LONDON METROPOLITAN UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CC6011NI Digital Investigation and E-Discovery

Assessment Weightage & Type

50% Individual Report

Year and Semester

2023-24 Autumn

Student Name: Sharams Kunwar

London Met ID: 21049701

College ID: np01nt4a210112

Assignment Due Date: 11th January 2024

Assignment Submission Date: 11th January 2024

Word Count: 1798

I confirm that I understand my report needs to be submitted online via Google Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a marks of zero will be awarded.

Table of Contents

Table of Figures

ABSTRACT

This report delves into the evolving landscape of digital crimes, focusing on the notorious ZeuS Trojan and its impact on cybersecurity. Through an exploration of historical context, functionalities, tactics, and a simulated attack scenario, the aim is to propose effective detection and investigation strategies to mitigate ZeuS' impact. The report successfully achieves its objectives by analyzing the ZeuS malware's evolution, its notable case studies, and presenting practical insights and recommendations. The simulated attack scenario illustrates the real-world implications, emphasizing the importance of a multi-layered cybersecurity approach. The report concludes with preventive measures and recommendations, guiding organizations and individuals to enhance their defenses against ZeuS and similar threats in our constantly evolving digital landscape.

1 Introduction

1.1 Subject Matter

Digital crimes have become a significant concern in today's interconnected world. They can be increased in scale by the use of computers, computer networks, or other forms of ICT (HMICFRS, 2023). Cybercriminals wreak havoc in a multitude of ways—identity theft, cyberbullying, data leakage, distributed denials of service, and **malware attacks** (Cameron, 2018).

Malware, short for "malicious software," can compromise a system by performing an unauthorized function or process (Malwarebytes, 2021).

As of 2023, the top malware strains included remote access Trojans (RATs), banking Trojans, information stealers, and ransomware (CIS, 2023). The list is similar to that of 2021. Most of these malware strains have been in use for more than five years, with their respective code bases evolving into multiple variations (CISA, 2022).

One of the notably repeated strains in these lists is the ZeuS malware, alternatively referred to as ZeuS/Zbot, which operates through a client/server model, enabling perpetrators to establish massive botnets and steal financial credentials. This malware has emerged as a pervasive and impactful network security threat on a global scale, significantly impacting the landscape of digital crimes. Notably, it has infiltrated over 3 million computers within USA, with prominent organizations such as NASA and Bank of America as its victim (cynet, 2023). Despite efforts to curb its activity multiple times, ZeuS continues to evolve and remain active, demonstrating the persistent and adaptable nature of such digital threats (Westervelt, 2014).

1.2 Evolution of ZeuS Malware

Appendix-1

1.3 Aim and Objectives

1.3.1 Aim

The main aim of this report is to gain insights into the evolving landscape of digital crime, with a specific focus on the notorious ZeuS Trojan, and propose effective detection and investigation strategies to mitigate its impact.

1.3.2 Objectives

- To investigate the historical context and evolution of digital crimes.
- To analyse the functionalities and tactics employed by threat actors using the ZeuS Trojan.
- To demonstrate a simulated attack scenario to illustrate the real-world implications of ZeuS.
- To present detection and investigation methodologies to counter ZeuS-related threats.
- To provide practical insights and recommendations for enhancing cybersecurity measures against ZeuS and similar threats.

2 Background/Literature Review

2.1 ZeuS-In-Detail

Appendix-2

2.2 Case study

ZeuS was first identified in 2007 (Vaidya, 2015). The cyberattack revealed vulnerabilities in security systems of major entities like the U.S. Department of Transportation and companies like Booz Allen, Unisys, Hewlett-Packard, and Hughes Network Systems. Fake job listings tricked employees into downloading NTOS.exe malware, stealing confidential data and transmitting it to Yahoo Inc., using a discreet strategy, with limited targets to bypass detection and security protocols. The ZeuS attack targeted several high-profile organizations, with only Unisys acknowledging the virus detection and removal. British internet security provider Prevx identified the malware and raised alarms, highlighting the complexity of the threat. The malware's ability to go undetected and the lack of advanced security features exacerbated the situation. Prevx CEO Mel Morris publicly named the victims and cooperated with the FBI's Law Enforcement Online program to investigate the vulnerabilities (Reuters, 2007).

Later, in 2009, Jacques Erasmus and his research team at Prevx exposed a cache of FTP credentials, exposing high-profile domains as potential victims of the ZeuS Trojan, which infiltrated systems and extracted stored FTP credentials and other sensitive information. Over 74,000 accounts were compromised, with notable entities like NASA, Cisco, Kaspersky, McAfee, Symantec, Amazon, Bank of America, Oracle, ABC, BusinessWeek, Bloomberg, Disney, Monster, and the Queensland government domain among the victims (Ragen, 2009).

2.3 Analysis

ZeuS employs two primary infection methods: drive-by downloads and spam messages. In the incident of 2007, it victimized employees using spam messages linked to fake job listings luring them to download malware – "NTOS.exe".

ZeuS's functionality is extensive, involving stolen data exfiltration and remote commands through encrypted HTTP POST requests to a Command and Control (C&C) server. It can be seen doing the same here by transmitting confidential data to Yahoo Inc., bypassing detection, and security protocols.

The attack compromised over 74,000 accounts, emphasizing the widespread impact of ZeuS. Victims of ZeuS include NASA, Cisco, Kaspersky, McAfee, Symantec, Amazon, Bank of America, Oracle, ABC, BusinessWeek, Bloomberg, Disney, Monster, and the Queensland government.

It managed to remain undetected as the victims themselves didn't know they were infected. Also, ZeuS had been seen linked to the emails that offer "Microsoft Outlook Critical Updates" by linking to a long, confusing URL:

```
update microsoft com kiffil com mx/microsoftofficeupdate/isapdl/default.aspx?ln=en-
us&id=51168819316874756664669014767816637995466048506302358260
```

Figure 1 URL linked to ZeuS (Ragen, 2009)

It may have contributed to its low profile. It also runs with "low" integrity reducing suspicion.

The attack of such scale in such notable organizations revealed weaknesses in security systems and prompted responses from organizations and law enforcement. Prevx, an internet security provider, played a crucial role in identifying and raising alarms about malware.

The ZeuS case study serves as a reminder of the evolving nature of cyber threats and the critical role of cybersecurity measures in safeguarding organizations against sophisticated malware attacks.

3 Demonstration

In this section, an attack-scenario has been simulated similar to that of forementioned case-study to illustrate its real-world implications.

Zeus-Malware Sample:

https://github.com/ytisf/theZoo/tree/master/malware/Binaries/ZeusBankingVersion_26Nov2013

3.1 Attack

A phishing mail was sent to the victim by attaching malicious file.

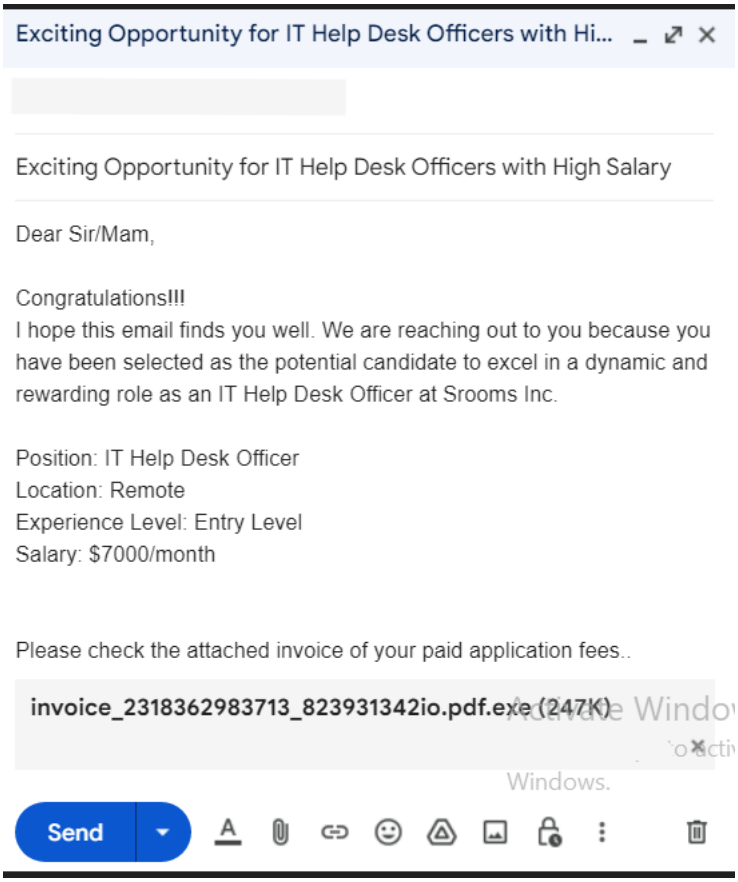


Figure 2 Phishing Mail delivered to Victim.

Victim clicks on the invoice and downloads the malicious file into his PC.

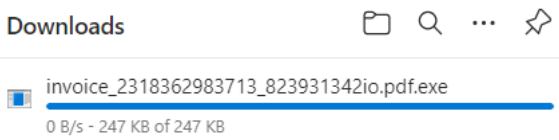


Figure 3 Victim Downloading Malicious File to his PC.

Victim/User clicks on the pdf file to open it. Instead, a prompt to install Adobe Flash Player is displayed.

Figure 4 Prompt to install Adobe Flash Player

Shortly after, the file deletes itself from the PC and it can no longer be discovered.

4 Investigation and Detection

4.1 Static Analysis

The file was analyzed before execution, viewing its hashes, and checking if it had been flagged as malicious , previously inputting its hashes into the VirusTotal database. Also, its API calls and

function calls were analyzed to identify its potential actions and ease the process of dynamic analysis.

