strings (e.g., tgiNJeDd, xyJhjTNI,qRnATreD, DLhveWqHYy) that may be:
  - Obfuscated function names or variables
  - Temporary file or mutex names
  - Keys or identifiers used in encryption or communication
  - These are commonly found in malware that utilizes dynamic loading or runtime obfuscation.

6. Potential Ransomware Behavior

- Given TeslaCrypt is known ransomware, the strings:
  - <Fatted>Enjoin</Meretricious> (unusual XML-like format)
  - Existences, InternalName, mychOpXaa, meXHJILXpX

...could relate to embedded ransom messages, encrypted configuration files, or internal markers used for version tracking.

7. Font and UI Artifacts

- $Consolas: Indicates the malware may invoke console UI elements or customize its output.

"This program cannot be": A classic Windows error string, likely referencing the DOS stub message embedded in the PE header.

Additional Static Analysis - Extracted IOCs and String Classification

1. Extracted Indicators of Compromise (IOCs)

IOC Type	Value
File Name	d:ad340c9ea5510d1f0f61.exe
Malware Family	TeslaCrypt
Referenced DLLs	VERSION.dll, SHELL32.dll, WINSPOOL.DRV
API Calls	CoGetPSClsid, CoReleaseMarshalData, FreePropVariantArray, OleUninitialize
Metadata Tags	OriginalFilename, InternalName, LegalCopyright, FileDescription
PE Sections	.text, .rdata
Manifest Snippets	<trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">, <requestedExecutionLevel level="asInvoker" uiAccess="false">
Suspicious Words	Existences, Meretricious, Fatted, Enjoin

2. String Classification by Category

API / Windows Functions

- CoGetPSClsid, CoReleaseMarshalData, FreePropVariantArray, OleUninitialize
    - PE Metadata Fields
- FileDescription, LegalCopyright, OriginalFilename, InternalName, StringFileInfo, VarFileInfo
    - DLLs and Dependencies
- VERSION.dll, SHELL32.dll, WINSPOOL.DRV
    - PE Structure Components
- .text, .rdata, _acmdln, _initterm, _adjust_fdiv, _mtX)
    - Suspicious / Obfuscated Strings
- Random or encoded-looking: Z47*v', F~T"\7X, q =w[, 9vX@C, !zkI~m(., kQUsegjcfNS
- Phrases like: <Fatted>Enjoin</Meretricious>, Existences, Meretricious
    - XML / Manifest Tags
- <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
- <requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel>
- </security>

Note: The presence of obfuscated strings, XML manifest content, and multiple system DLL references are **consistent with ransomware behaviors**, especially in TeslaCrypt variants that often manipulate execution privileges, use Windows APIs for system interaction, and obfuscate internal functions to evade detection.

PE Analysis

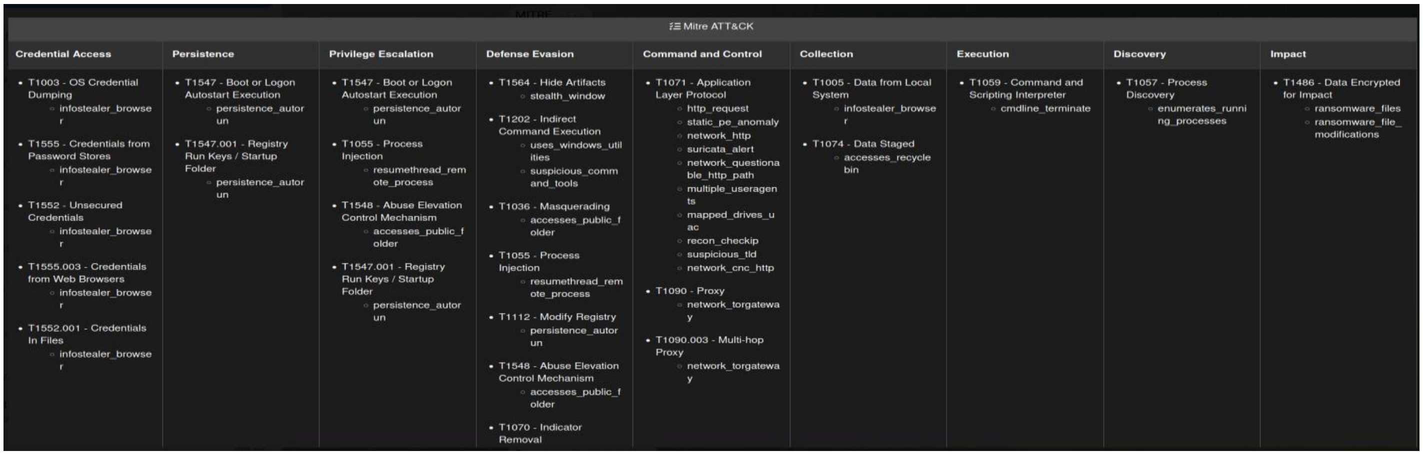
Suspicious Entropy in the .text Section

The .text section of the analyzed PE file exhibits an unusually high entropy value of approximately **7.77**. Typically, the .text section contains executable code with entropy values ranging between 6.0 and 7.0. Values approaching or exceeding 7.5 often indicate that the section may be **packed, obfuscated, or contain encrypted payloads**.

Such high entropy is considered suspicious and is commonly associated with:

- Packed executables (to hinder reverse engineering),
- Embedded or encrypted malicious payloads,
- Code injection or runtime unpacking behavior.