4.1.1 Overview

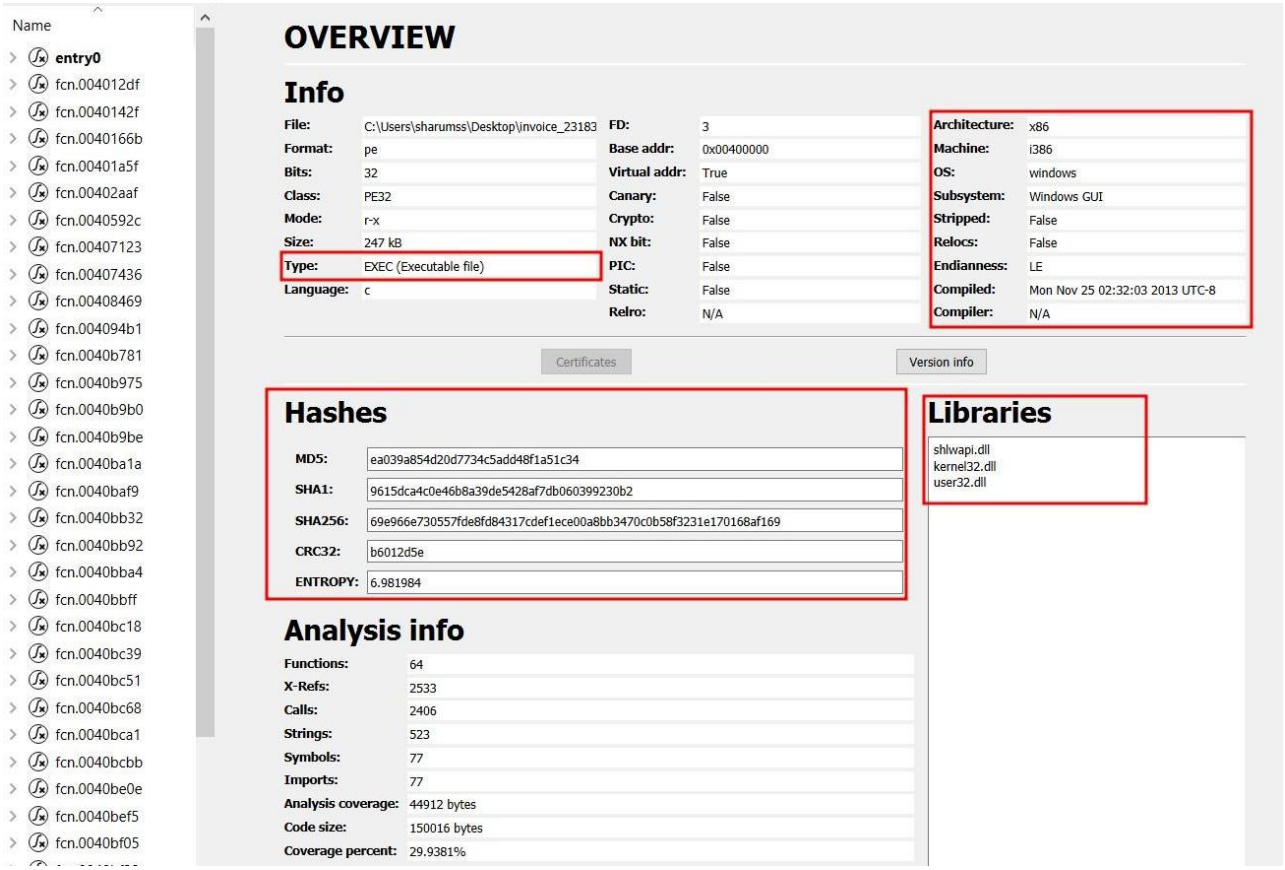


Figure 6 Cutter Overview

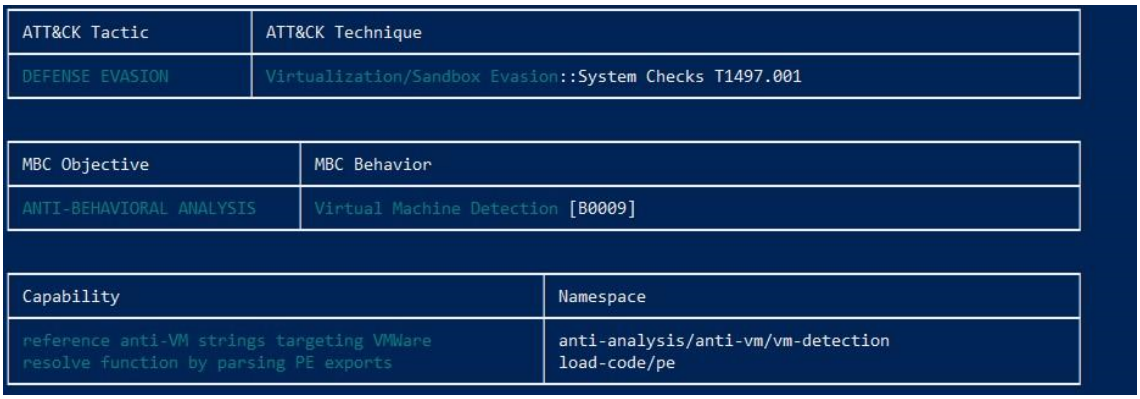
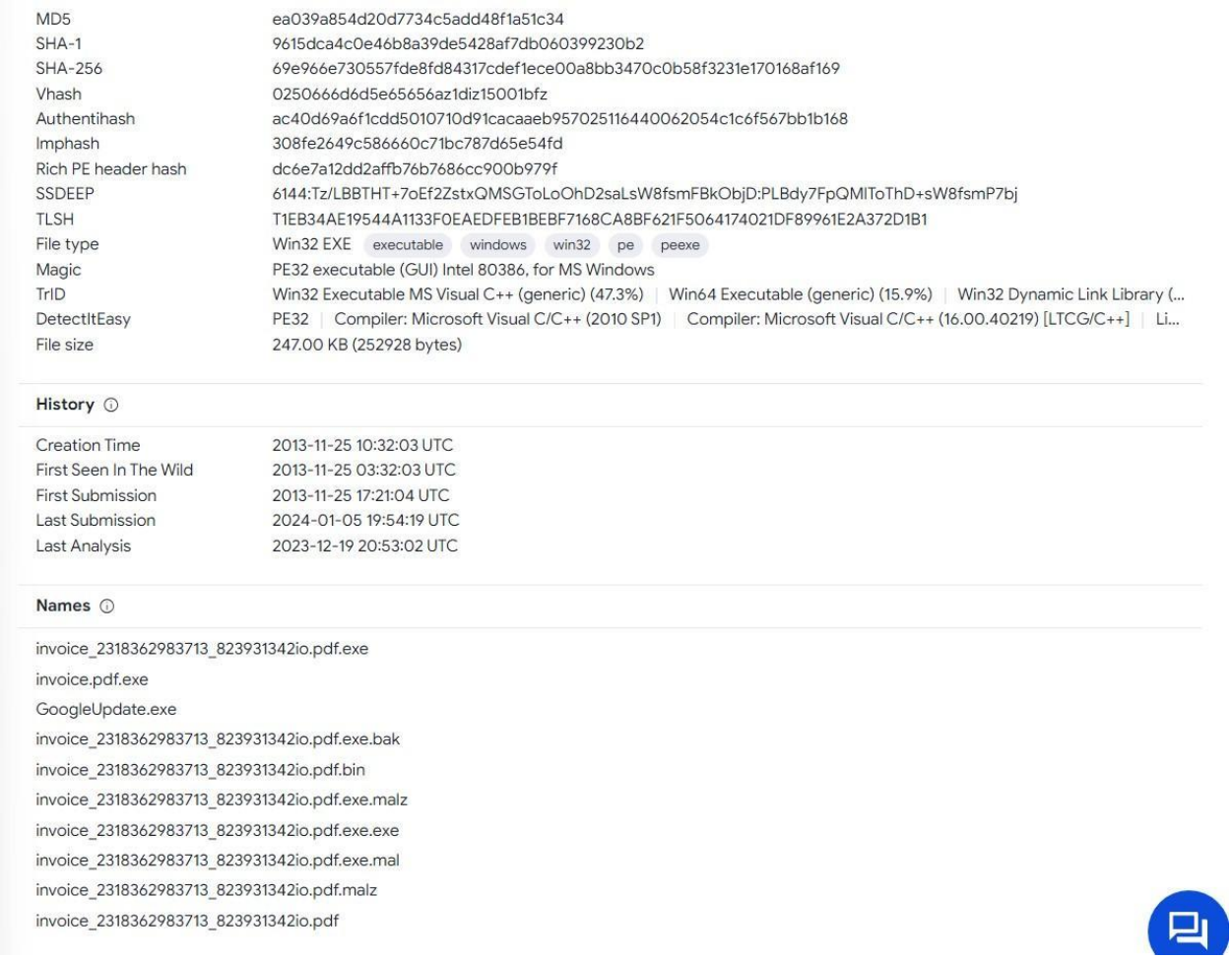