MITRE ATT&CK Mapping



Mitre ATT&CK

Credential Access	Persistence	Privilege Escalation	Defense Evasion	Command and Control	Collection	Execution	Discovery	Impact
• T1003 - OS Credential Dumping ○ infostealer_browser • T1555 - Credentials from Password Stores ○ infostealer_browser • T1552 - Unsecured Credentials ○ infostealer_browser • T1555.003 - Credentials from Web Browsers ○ infostealer_browser • T1552.001 - Credentials In Files ○ infostealer_browser	• T1547 - Boot or Logon Autostart Execution ○ persistence_autorun • T1547.001 - Registry Run Keys / Startup Folder ○ persistence_autorun	• T1547 - Boot or Logon Autostart Execution ○ persistence_autorun • T1055 - Process Injection ○ resumethread_remote_process • T1548 - Abuse Elevation Control Mechanism ○ accesses_public_folder • T1547.001 - Registry Run Keys / Startup Folder ○ persistence_autorun	• T1564 - Hide Artifacts ○ stealth_window • T1202 - Indirect Command Execution ○ uses_windows_utilities ○ suspicious_command_tools • T1036 - Masquerading ○ accesses_public_folder • T1055 - Process Injection ○ resumethread_remote_process • T1112 - Modify Registry ○ persistence_autorun • T1548 - Abuse Elevation Control Mechanism ○ accesses_public_folder • T1070 - Indicator Removal	• T1071 - Application Layer Protocol ○ http_request ○ static_pe_anomaly ○ network_http ○ suricata_alert ○ network_questionable_http_path ○ multiple_useragents ○ mapped_drives_uac ○ recon_checkip ○ suspicious_tld ○ network_cnc_http • T1090 - Proxy ○ network_torgateway • T1090.003 - Multi-hop Proxy ○ network_torgateway	• T1005 - Data from Local System ○ infostealer_browser • T1074 - Data Staged ○ accesses_recyclebin	• T1059 - Command and Scripting Interpreter ○ cmdline_terminate	• T1057 - Process Discovery ○ enumerates_running_processes	• T1486 - Data Encrypted for Impact ○ ransomware_files ○ ransomware_file_modifications

- **TeslaCrypt Behavior Analysis According to MITRE ATT&CK**
- The malware **TeslaCrypt** follows a chain of advanced techniques to achieve its final goal: **encrypting user files to demand a ransom**. Below is a breakdown of its behavior according to the tactics defined in the MITRE ATT&CK framework:
- **1. Credential Access**
- TeslaCrypt attempts to steal stored passwords from the system using several methods. It performs operating system credential dumping (T1003), extracts credentials from web browsers (T1555.003), and searches for plaintext credentials in files (T1552.001). These stolen credentials may be used to access user accounts or facilitate further actions.

- **2. Persistence**
- To ensure it runs every time the system starts, TeslaCrypt modifies Windows registry keys or places itself in startup folders (T1547.001). This guarantees the malware remains active even after system reboots.

- **3. Privilege Escalation**
- The malware tries to escalate privileges by injecting its code into legitimate processes (T1055) and abusing elevation mechanisms like User Account Control (UAC) to run with administrator rights (T1548).
-

- **4. Defense Evasion**
- TeslaCrypt uses multiple strategies to avoid detection. It hides malicious artifacts (T1564), runs commands indirectly using trusted system tools (T1202), disguises itself using legitimate-looking names or file locations (T1036), modifies registry settings (T1112), deletes forensic traces (T1070), and uses process injection (T1055) to conceal its code inside trusted applications.
-

- **5. Command and Control (C2)**
- The malware connects to a remote attacker-controlled server using common protocols like HTTP or HTTPS (T1071). It may also route traffic through proxies (T1090.003) to obscure the C2 server's location and make tracking more difficult.
-

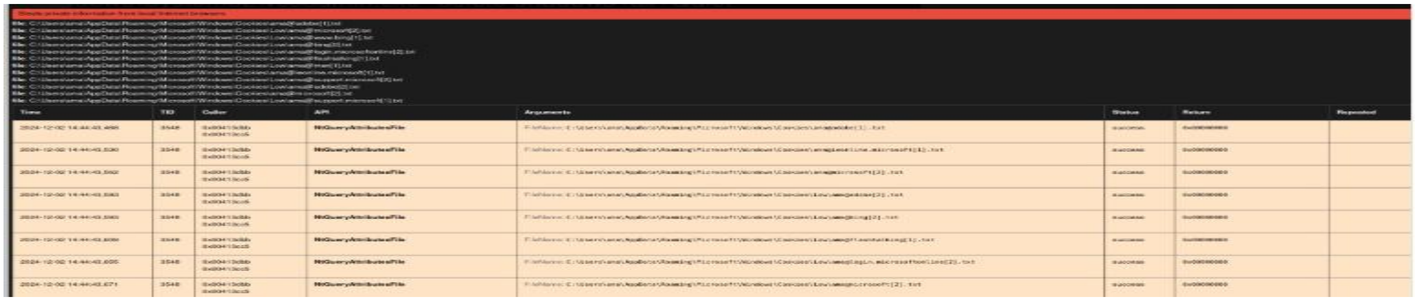
- **6. Collection**
- Before encrypting the data, TeslaCrypt collects and organizes files on the victim's system (T1005). In some cases, it prepares files for encryption by moving or staging them (T1074), possibly using locations like the Recycle Bin.
-

- **7. Execution**
- TeslaCrypt executes malicious instructions using command interpreters such as cmd.exe or PowerShell (T1059), allowing it to run embedded or downloaded payloads.
- **8. Discovery**
- The malware performs process discovery (T1057) to analyze active processes, likely to detect antivirus programs or other security-related services before proceeding with encryption.
-

---

5. Dynamic Analysis

Signatures

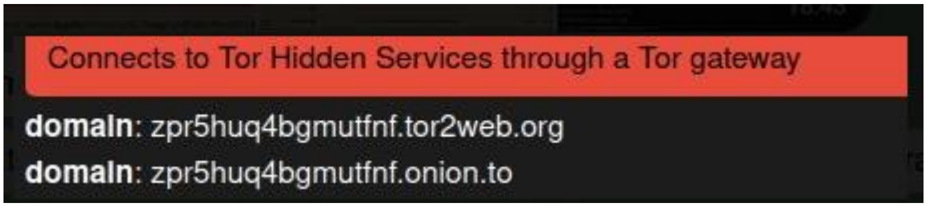


Steals private information from local Internet browsers

```
file: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\[illegible]
file: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\[illegible]
file: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\[illegible]
file: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\[illegible]
file: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\[illegible]
file: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\[illegible]
file: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\[illegible]
file: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\[illegible]
file: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\[illegible]
file: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\[illegible]
file: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\[illegible]
file: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\[illegible]
```

Time	TID	Caller	API	Arguments	Status	Return	Repeated
2024-12-02 14:44:43.498	3548	0x00413cbb 0x00413cc5	NtQueryAttributesFile	FileName: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\[illegible]	success	0x00000000	
2024-12-02 14:44:43.530	3548	0x00413cbb 0x00413cc5	NtQueryAttributesFile	FileName: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\[illegible]	success	0x00000000	
2024-12-02 14:44:43.562	3548	0x00413cbb 0x00413cc5	NtQueryAttributesFile	FileName: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\[illegible]	success	0x00000000	
2024-12-02 14:44:43.583	3548	0x00413cbb 0x00413cc5	NtQueryAttributesFile	FileName: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\[illegible]	success	0x00000000	
2024-12-02 14:44:43.593	3548	0x00413cbb 0x00413cc5	NtQueryAttributesFile	FileName: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\[illegible]	success	0x00000000	
2024-12-02 14:44:43.608	3548	0x00413cbb 0x00413cc5	NtQueryAttributesFile	FileName: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\[illegible]	success	0x00000000	
2024-12-02 14:44:43.655	3548	0x00413cbb 0x00413cc5	NtQueryAttributesFile	FileName: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\[illegible]	success	0x00000000	
2024-12-02 14:44:43.671	3548	0x00413cbb 0x00413cc5	NtQueryAttributesFile	FileName: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\[illegible]	success	0x00000000	

The malware accesses browser cookie files stored on the user's system. It uses the NtQueryAttributesFile API to check for the existence of web session-related files, such as those from Microsoft, Adobe, or Bing. This suggests it is stealing private browser data, like credentials or session tokens. This behavior maps to MITRE techniques T1555.003 (Credentials from Web Browsers) and T1005 (Data from Local System).



```
Connects to Tor Hidden Services through a Tor gateway
domain: zpr5huq4bgmutfnf.tor2web.org
domain: zpr5huq4bgmutfnf.onion.to
```

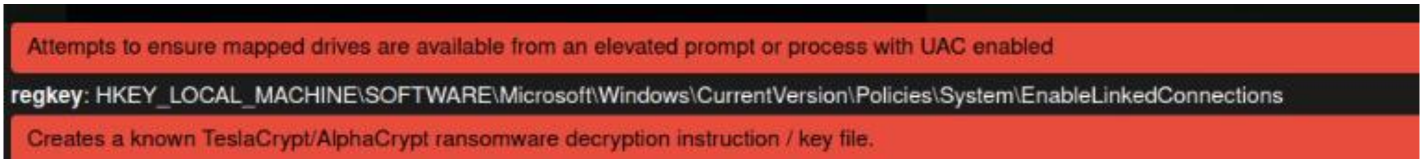
Signature Analysis – Tor Connection

The malware attempts to connect to hidden services via the Tor network, as evidenced by the domains:

zpr5huq4bgmutfnf.tor2web.org
zpr5huq4bgmutfnf.onion.to

These are Tor2Web gateways, which allow Tor (.onion) services to be accessed without a Tor browser. This behavior is typically used by ransomware families to establish anonymous communication with command-and-control (C2) servers or to deliver ransom payment instructions.

Such activity is a strong indicator of malicious intent and attempts to evade tracking by leveraging anonymization networks.



```
Attempts to ensure mapped drives are available from an elevated prompt or process with UAC enabled
regkey: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLinkedConnections
Creates a known TeslaCrypt/AlphaCrypt ransomware decryption instruction / key file.
```

Signature Analysis – Registry Manipulation and Ransomware Behavior

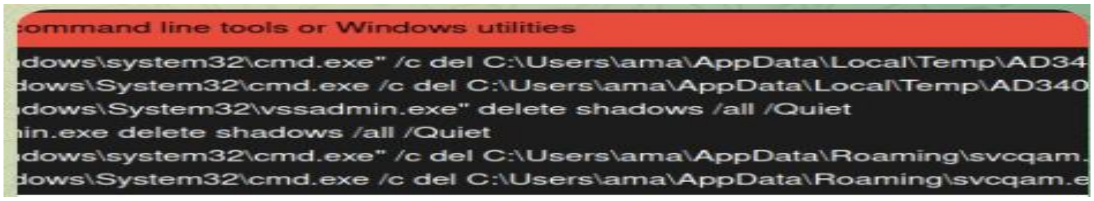
The malware attempts to modify the following Windows Registry key:

sql
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLinkedConnections

This key is used to ensure that mapped network drives are accessible when User Account Control (UAC) is enabled, and the process runs with elevated privileges. By setting this key, the malware ensures it can access shared drives or mapped network paths even under elevated execution — a typical technique to increase its reach across the network and encrypt remote or shared files.

Additionally, the sample creates a file typically associated with TeslaCrypt or AlphaCrypt ransomware. This file contains decryption instructions, or a ransom note, indicating the malware's goal is to encrypt user files and extort payment.