Figure 7 Capa overview

4.1.2 VirusTotal Check

Fortinet	W32/Generic.AC.3F8DF6!tr	GData	Win32.Trojan.Agent.TKFRZ8
Google	Detected	Gridinsoft (no cloud)	Trojan.Win32.Gen.cc!s4
Ikarus	Trojan-Spy.Zbot	Jiangmin	Backdoor/ZAccess.psh
K7AntiVirus	RootKit (004b9ee21)	K7GW	RootKit (004b9ee21)
Kaspersky	Backdoor.Win32.ZAccess.evyo	Kingsoft	Malware.kb.a.1000
Lionic	Trojan.Win32.ZAccess.tnpa	Malwarebytes	Sirefef.Trojan.Bot.DDS
MAX	Malware (ai Score=100)	MaxSecure	Trojan.Malware.6700596.susgen
McAfee	Generic.ru	Microsoft	TrojanDropper:Win32/Sirefef.gen!B
NANO-Antivirus	Trojan.Win32.ZAccess.cqjtnp	Panda	Trj/WLT.A
QuickHeal	TrojanDropper.Sirefef.A9	Rising	Dropper.Sirefef!8.525 (TFE:2:1ubYWh7D..
Sangfor Engine Zero	Suspicious.Win32.Save.a	SentinelOne (Static ML)	Static AI - Malicious PE
Skyhigh (SWG)	BehavesLike.Win32.Generic.dh	Sophos	Troj/Agent-AEYC
SUPERAntiSpyware	Backdoor.ZAccess/Variant	Symantec	ML.Attribute.HighConfidence
TACHYON	Backdoor/W32.ZAccess.252928.B	Tencent	Malware.Win32.Gencirc.1159ee79
Trapmine	Malicious.high.ml.score	Trellix (FireEye)	Generic.mg.ea039a854d20d773
TrendMicro	BKDR_SIREFEF.NIS	TrendMicro-HouseCall	BKDR_SIREFEF.NIS
Varist	W32/Zbot.QZDC-5119	VBA32	SScope.Trojan-Dropper.31107
VIPRE	Trojan.WLDCR.C	VirIT	Trojan.Win32.Dropper.JH
Webroot	W32.Trojan.Gen	Xcitium	Malware@#3cscsamn9ftuw
Yandex	Backdoor.ZAccess!UkzQ0/sevQU	Zillya	Backdoor.ZAccess.Win32.30281
ZoneAlarm by Check Point	Backdoor.Win32.ZAccess.evyo	Zoner	Trojan.Win32.19899

Figure 8 Vendor Analysis



MD5	ea039a854d20d7734c5add48f1a51c34
SHA-1	9615dca4c0e46b8a39de5428af7db060399230b2
SHA-256	69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169
Vhash	0250666d6d5e65656az1diz15001bfz
Authentihash	ac40d69a6f1cdd5010710d91cacaaeb95702511644006205 4c1c6f567bb1b168
Imphash	308fe2649c586660c71bc787d65e54fd
Rich PE header hash	dc6e7a12dd2affb76b7686cc900b979f
SSDEEP	6144:Tz/LBBTHT+7oEf2ZstxQMSGToLoOhD2saLsW8fsmFBkObjD:PLBdy7FpQMlToThD+sW8fsmP7bj
TLSH	T1EB34AE19544A1133F0EAEDFEB1BEBF7168CA8BF621F5064174021DF89961E2A372D1B1
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 Executable MS Visual C++ (generic) (47.3%) | Win64 Executable (generic) (15.9%) | Win32 Dynamic Link Library (...
DetectItEasy	PE32 | Compiler: Microsoft Visual C/C++ (2010 SP1) | Compiler: Microsoft Visual C/C++ (16.00.40219) [LTCG/C++] | Li...
File size	247.00 KB (252928 bytes)

History

Creation Time	2013-11-25 10:32:03 UTC
First Seen In The Wild	2013-11-25 03:32:03 UTC
First Submission	2013-11-25 17:21:04 UTC
Last Submission	2024-01-05 19:54:19 UTC
Last Analysis	2023-12-19 20:53:02 UTC

Names

invoice_2318362983713_823931342io.pdf.exe
invoice.pdf.exe
GoogleUpdate.exe
invoice_2318362983713_823931342io.pdf.exe.bak
invoice_2318362983713_823931342io.pdf.bin
invoice_2318362983713_823931342io.pdf.exe.malz
invoice_2318362983713_823931342io.pdf.exe.exe
invoice_2318362983713_823931342io.pdf.exe.mal
invoice_2318362983713_823931342io.pdf.malz
invoice_2318362983713_823931342io.pdf

Figure 9 About file

4.1.3 PEstudio Analysis

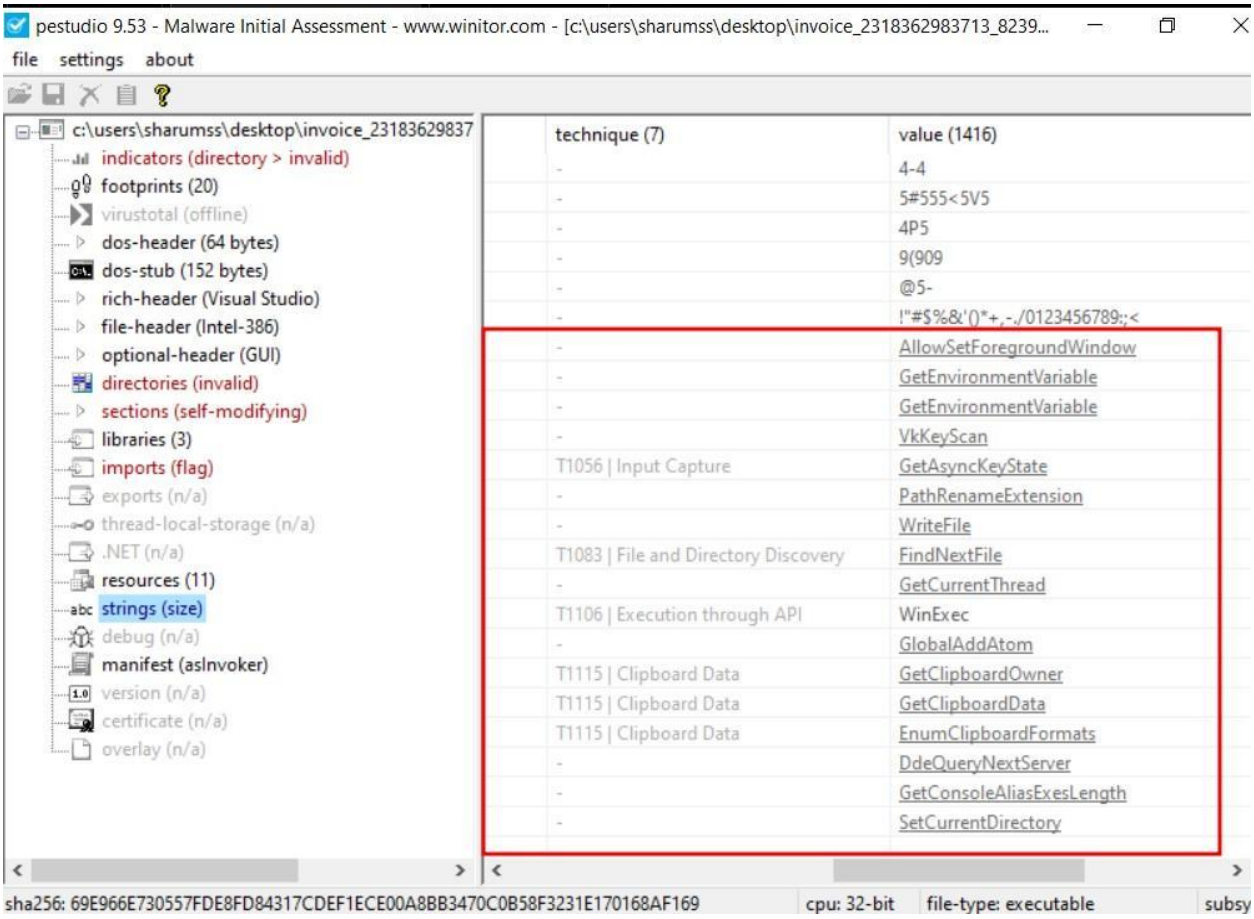


Figure 10 Flagged API calls.

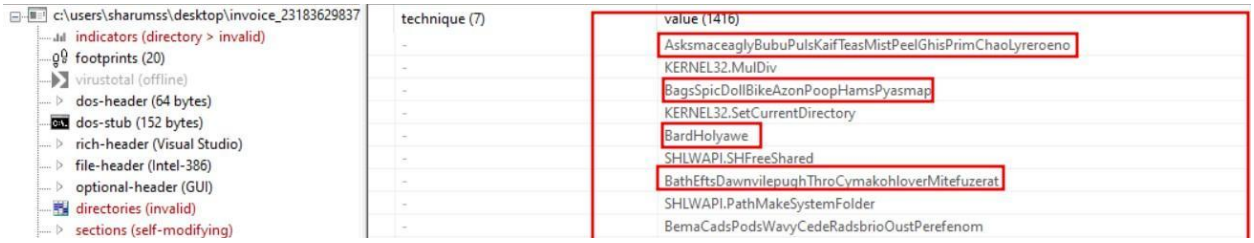


Figure 11 Suspicious Function calls (gibberish)

library (3)	duplicate (0)	flag (0)	bound (0)	first-thunk-original (INT)	first-thunk (IAT)	type (1)
SHLWAPI.dll	-	-	-	0x00020208	0x00020078	implicit
KERNEL32.dll	-	-	-	0x00020190	0x00020000	implicit
USER32.dll	-	-	-	0x00020260	0x000200D0	implicit

Figure 12 Libraries

4.1.4 Function calls

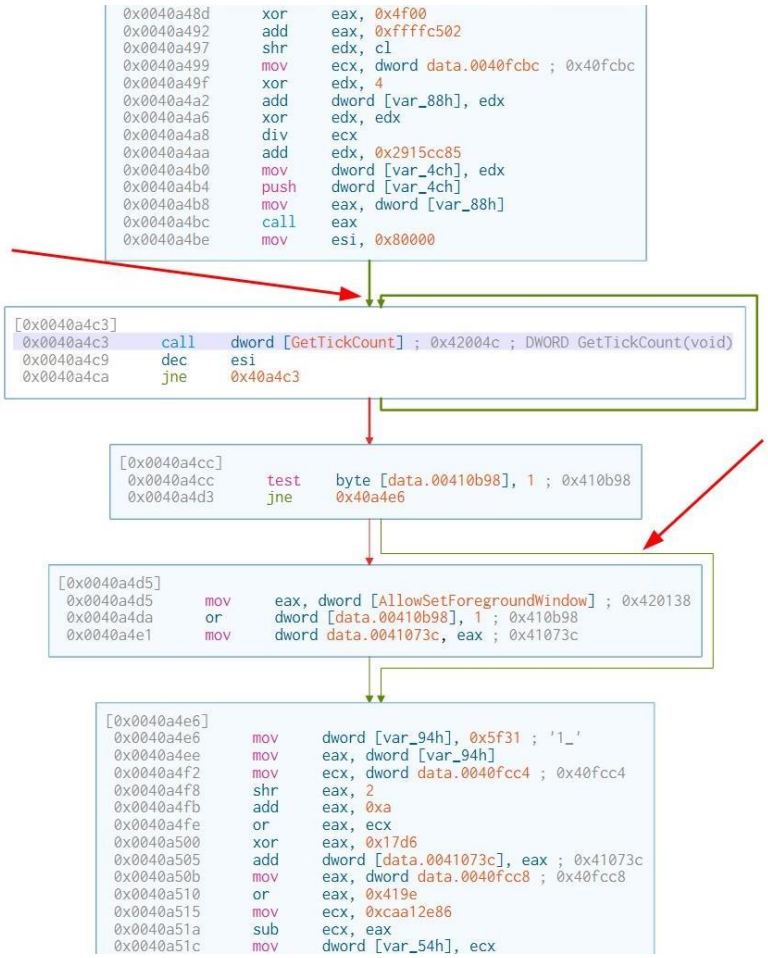


Figure 13 Graph of function calls before exporting.