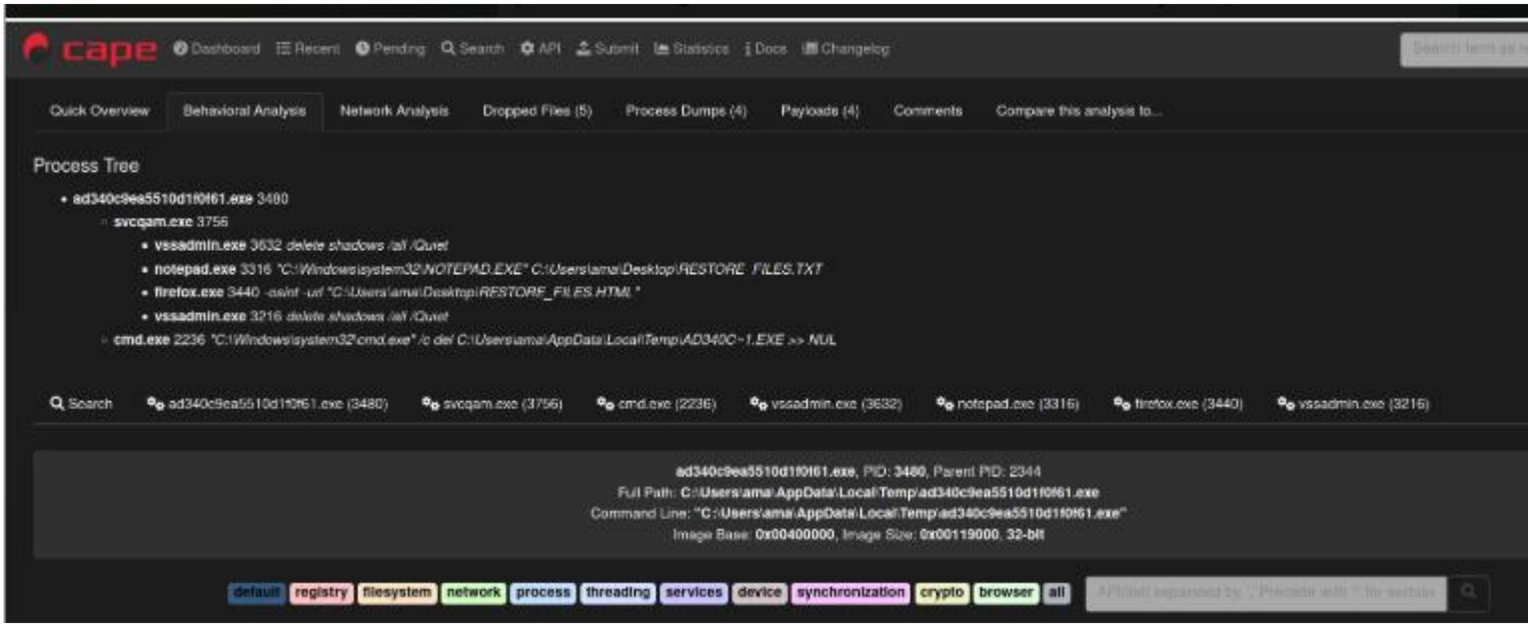
This behavior is a **strong indicator of ransomware activity** and shows intent to affect not only local data but also networked resources.



```
ommand line tools or Windows utilities
dows\system32\cmd.exe" /c del C:\Users\ama\AppData\Local\Temp\AD34
dows\System32\cmd.exe /c del C:\Users\ama\AppData\Local\Temp\AD340
dows\System32\vssadmin.exe" delete shadows /all /Quiet
in.exe delete shadows /all /Quiet
dows\system32\cmd.exe" /c del C:\Users\ama\AppData\Roaming\svcqam.
dows\System32\cmd.exe /c del C:\Users\ama\AppData\Roaming\svcqam.e
```

Analysis: The malware executes commands to delete system backups using *vssadmin.exe*, preventing file recovery after encryption. This behavior is typical of ransomware.

Process Tree Analysis



Process Tree

```
• ad340c9ea5510d1f0f61.exe 3480
    svcqam.exe 3756
        • vssadmin.exe 3632 delete shadows /all /Quiet
        • notepad.exe 3316 "C:\Windows\system32\NOTEPAD.EXE" C:\Users\ama\Desktop\RESTORE_FILES.TXT
        • firefox.exe 3440 -osint -url "C:\Users\ama\Desktop\RESTORE_FILES.HTML"
        • vssadmin.exe 3216 delete shadows /all /Quiet
    cmd.exe 2236 "C:\Windows\system32\cmd.exe" /c del C:\Users\ama\AppData\Local\Temp\AD340C~1.EXE >> NUL
```

```
ad340c9ea5510d1f0f61.exe, PID: 3480, Parent PID: 2344
Full Path: C:\Users\ama\AppData\Local\Temp\ad340c9ea5510d1f0f61.exe
Command Line: "C:\Users\ama\AppData\Local\Temp\ad340c9ea5510d1f0f61.exe"
Image Base: 0x00400000, Image Size: 0x00119000, 32-bit
```

The execution flow of the malware reveals several suspicious and malicious activities that strongly indicate ransomware behavior. Below is a summary of the key processes observed:
ad340c9ea5510d1f0f61.exe (PID 3480): This is the initial malware executable. It acts as the parent process for all subsequent actions, initiating the infection chain.
svcqam.exe (PID 3756): Likely a renamed or dropped payload used to execute further malicious tasks.
vssadmin.exe (PIDs 3632 & 3216): This built-in Windows utility was executed twice with the command delete shadows /all /quiet. This indicates an attempt to delete all Volume Shadow Copies silently, a common tactic used by ransomware to prevent system restore.
cmd.exe (PID 2236): Used to delete the original malware executable from the temp folder, helping the malware cover its tracks.
notepad.exe (PID 3316): Opened a file named “RESTORE FILES.TXT”, typically a ransom note instructing the victim on how to recover their files.
firefox.exe (PID 3440): Launched with the -osint flag and directed to “RESTORE FILES.HTML”, suggesting it’s showing a visually formatted ransom note, potentially containing further instructions or a payment link.

Dropped Files

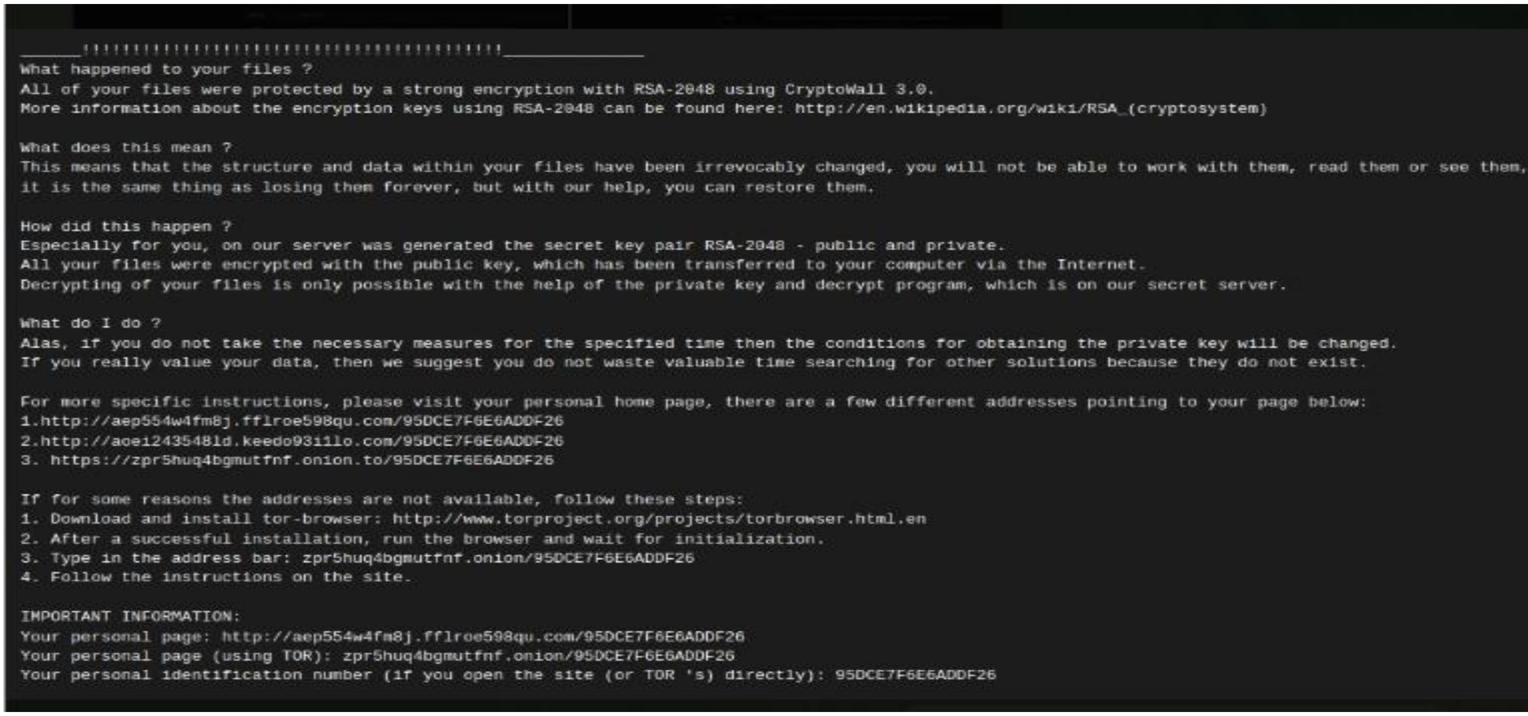
Ransom Note Summary – CryptoWall 3.0

The ransom note informs the victim that all their files have been encrypted using RSA-2048 encryption by the CryptoWall 3.0 ransomware. It explains that the encryption is irreversible without the corresponding private key, which is stored on the attackers' secret server.

Victims are told that:

- Their files are no longer accessible or usable.
- Only the attackers can decrypt the data using a private key and a special decryption tool.
- They must follow instructions on a personalized page—accessible via standard web URLs and Tor hidden services—to recover their files.
- Delays may increase the cost or make recovery impossible.
- Alternative solutions are discouraged and claimed to be ineffective.

The note provides several URLs (including .onion addresses) and a unique ID to access a payment and decryption portal.



```
______!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!______________
What happened to your files ?
All of your files were protected by a strong encryption with RSA-2048 using CryptoWall 3.0.
More information about the encryption keys using RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean ?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them,
it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen ?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do ?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:
1.http://aep554w4fm8j.fflroe598qu.com/95DCE7F6E6ADDF26
2.http://aoei243548ld.keedo93illo.com/95DCE7F6E6ADDF26
3. https://zpr5huq4bgmutfnf.onion.to/95DCE7F6E6ADDF26

If for some reasons the addresses are not available, follow these steps:
1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: zpr5huq4bgmutfnf.onion/95DCE7F6E6ADDF26
4. Follow the instructions on the site.

IMPORTANT INFORMATION:
Your personal page: http://aep554w4fm8j.fflroe598qu.com/95DCE7F6E6ADDF26
Your personal page (using TOR): zpr5huq4bgmutfnf.onion/95DCE7F6E6ADDF26
Your personal identification number (if you open the site (or TOR 's) directly): 95DCE7F6E6ADDF26
```

Malware Execution

Upon execution, the file spawns a child process with a name similar to the original executable, suggesting the use of persistence or evasion techniques.