4.1.4.1 Json of Function calls exported using Cutter.

Analyzing the Json file, it has many suspicious function calls, especially “0x40a3b6: call 0x40a3e8” raises the suspicion significantly as it calls an internal function within the malware, which is often used for malicious tasks like downloading and executing additional malware. The malware creates a new thread to download and execute the additional malware, terminating the thread after it finishes executing.

4.2 Dynamic Analysis

Dynamic analysis revealed a malicious file posing as an Adobe Flash Player installation triggered a series of alarming events, including tampering with Google updates registry key values and suspicious Chrome processes running'setup.exe.' The malicious files were discovered in the system, indicating the installation of backdoors designed to achieve persistence and evade detection. Procmon analysis revealed a stealthy process named "Microsoft.Photos.exe" running continuous process profiling operations, despite limited access. The malicious process made significant changes in the registry, downloaded, and interacted with backdoor files, and unlocked local files. The discovery triggered a cascade of malicious activities, including 'HxTsr.exe' masquerading as a Microsoft Outlook component, modifying system files and registry entries, and potentially stealing sensitive data. Network analysis revealed requests for client metadata, certificate validation, and suspicious HTTP requests to various servers. The attack was sophisticated, involving backdoors, manipulation of system processes, and extensive network interactions aimed at data exfiltration, evasion of security measures, and potentially establishing persistent control over the compromised system.

It has been covered in detail in Appendix-4.

4.3 Detection Techniques

- **File extension**

  In this scenario, the malicious file has the extension ".pdf.exe". It is an executable file disguised as a pdf document.

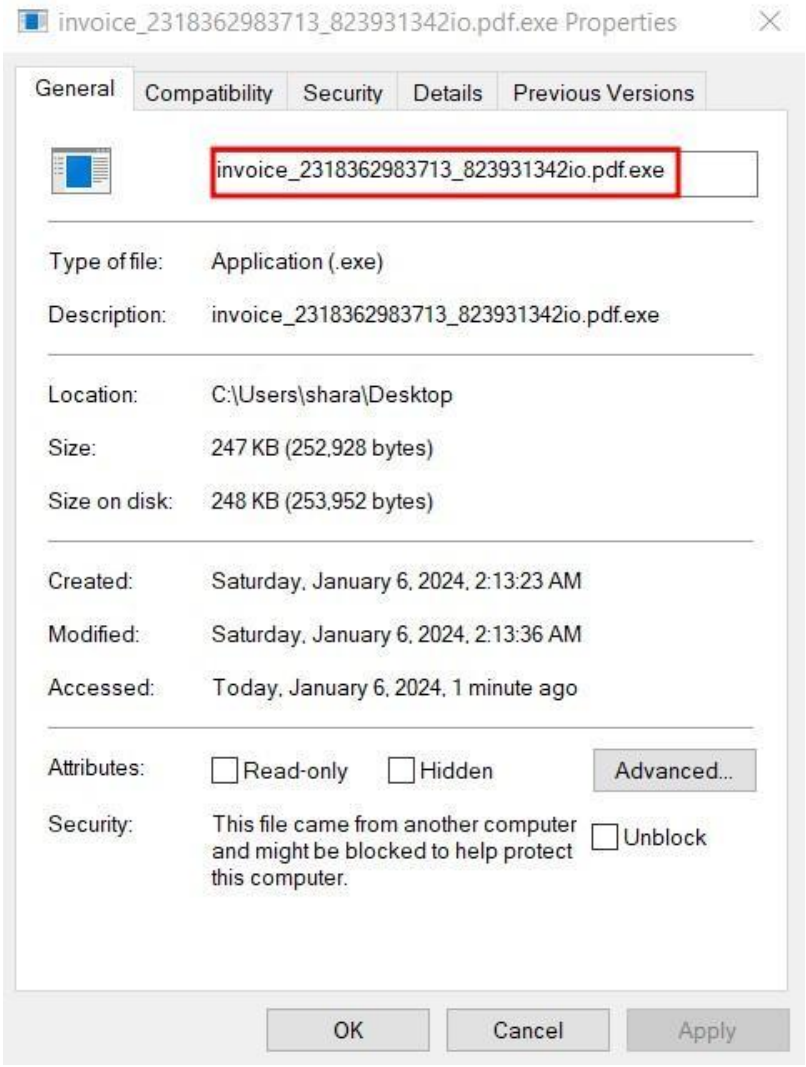


Figure 14 Extension of File

- **Unusual files or directories:**

  In this scenario, directories dating back to 2019 were created, which raised suspicion.

Figure 15 Unusual Files/Directories

- **Unusual Processes:**

  In this scenario, process named Microsoft.Photos.exe was discovered, which helped in detection of malware.

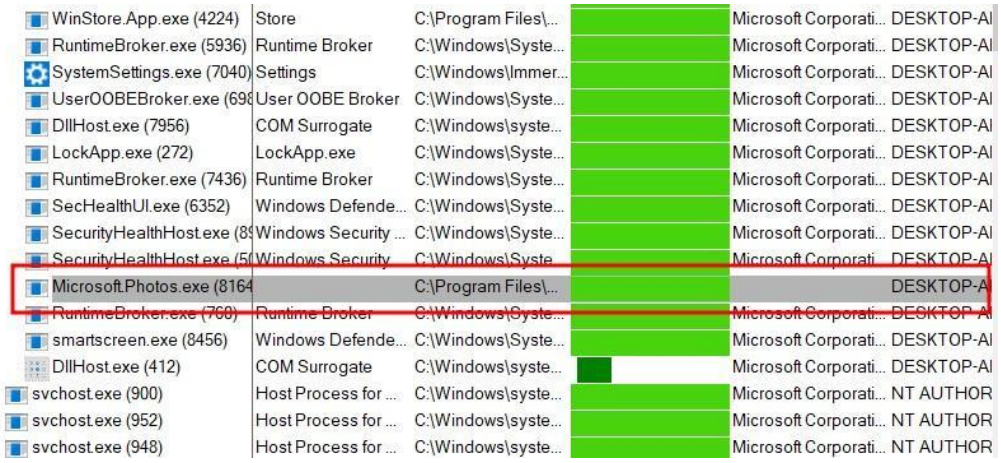


Figure 16 Unusual Processes

- **Unusual changes in System Settings**

  Noticing unusual changes in system settings is an easy giveaway of malware infection. During investigation, the malware changed system clock from Nepal Standard Time (GMT+5:45) to that of Los Angeles (GMT-8).

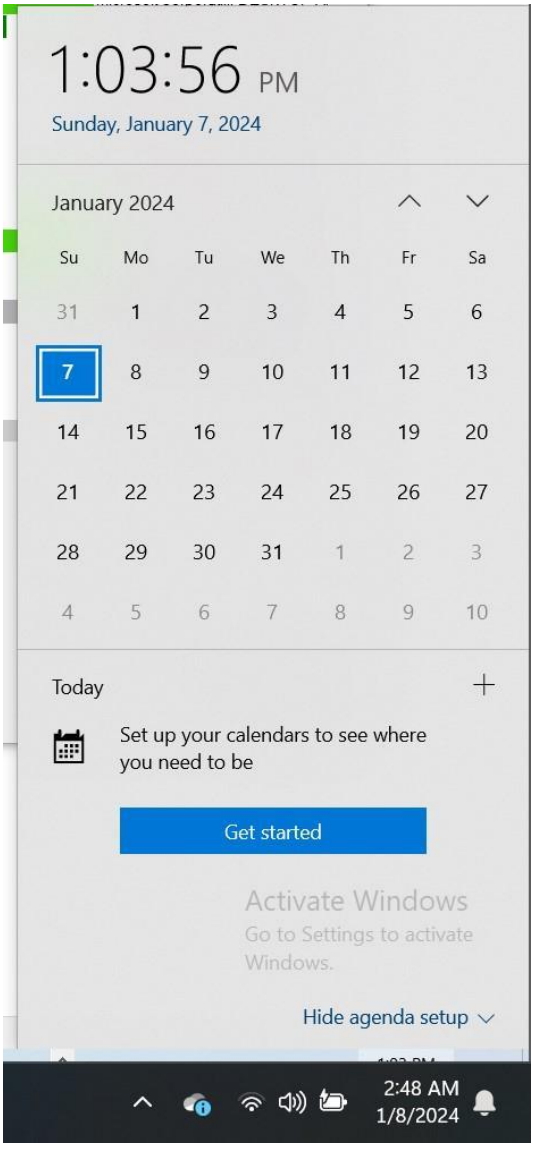


Figure 17 Unusual changes in System Clock

- **Increased CPU Usage**

Since malware runs multiple processes in the background, it leads to increased CPU usage which is often caused due to unusual process.

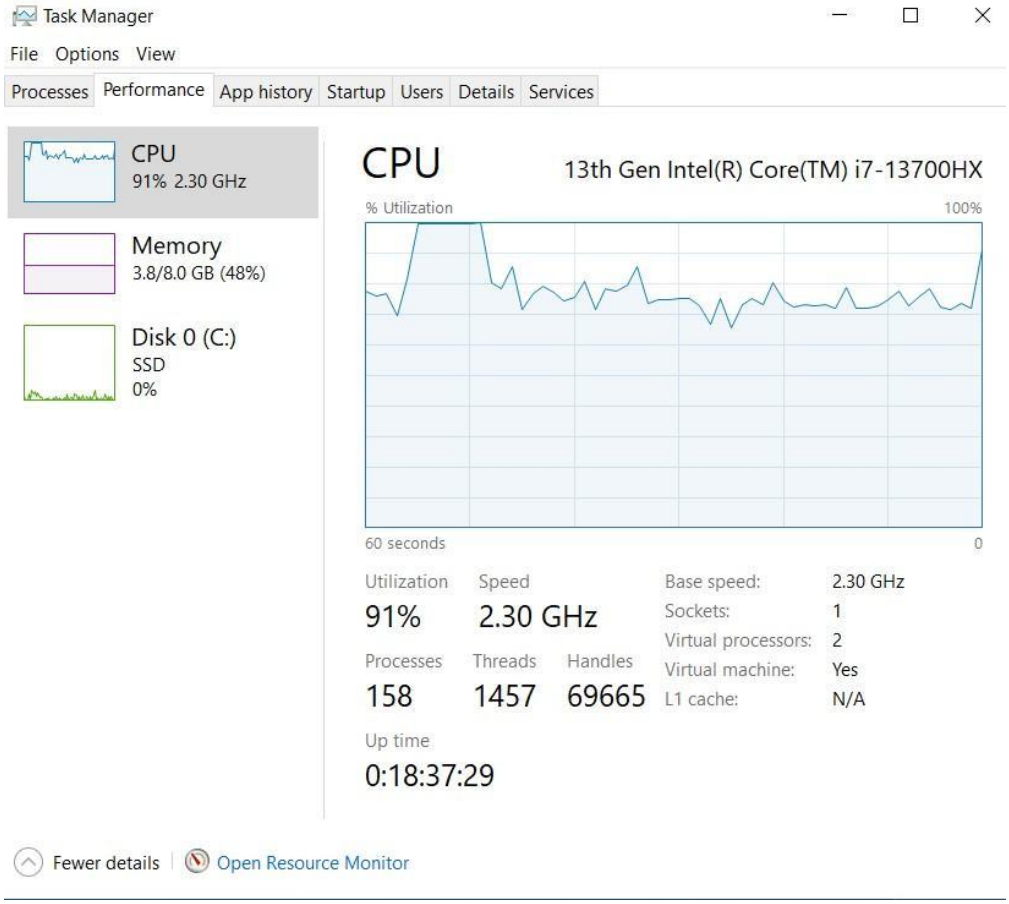


Figure 18 Increased CPU Usage

5 Preventive Measures/ Recommendation

Fighting against **ZeuS** malware requires a combination of technical and behavioral preventive measures. Below are some recommendations:

- **Email Security:**
  Use email filtering solutions to detect and quarantine malicious emails before they reach users, ensuring caution with attachments and links from unknown or suspicious sources.

- **Monitor for Unusual System Activities:**
  Regularly monitor system logs, network traffic, and behaviour patterns for unusual or suspicious activities, including unexpected system processes, unusual network connections, and unauthorized access attempts.

- **Keep Software and Systems Updated:**
  Regularly update operating systems, antivirus software, browsers, and all installed applications to patch vulnerabilities exploited by malware.

- **Use a Reliable Antivirus and Anti-malware Solution:**
  Employ reputable antivirus and anti-malware software, keep it updated, and enable real-time protection to detect and block threats in real-time.

- **Firewall Configuration:**
  Configure firewalls on network and devices to monitor and control traffic, preventing unauthorized access and communication with command-and-control servers.

- **User Education and Awareness:**
  Educate users on recognizing phishing scams and suspicious websites, and to not click on unknown links or download attachments from unreliable sources (Arthur, 2022).

  More on Appendix-5

6 Conclusion

In conclusion, the persistent and adaptive nature of cyber threats, particularly ZeuS malware, has evolved over the years posing significant challenges to cybersecurity. The case study of ZeuS attacks on prominent organizations like NASA and Bank of America serves as a stark reminder of the potential impact and sophistication of digital crimes.

The aim of this report was to explore the evolving digital crime landscape, focusing on the ZeuS Trojan, and propose effective detection and investigation strategies to mitigate its impact. The objectives were successfully achieved through an in-depth analysis of malware's historical context, functionalities, tactics, and simulated attack scenario. The report also provided practical insights and recommendations for enhancing cybersecurity measures against ZeuS and similar threats.

The simulated attack scenario demonstrated the real-world implications of ZeuS, emphasizing the need for robust detection and investigation methodologies. It highlighted the importance of a multi-layered approach to cybersecurity, including monitoring unusual system activities, updating software, using reliable antivirus solutions, and educating users.

Preventive measures and recommendations outlined in the report provide guide organizations and individuals to enhance their defenses against ZeuS and other malware, emphasizing email security, regular system monitoring, software updates, and user education as key measures.

The digital landscape is constantly evolving, necessitating cybersecurity professionals, organizations, and individuals to remain vigilant, adaptive, and proactive against emerging threats. Collaboration, continuous learning, and robust security measures are crucial for safeguarding sensitive information and ensuring digital infrastructure resilience.

7 References

ABC News, 2010. *FBI: Crime Ring Stole $70 Million Using Computer Virus.* [Online] Available at: https://abcnews.go.com/Blotter/fbi-crime-ring-stole-70-million-computer-virus/story?id=11777873
[Accessed 2024].

Arthur, 2022. *What Is Zeus Malware?.* [Online] Available at: https://www.xcitium.com/blog/malware/what-is-zeus-malware/
[Accessed 2024].

Avast, 2024. *The Zeus Trojan — What It Is, and How to Remove and Prevent it.* [Online] Available at: https://www.avast.com/c-zeus
[Accessed 2024].

Baker, K., 2023. *THE ZEUS TROJAN MALWARE — DEFINITION AND PREVENTION.* [Online] Available at: https://www.crowdstrike.com/cybersecurity-101/malware/trojan-zeus-malware/
[Accessed 2024].

Cameron, L., 2018. *Future of digital forensics faces six security challenges in fighting borderless cybercrime and dark web tools.* [Online] Available at: https://www.computer.org/publications/tech-news/research/digital-forensics-security-challenges-cybercrime
[Accessed 2023].

Cheng, J., 2009. *Botnet master hits the kill switch, takes down 100,000 PCs.* [Online] Available at: https://arstechnica.com/information-technology/2009/05/zeus-botnet-hits-the-kill-switch-takes-down-100000-pcs/
[Accessed 2023].

CIS, 2023. *Top 10 Malware Q2 2023.* [Online] Available at: https://www.cisecurity.org/insights/blog/top-10-malware-q2-2023
[Accessed 2023].

CISA, 2022. *2021 Top Malware Strains.* [Online] Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-216a [Accessed 2023].

cynet, 2023. *Zeus Malware: Variants, Methods and History.* [Online] Available at: https://www.cynet.com/malware/zeus-malware-variants-methods-and-history/ [Accessed 2023].

Etaher, N., Weir, G. R. & Alazab, M., 2015. From ZeuS to Zitmo: Trends in Banking Malware. *IEEE International Conference on Trust, Security and Privacy in Computing and Communications,* pp. 1386-1391.

Fortra's Digital Defense, 2024. *Zeus Trojan - What It Is & How to Prevent it.* [Online] Available at: https://www.digitaldefense.com/blog/zeus-trojan-what-it-is-how-to-prevent-it-digital-defense/
[Accessed 2024].

Hendry, A., 2008. *Non-tech criminals can now rent-a-botnet.* [Online] Available at: https://web.archive.org/web/20111119172322/http://www.computerworld.com.au/article/216322/non-tech_criminals_can_now_rent-a-botnet/
[Accessed 2023].

HMICFRS, 2023. *Digital crime and policing.* [Online] Available at: https://hmicfrs.justiceinspectorates.gov.uk/our-work/article/digital-crime-and-policing/
[Accessed 2023].

Hutchings, A. & Clayton, R., 2017. Configuring Zeus: A case study of online crime target selection and knowledge transmission. *APWG Symposium on Electronic Crime Research (eCrime),* pp. 33-40.

Jagan, S., Mahdal, M. & Dhanke, J., 2023. A Meta-Classification Model for Optimized ZBot Malware Prediction Using Learning Algorithms. *Mathematics,* 11(13).

Kirk, J., 2008. *Rock Phish gang adds second punch to phishing attacks.* [Online] Available at: https://web.archive.org/web/20140409042644/http://www.computerworld.com.au/article/213028/rock_phish_gang_adds_second_punch_phishing_attacks/
[Accessed 2023].

Malwarebytes, 2021. *The life and death of the ZeuS Trojan.* [Online] Available at: https://www.malwarebytes.com/blog/news/2021/07/the-life-and-death-of-the-zeus-trojan
[Accessed 2024].

Masters, G., 2010. *New version of Zeus targeting AIM users.* [Online] Available at: https://web.archive.org/web/20111214174845/http://www.scmagazineus.com/new-version-of-zeus-targeting-aim-users/article/162090/
[Accessed 2023].