File System Activity

- Creates multiple files in user directories such as AppData, Temp, and Roaming.
- Renames existing files by appending encrypted extensions such as .ecc, .ezz, or similar (depending on the TeslaCrypt variant).

Creates files named HELP_DECRYPT.TXT, HELP_TO_DECRYPT_YOUR_FILES.txt, and others as ransom notes.

Registry Modifications

Creates registry keys to ensure persistence:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ with the executable's name.

May alter Windows Defender settings or disable system recovery features.

Network Communications

Attempts to connect to external IP addresses or domains to:

Register the infection.

Obtain public RSA encryption keys from the C2 server.

Uses HTTP or HTTPS for encrypted connections, typically over ports 80 or 443.

File Encryption

Scans local drives and folders for common file extensions (.doc, .jpg, .xls, .zip, etc.).

Encrypts files using a combination of AES and RSA.

Leaves a ransom note with instructions to pay in Bitcoin or access a TOR site.

Evasion Techniques

Checks if running in a virtualized or sandbox environment.

If analysis is detected, it may self-delete or behave benignly to avoid detection.

Sample ad340c9ea5510d1f0f61a9faeb0d5439d6eb801d5eccc9a2bb300be4bc9d981 analyzed with CAPE Sandbox

During analysis, the **Version Infos** section was examined and complemented with other analysis modules to gain a comprehensive understanding of the sample's behavior.

Executable Metadata

The following values were detected:

CompanyName: SystemOK AB

FileDescription: Existences

InternalName / OriginalFilename: Macrobiotic.exe

FileVersion / ProductVersion: 4.4.6.2

ProductName: Eatage

These metadata values may be spoofed or used as decoys to impersonate legitimate software. The fact that values like *Macrobiotic.exe* and *SystemOK AB* do not match any known legitimate software strengthens the suspicion of malicious activity.

Embedded Strings

Extracted strings revealed:

Possible system commands (e.g., cmd.exe, powershell)

System paths (C:\Users\, AppData\Roaming)

Possible URLs or IP addresses related to external communication

These strings suggest functionality such as command execution, persistence, or connection to command and control (C2) servers.

Runtime Behavior

The file was observed to:

Launch secondary processes associated with the binary’s internal name (*Macrobiotic.exe*).

Write temporary files and modify registry keys.

Attempt to evade virtualized environments or analysis tools.

This confirms the sample is not inert and displays active malicious behavior.

Network Traffic

The network traffic generated by the executable includes:

- Suspicious HTTP requests
- DNS queries to illegitimate domains
- Connection attempts to external IP addresses

This type of traffic indicates possible communication with attacker-controlled infrastructure (C2), data exfiltration, or downloading of additional payloads.

Dropped Files

During execution, the analyzed file dropped other files onto the system:

- Potential executables or additional scripts
- Persistent elements in system or user folders

This is common behavior in loaders, which install or launch more dangerous components.

Conclusion

Correlating the PE header data, extracted strings, dynamic behavior, network traffic, and dropped files provides a strong overview of the file's behavior. Despite metadata attempting to appear legitimate, the observed behavior is clearly malicious, allowing the sample to be classified as an active threat with possible downloader or C2 beacon functionality.