Microsoft, 2023. *Process Monitor v3.96.* [Online] Available at: https://learn.microsoft.com/en-us/sysinternals/downloads/procmon
[Accessed 2024].

Proofpoint, 2024. *What Is GameOver Zeus Malware (GOZ)?.* [Online] Available at: https://www.proofpoint.com/us/threat-reference/gameover-zeus-goz
[Accessed 2024].

Ragen, S., 2009. *ZBot data dump discovered with over 74,000 FTP credentials.* [Online] Available at: https://www.thetechherald.com/tech-news/zbot-data-dump-discovered-with-over-74000-ftp-credentials/
[Accessed 2024].

Reuters, 2007. *Hackers steal U.S. govt, corporate data from PCs.* [Online] Available at: https://www.reuters.com/article/domesticNews/idUSN1638118020070717/
[Accessed 2023].

Stevens, K. & Jackson, D., 2010. *ZEUS BANKING TROJAN REPORT*. [Online] Available at: https://www.secureworks.com/research/zeus
[Accessed 2024].

tutorialspoint, 2023. *What is Zeus Trojan? How does it Work, and How to Stay Safe?*. [Online] Available at: https://www.tutorialspoint.com/what-is-zeus-trojan-how-does-it-work-and-how-to-stay-safe
[Accessed 2024].

Vaidya, T., 2015. *2001-2013: Survey and Analysis of Major Cyberattacks.* [Online] Available at: https://arxiv.org/pdf/1507.06673.pdf
[Accessed 2023].

Warner, G., 2009. *IRS Version of Zeus Bot continues.* [Online] Available at: https://garwarner.blogspot.com/2009/09/irs-version-of-zeus-bot-continues.html
[Accessed 2023].

Westervelt, R., 2014. *Zeus Banking Malware Active Despite Recent Botnet Takedown.* [Online] Available at: https://www.crn.com/news/security/300073359/zeus-banking-malware-active-despite-recent-botnet-takedown
[Accessed 2024].

Wilson, T., 2009. *Facebook Phishing Attack Powered By Zeus Botnet, Researchers Say.* [Online] Available at: https://web.archive.org/web/20111119225622/http://www.darkreading.com/security/attacks-breaches/221100157/index.html
[Accessed 2023].

8 Bibliography

CSNP, 2021. *CyberChef – Data decoding made easy.* [Online] Available at: https://www.csnp.org/post/cyberchef-data-decoding-made-easy [Accessed 2024].

CyberAcademy, 2024. *The Malware Analysis Project 101.* [Online] Available at: https://cybercademy.org/the-malware-analysis-project-101/#notes [Accessed 2024].

Higgins, M., 2022. *Zeus malware: Its history and how it works.* [Online] Available at: https://nordvpn.com/blog/zeus-virus/ [Accessed 2024].

Ibrahim, L. M. & Hatim, K., 2015. Analysis and Detection of the Zeus Botnet Crimeware. *International Journal of Computer Science and Information Security,* 13(9), pp. 121-135.

Kaspersky, 2024. *Zeus Virus.* [Online] Available at: https://www.kaspersky.com/resource-center/threats/zeus-virus [Accessed 2024].

Kirk, J., 2008. *Rock Phish gang adds second punch to phishing attacks.* [Online] Available at: https://web.archive.org/web/20140409042644/http://www.computerworld.com.au/article/213028/rock_phish_gang_adds_second_punch_phishing_attacks/ [Accessed 2023].

Martens, M. & Wolf, R. D., 2019. Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior,* Volume 92, pp. 139-150.

Office of Public Affairs, 2014. *U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator.* [Online] Available at: https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware

Paganini, P., 2015. *NEWS ZEUS SHOWS SIGNIFICANT A EVOLUTION IN THE CRIMINAL ECOSYSTEM.* [Online]
Available at: https://securityaffairs.com/32875/cyber-crime/news-sophisticated-zeus-variant.html

Reed, J., 2023. *How the ZeuS Trojan info stealer changed cybersecurity.* [Online]
Available at: https://securityintelligence.com/articles/how-the-zeus-trojan-info-stealer-changed-cybersecurity/
[Accessed 2024].

Sourcefire VRT Labs, 2010. *VRT Labs - Zeus Trojan Analysis.* [Online]
Available at: https://web.archive.org/web/20120116131113/http://labs.snort.org/papers/zeus.html
[Accessed 2024].

viktik, 2015. *Guide | How To Using Sysinternals Process Monitor to troubleshoot problems in Windows.* [Online]
Available at: https://malwaretips.com/threads/using-sysinternals-process-monitor-to-troubleshoot-problems-in-windows.45250/
[Accessed 2024].

VirusTotal, 2024. *VirusTotal.* [Online]
Available at: https://www.virustotal.com/gui/url/fa6cfcabea7852abf1a040b4ea995a4f0ed6e58e1220204ac903a34eb1659481
[Accessed 2024].

9 Appendix

9.1 Appendix 1: Evolution of ZeuS Malware

The ZeuS malware, also recognized as Zbot, has undergone significant transformations since its initial detection in 2007. In its early stages, ZeuS operated clandestinely, targeting sensitive information from systems affiliated with the United States Department of Transformation. Believed to have originated in Eastern Europe, ZeuS gained notoriety in 2009 when security firm Prevx uncovered its compromise of over 74,000 FTP accounts, affecting prominent entities such as Bank of America, NASA, Monster.com, ABC, Oracle, Play.com, Cisco, Amazon, and BusinessWeek (Malwarebytes, 2021).

The polymorphic nature of ZeuS has made it challenging to combat, with numerous versions, botnets operated by different groups, and various attack vectors. Initially emerging as a Do-It-Yourself kit, ZeuS allowed users to purchase and modify it with customized features. Over the years, it has evolved into a highly sophisticated threat with stealthy targeted attacks (Etaher, et al., 2015).

Several variants of ZeuS have been identified, making it difficult for antivirus programs to detect them using traditional signature-based methods. The trojan can exploit software vulnerabilities on phishing websites and, if successful, load onto the victim's computer. It has the capability to collect data from forms, capture screenshots, steal passwords from browsers, and remotely control infected machines (Jagan, et al., 2023).

The evolution of ZeuS has been marked by significant events and campaigns. In 2008, a phishing kit for ZeuS was sold for $700, utilizing a binary generator to create new variants, making detection by antivirus programs more challenging. Additionally, non-tech criminals could rent a service that offered an all-in-one hosting server with a built-in ZeuS trojan administration panel and infecting tools (Hendry, 2008).

In 2009, a notable event occurred when the controllers of a ZeuS botnet initiated a kill switch, taking down around 100,000 infected computers (Cheng, 2009). The trojan continued to be a threat with new spam campaigns, such as those impersonating the Internal Revenue Service (IRS) or

using fake Facebook and MySpace updates to lure users into compromising their accounts (Warner, 2009) (Wilson, 2009).

The trojan persisted in its malicious activities, with new iterations targeting users of AOL Instant Messenger in 2010 (Masters, 2010). Users were tricked into downloading what appeared to be legitimate updates, but were, in fact, ZeuS installers.

Throughout its history, ZeuS has posed a significant threat to cybersecurity, continually adapting, and evolving to exploit vulnerabilities and compromise sensitive information.

By 2010, the U.S. FBI reported a global impact as hackers in Eastern Europe utilized ZeuS to infect computers worldwide. Over 37 individuals/ ‘mules’ faced charges in New York itself, related to conspiracy to commit bank fraud and money laundering (ABC News, 2010).

In 2011, the malware's author furthered its impact by releasing the ZeuS source code, paving the way for the creation of numerous updated versions. The exposure of ZeuS 2.0.8.9's source code in 2011 gave rise to novel business models, including subscription-based services providing hosting, configuration, and installations for ZeuS users. Concurrently, new iterations of the malware, such as Citadel and GameOver ZeuS, emerged, enhancing the original ZeuS's functionality and resilience (Hutchings & Clayton, 2017).

The following years after the encryption saw the evolution of ZeuS variants incorporating new infection patterns derived from hooking procedures used by Zberp in 2014.

Originally designed as a financial or banking Trojan, ZeuS, also known as crimeware, extended its threat beyond pilfering financial information due to its adept information-stealing capabilities. With a total of 545 versions documented to date, ZeuS has experienced ongoing evolution. Despite the neutralization of the original ZeuS malware, its components persist in newer malware iterations, reflecting a continuous and adaptive nature in the realm of cybersecurity (Malwarebytes, 2021).

Back to Report

9.2 Appendix 2: ZeuS-In-Detail

ZeuS is a type of Trojan, a form of malware that pretends to be legitimate software. It steals passwords and financial data using keylogging and website tracking. This allows the malware to detect when the user is on a banking site or conducting a financial transaction, enabling it to record keystrokes used by the user when logging in (tutorialspoint, 2023).

9.2.1 Method of infection

The ZeuS Virus has two main infection methods: drive-by downloads and spam messages. Drive-by downloads involve malware developers injecting ZeuS code into legitimate websites, allowing the virus to be installed when a user visits. Spam messages, transmitted through phishing emails and fraudulent social media campaigns, are used by hackers to spread malware. ZeuS is a robust botnet that can access login credentials, allowing it to send spam messages from legitimate sources, increasing the chances of infecting victims (tutorialspoint, 2023).

9.2.2 Working of ZeuS

ZeuS performs stolen data exfiltration and remote commands via encrypted HTTP POST requests to a Command and Control (C&C) web server. The encryption method used by ZeuS is RC4, with the key embedded in the binary. Special scripts can be executed on selected infected systems through an HTTP-based control panel. These scripts enable on-demand tasks such as taking screenshots of infected systems or performing ZeuS binary updates.

It works by:

- Modifying the local hosts file to redirect traffic to malicious sites.
- Injecting code into winlogon.exe or explorer.exe to hide its presence and infect other processes.
- Capturing data from web forms, such as usernames, passwords, and personal information, and sending it to a command-and-control server.
- Using modules to enable additional features, such as backconnect, Firefox form grabber, VNC, Vista/Windows 7 support, and polymorphic encryption.
- Using webinjects to display extra fields on banking sites, asking for more data from the victims.
- Stealing digital certificates to bypass authentication mechanisms.

- Using a hardware-based licensing system to protect the malware from being copied or analysed (Stevens & Jackson, 2010).

9.2.3 Identification of ZeuS

Computers infected with this version of ZeuS will have suspicious files and folders installed. The location of file depends on victim's access list entry. The files will most likely have the HIDDEN attribute set to hide them from casual inspection.

Example:

With Administrator rights:

%systemroot%\system32\sdra64.exe (malware)

%systemroot%\system32\lowsec

%systemroot%\system32\lowsec\user.ds (encrypted stolen data file)
%systemroot%\system32\lowsec\user.ds.lll (temporary file for stolen data)
%systemroot%\system32\lowsec\local.ds (encrypted configuration file)

Without Administrator rights:

%appdata%\sdra64.exe

%appdata%\lowsec

%appdata%\lowsec\user.ds

%appdata%\lowsec\user.ds.lll

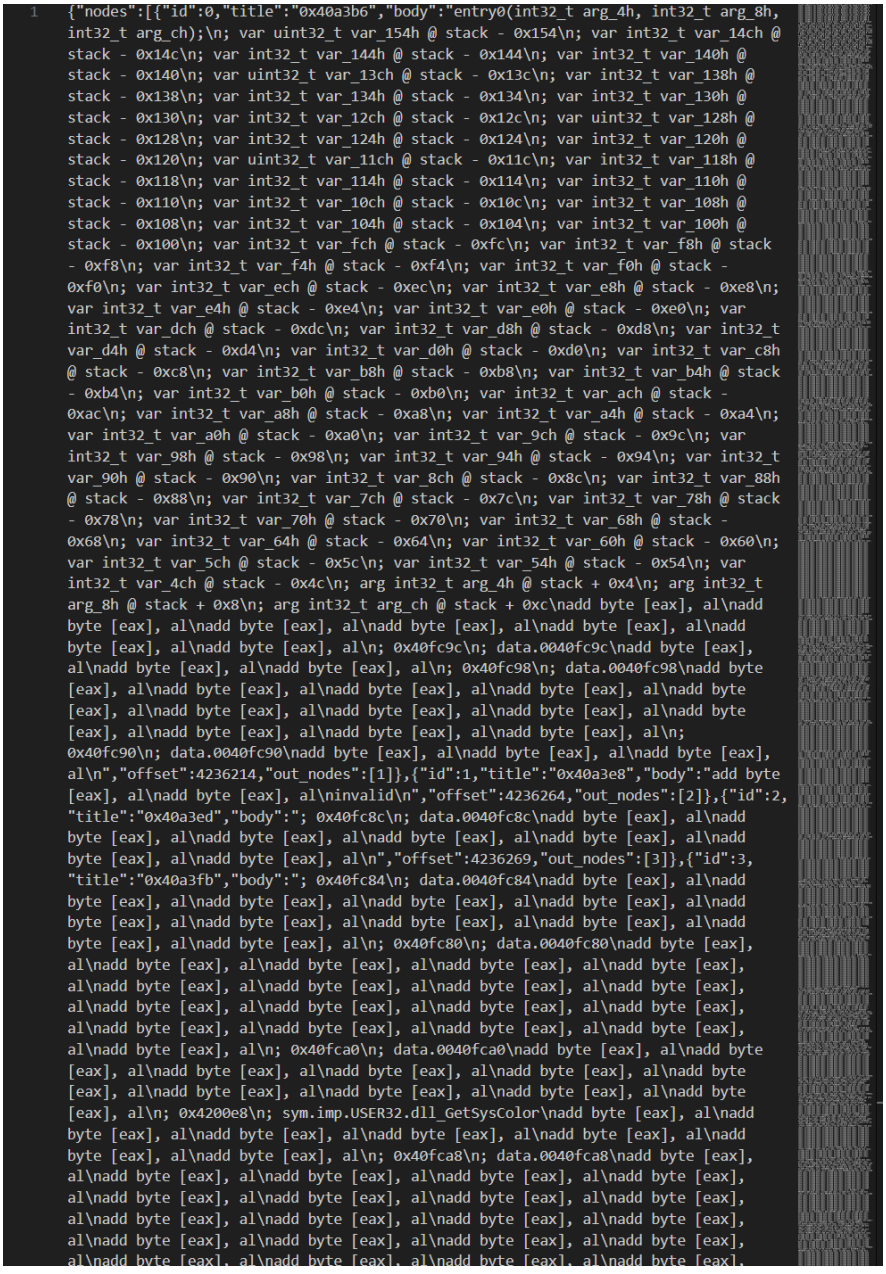
%appdata%\lowsec\local.ds

Likewise, ZeuS also makes registry changes to ensure that it starts up with Administrator privileges. The executable it uses to ensure that uses process injection to hide its presence in the list of running processes. Upon startup, it will inject code into winlogon.exe (if Administrator rights available) or explorer.exe (for non-Administrators) and exit. The injected code infects other processes to perform its data theft capabilities (Stevens & Jackson, 2010).

Back to Report

9.3 Appendix 3: Json of Function calls exported using Cutter.

entry.json




```
{"nodes":[{"id":0,"title":"0x40a3b6","body":"entry0(int32_t arg_4h, int32_t arg_8h,
int32_t arg_ch);\n; var uint32_t var_154h @ stack - 0x154\n; var int32_t var_14ch @
stack - 0x14c\n; var int32_t var_144h @ stack - 0x144\n; var int32_t var_140h @
stack - 0x140\n; var uint32_t var_13ch @ stack - 0x13c\n; var int32_t var_138h @
stack - 0x138\n; var int32_t var_134h @ stack - 0x134\n; var int32_t var_130h @
stack - 0x130\n; var int32_t var_12ch @ stack - 0x12c\n; var uint32_t var_128h @
stack - 0x128\n; var int32_t var_124h @ stack - 0x124\n; var int32_t var_120h @
stack - 0x120\n; var uint32_t var_11ch @ stack - 0x11c\n; var int32_t var_118h @
stack - 0x118\n; var int32_t var_114h @ stack - 0x114\n; var int32_t var_110h @
stack - 0x110\n; var int32_t var_10ch @ stack - 0x10c\n; var int32_t var_108h @
stack - 0x108\n; var int32_t var_104h @ stack - 0x104\n; var int32_t var_100h @
stack - 0x100\n; var int32_t var_fch @ stack - 0xfc\n; var int32_t var_f8h @ stack
- 0xf8\n; var int32_t var_f4h @ stack - 0xf4\n; var int32_t var_f0h @ stack -
0xf0\n; var int32_t var_ech @ stack - 0xec\n; var int32_t var_e8h @ stack - 0xe8\n;
var int32_t var_e4h @ stack - 0xe4\n; var int32_t var_e0h @ stack - 0xe0\n; var
int32_t var_dch @ stack - 0xdc\n; var int32_t var_d8h @ stack - 0xd8\n; var int32_t
var_d4h @ stack - 0xd4\n; var int32_t var_d0h @ stack - 0xd0\n; var int32_t var_c8h
@ stack - 0xc8\n; var int32_t var_b8h @ stack - 0xb8\n; var int32_t var_b4h @ stack
- 0xb4\n; var int32_t var_b0h @ stack - 0xb0\n; var int32_t var_ach @ stack -
0xac\n; var int32_t var_a8h @ stack - 0xa8\n; var int32_t var_a4h @ stack - 0xa4\n;
var int32_t var_a0h @ stack - 0xa0\n; var int32_t var_9ch @ stack - 0x9c\n; var
int32_t var_98h @ stack - 0x98\n; var int32_t var_94h @ stack - 0x94\n; var int32_t
var_90h @ stack - 0x90\n; var int32_t var_8ch @ stack - 0x8c\n; var int32_t var_88h
@ stack - 0x88\n; var int32_t var_7ch @ stack - 0x7c\n; var int32_t var_78h @ stack
- 0x78\n; var int32_t var_70h @ stack - 0x70\n; var int32_t var_68h @ stack -
0x68\n; var int32_t var_64h @ stack - 0x64\n; var int32_t var_60h @ stack - 0x60\n;
var int32_t var_5ch @ stack - 0x5c\n; var int32_t var_54h @ stack - 0x54\n; var
int32_t var_4ch @ stack - 0x4c\n; arg int32_t arg_4h @ stack + 0x4\n; arg int32_t
arg_8h @ stack + 0x8\n; arg int32_t arg_ch @ stack + 0xc\nadd byte [eax], al\nadd
byte [eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd
byte [eax], al\nadd byte [eax], al\n; 0x40fc9c\n; data.0040fc9c\nadd byte [eax],
al\nadd byte [eax], al\nadd byte [eax], al\n; 0x40fc98\n; data.0040fc98\nadd byte
[eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd byte
[eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd byte
[eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax], al\n;
0x40fc90\n; data.0040fc90\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax],
al\n","offset":4236214,"out_nodes":[1]},{"id":1,"title":"0x40a3e8","body":"add byte
[eax], al\nadd byte [eax], al\ninvalid\n","offset":4236264,"out_nodes":[2]},{"id":2,
"title":"0x40a3ed","body":"; 0x40fc8c\n; data.0040fc8c\nadd byte [eax], al\nadd
byte [eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd
byte [eax], al\nadd byte [eax], al\n","offset":4236269,"out_nodes":[3]},{"id":3,
"title":"0x40a3fb","body":"; 0x40fc84\n; data.0040fc84\nadd byte [eax], al\nadd
byte [eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd
byte [eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd
byte [eax], al\nadd byte [eax], al\n; 0x40fc80\n; data.0040fc80\nadd byte [eax],
al\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax],
al\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax],
al\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax],
al\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax],
al\nadd byte [eax], al\n; 0x40fca0\n; data.0040fca0\nadd byte [eax], al\nadd byte
[eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd byte
[eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd byte
[eax], al\n; 0x4200e8\n; sym.imp.USER32.dll_GetSysColor\nadd byte [eax], al\nadd
byte [eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd
byte [eax], al\nadd byte [eax], al\n; 0x40fca8\n; data.0040fca8\nadd byte [eax],
al\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax],
al\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax],
al\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax],
al\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax], al\nadd byte [eax],
```


Figure 19 Screenshot of Json of Function Calls

Back to Report

9.4 Appendix 4: Dynamic Analysis in Depth

9.4.1.1 System Analysis

After execution, the file is nowhere to be located, but it can be seen running multiple processes in the background.