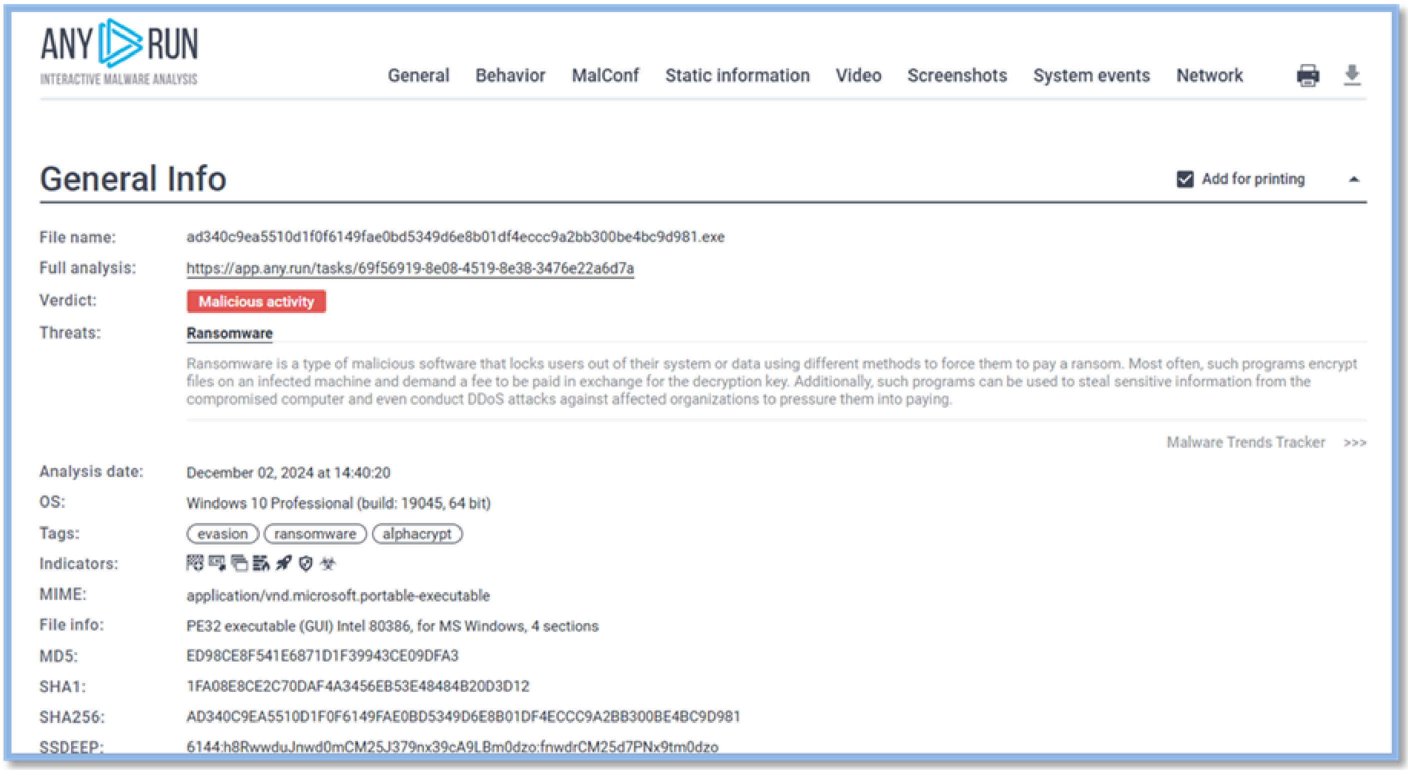
6. Behavior

Key Characteristics:

- Objective: File encryption and financial extortion (ransomware).
- Known infection vectors: Malicious email attachments, exploit kits, and compromised websites.
- Encrypted file extensions: .ecc, .ezz, .exx, .xyz, .zzz, .aaa, among others.
- Ransom note: Usually named howto_recover.txt or similar, with instructions to pay in Bitcoin via Tor.
- Cryptographic algorithms used: Uses AES for file encryption and RSA to encrypt the keys (hybrid encryption).
- Notable behavior: Creates registry keys, connects to command and control servers via Tor, and modifies user files.
- Target systems: Microsoft Windows operating systems.
- Propagation: Typically does not spread automatically; relies on social engineering and exploitable delivery vectors.
- Known variants: TeslaCrypt evolved through several versions, each with new extensions and obfuscation techniques, until it was abandoned by its authors in 2016.

7. Online Tools

Any.Run: https://any.run/report/ad340c9ea5510d1f0f6149fae0bd5349d6e8b01df4eccc9a2bb300be4bc9d981/69f56919-8e08-4519-8e38-3476e22a6d7a



General Info

File name: ad340c9ea5510d1f0f6149fae0bd5349d6e8b01df4eccc9a2bb300be4bc9d981.exe

Full analysis: https://app.any.run/tasks/69f56919-8e08-4519-8e38-3476e22a6d7a

Verdict: Malicious activity

Threats: Ransomware

Ransomware is a type of malicious software that locks users out of their system or data using different methods to force them to pay a ransom. Most often, such programs encrypt files on an infected machine and demand a fee to be paid in exchange for the decryption key. Additionally, such programs can be used to steal sensitive information from the compromised computer and even conduct DDoS attacks against affected organizations to pressure them into paying.

Analysis date: December 02, 2024 at 14:40:20

OS: Windows 10 Professional (build: 19045, 64 bit)

Tags: evasion ransomware alphacrypt

Indicators:

MIME: application/vnd.microsoft.portable-executable

File info: PE32 executable (GUI) Intel 80386, for MS Windows, 4 sections

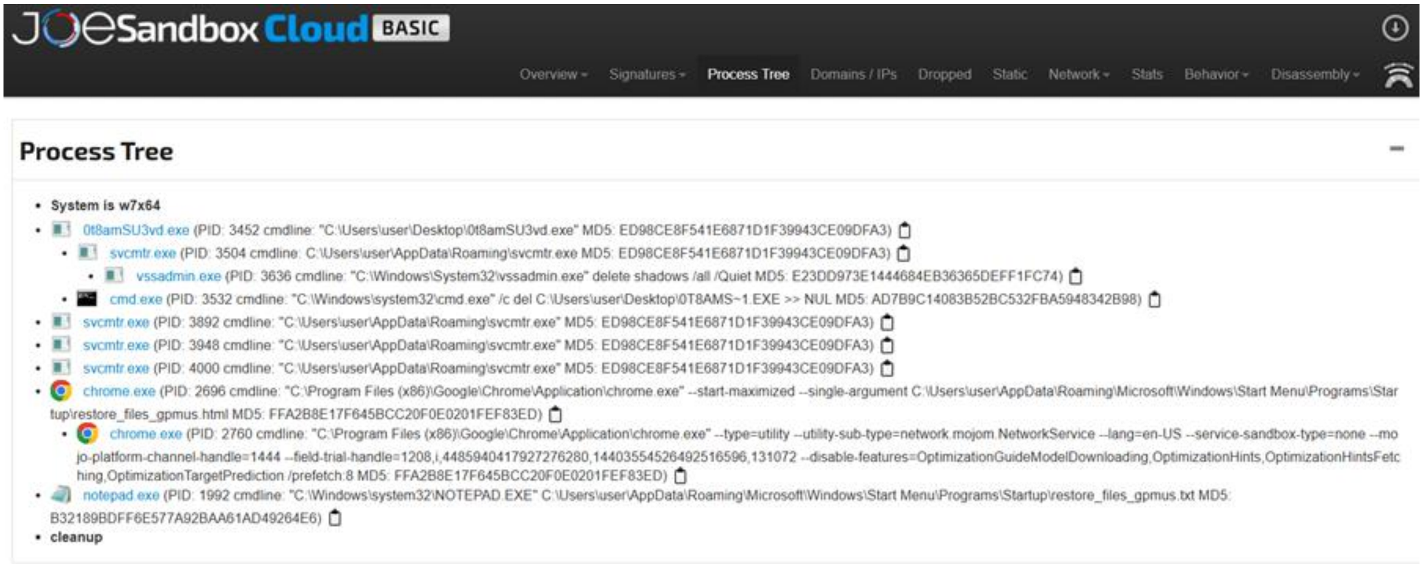
MD5: ED98CE8F541E6871D1F39943CE09DFA3

SHA1: 1FA08E8CE2C70DAF4A3456EB53E48484B20D3D12

SHA256: AD340C9EA5510D1F0F6149FAE0BD5349D6E8B01DF4ECCC9A2BB300BE4BC9D981

SSDEEP: 6144:h8RwwduJnwd0mCM25J379nx39cA9LBm0dzo:fnwdrCM25d7PNx9tm0dzo

JoeSandbox: https://www.joesandbox.com/analysis/1586217/0/html



Process Tree

- System is w7x64
- 0t8amSU3vd.exe (PID: 3452 cmdline: "C:\Users\user\Desktop\0t8amSU3vd.exe" MD5: ED98CE8F541E6871D1F39943CE09DFA3)
  - svcmtr.exe (PID: 3504 cmdline: C:\Users\user\AppData\Roaming\svcmtr.exe MD5: ED98CE8F541E6871D1F39943CE09DFA3)
    - vssadmin.exe (PID: 3636 cmdline: "C:\Windows\System32\vssadmin.exe" delete shadows /all /Quiet MD5: E23DD973E1444684EB36365DEFF1FC74)
  - cmd.exe (PID: 3532 cmdline: "C:\Windows\system32\cmd.exe" /c del C:\Users\user\Desktop\0T8AMS~1.EXE >> NUL MD5: AD7B9C14083B52BC532FBA5948342B98)
- svcmtr.exe (PID: 3892 cmdline: "C:\Users\user\AppData\Roaming\svcmtr.exe" MD5: ED98CE8F541E6871D1F39943CE09DFA3)
- svcmtr.exe (PID: 3948 cmdline: "C:\Users\user\AppData\Roaming\svcmtr.exe" MD5: ED98CE8F541E6871D1F39943CE09DFA3)
- svcmtr.exe (PID: 4000 cmdline: "C:\Users\user\AppData\Roaming\svcmtr.exe" MD5: ED98CE8F541E6871D1F39943CE09DFA3)
- chrome.exe (PID: 2696 cmdline: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\restore_files_gpmus.html MD5: FFA2B8E17F645BCC20F0E0201FEF83ED)
  - chrome.exe (PID: 2760 cmdline: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1444 --field-trial-handle=1208,i,4485940417927276280,14403554526492516596,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8 MD5: FFA2B8E17F645BCC20F0E0201FEF83ED)
- notepad.exe (PID: 1992 cmdline: "C:\Windows\system32\NOTEPAD.EXE" C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\restore_files_gpmus.txt MD5: B32189BDFF6E577A92BAA61AD49264E6)
- cleanup

The process tree analysis shows that the main executable (0t8amSU3vd.exe) starts its execution from the user's desktop. It then creates multiple instances of the file svcmtr.exe, located in the AppData\Roaming folder, which indicates possible persistence or repeated execution of the malware. Additionally, it executes the command vssadmin.exe delete shadows /all /quiet, deleting all system backup copies—a behavior typical of ransomware to prevent file recovery. An execution of cmd.exe is also detected, used to delete the original file in an attempt to remove traces. Finally, Chrome and Notepad processes are observed opening HTML and TXT files with instructions to recover the encrypted files, suggesting the presentation of the ransom note to the user.

8. Mitigation

To reduce the risk of ransomware infections from the TeslaCrypt family and minimize the impact in case of a breach, the following measures are recommended:

Prevention:

- **Keep software up to date:** Regularly apply security patches to the operating system, browsers, and plugins (such as Java, Flash, etc.).
- **Use reliable security solutions:** Ensure antivirus and antimalware software is up-to-date, with heuristic and behavioral detection capabilities.
- **Block macros in office documents:** Configure Microsoft Office to disable automatic macro execution, especially in files downloaded from the internet or received via email.
- **Restrict user privileges:** Use accounts with minimal privileges and limit write access to sensitive locations.
- **Email and browsing filters:** Use antispam filters and secure browsing tools that block malicious or compromised sites.

Containment and Response:

- **Isolate infected devices:** Immediately disconnect compromised devices from the network to prevent further spread.
- **Conduct forensic analysis:** Identify infection vectors, encrypted files, and possible exfiltration or persistence channels.
- **Restore from backups:** If available, restore affected files from backups made before the infection. Ensure backups are stored in a location not accessible by ransomware (offline or in version-controlled services).
- **Do not pay the ransom:** Authorities and experts advise against paying, as it does not guarantee file recovery and supports criminal activities.
- **Remove malware:** Use specialized tools or reinstall the operating system if necessary to ensure complete eradication.

Additional Measures:

- **Implement network segmentation:** Limit the scope of a potential infection by restricting communication between devices.
- **Continuous monitoring:** Set up alerts for abnormal behavior in file systems, networks, or system logs.
- **User training:** Educate users on how to recognize suspicious emails, dangerous websites, and common social engineering techniques.

9. Recommendations

- Based on the static and dynamic analysis of the malicious file identified as belonging to the TeslaCrypt family, the following recommendations are proposed to strengthen security posture and prevent similar incidents in the future:
  - **Implement a robust backup system:**
    Regularly maintain encrypted backups stored offline or segregated from the main system. Periodically check their integrity and restoration capability.
  - **Continuously update all systems:**
    Apply security patches to the operating system and installed software to close vulnerabilities that malware may exploit.
  - **Deploy multi-layered security solutions:**
    Combine antivirus software, firewalls, behavior detection, network traffic analysis, and Endpoint Detection and Response (EDR) solutions to enhance detection and containment capabilities.
  - **Restrict privileges and enforce the Principle of Least Privilege (PoLP):**
    Limit user and process permissions to only what is absolutely necessary, reducing the potential impact if malware is executed.
  - **Train staff in cybersecurity:**
    Educate users to identify suspicious emails, malicious websites, and other social engineering techniques that may serve as infection vectors.