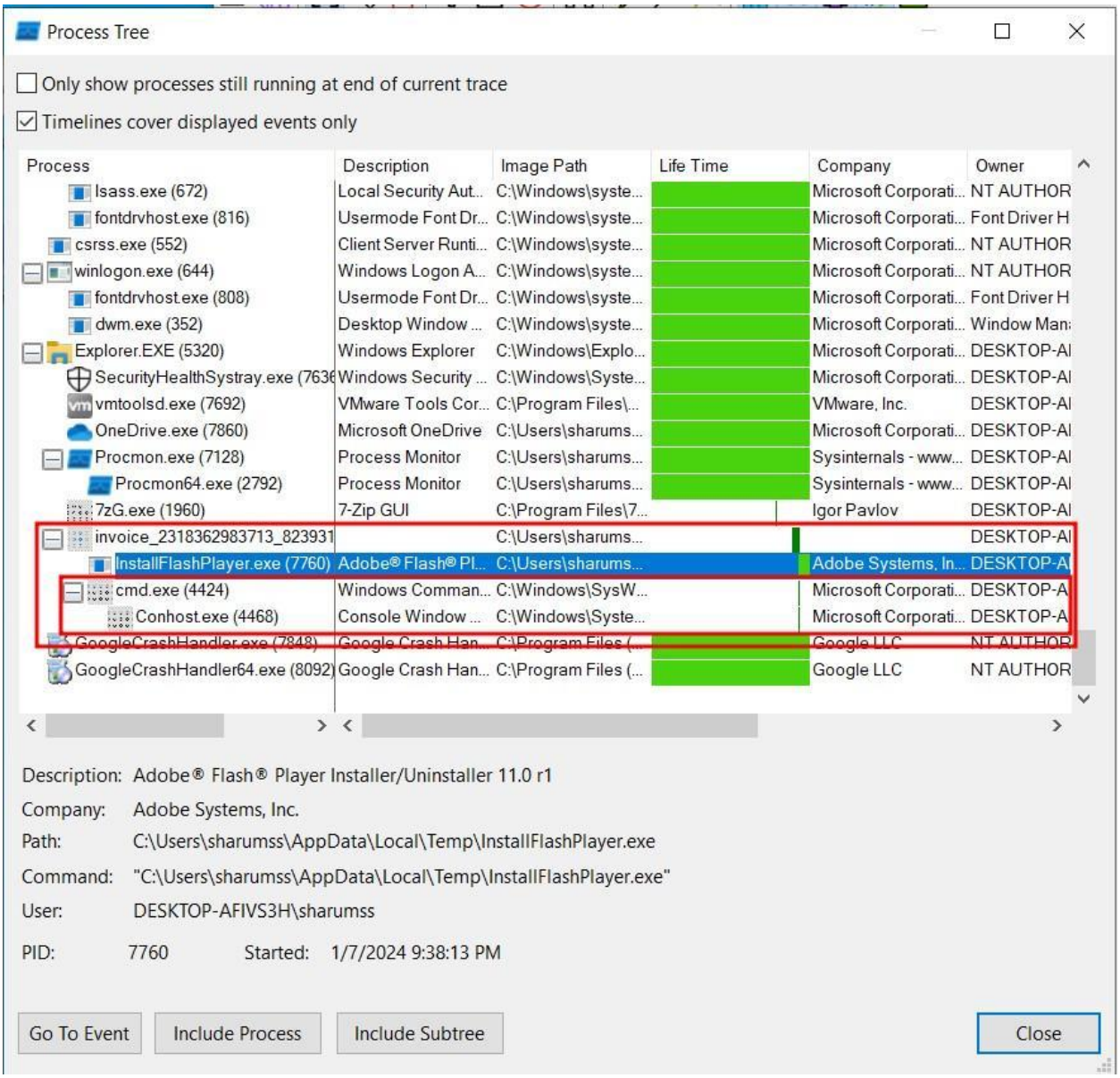


Figure 20 Malicious File running background processes.

It was running Adobe Flash Player installation as a process with a separate cmd running as a subprocess.

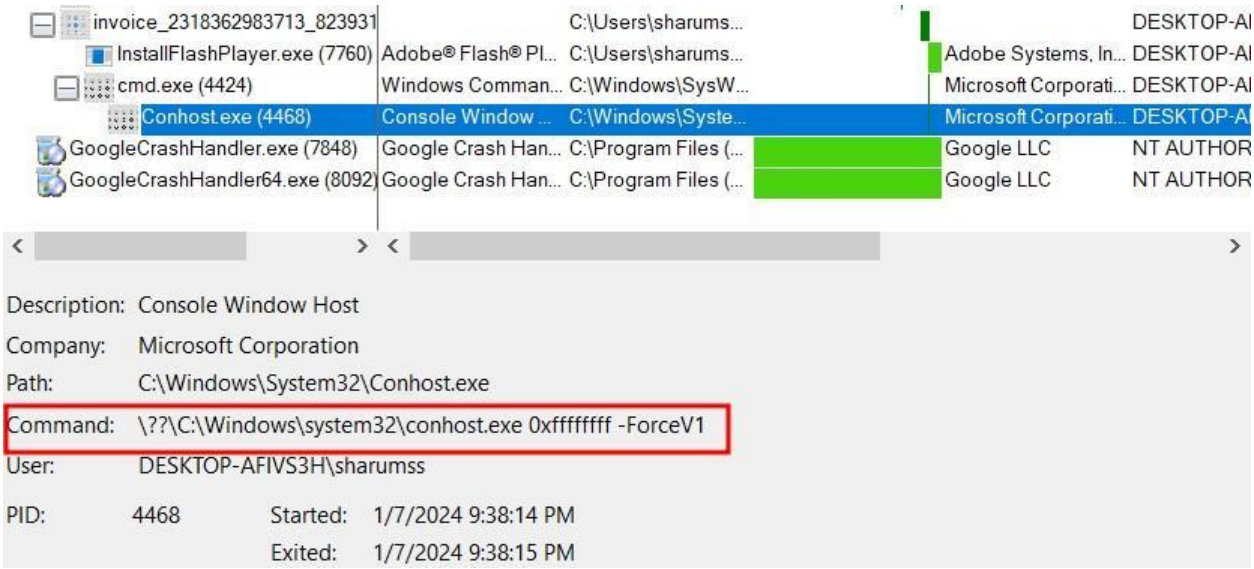


Figure 21 Command executed in cmd running in background.

Upon further exploration, the file had been editing registry key values.

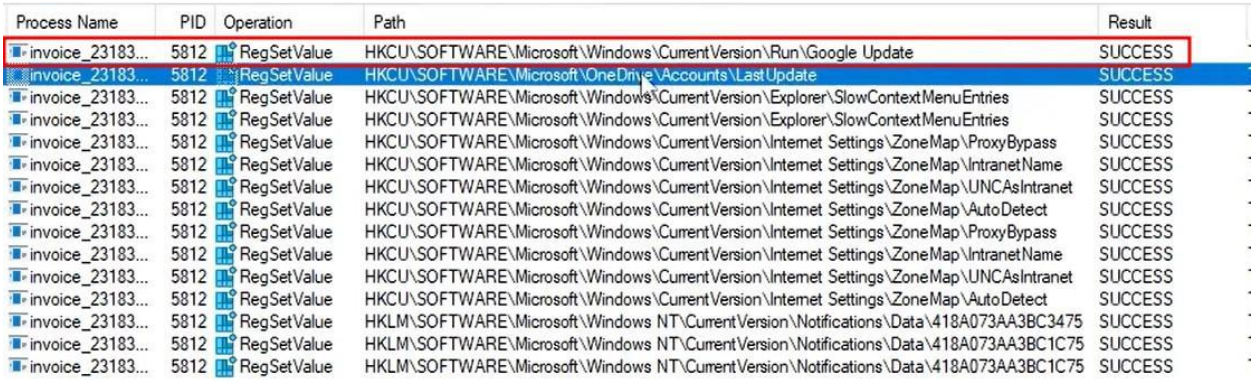


Figure 22 Registry key value edited by the malicious file.

It had been editing registry key values for google updates, which seemed a bit odd. Then, upon exploring the running processes further, another suspicious process was discovered.

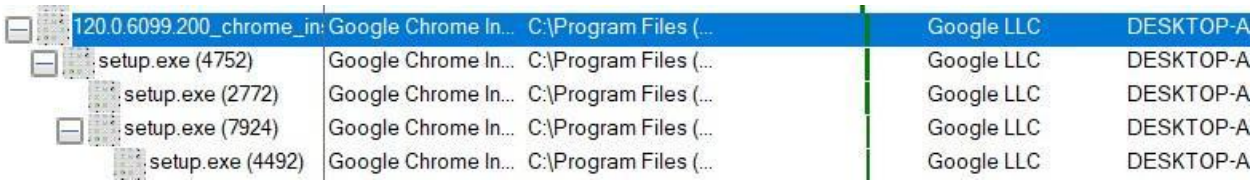


Figure 23 Suspicious Chrome processes running in the background.

It was odd for chrome to be running 'setup.exe' then, considering it had been installed way earlier. However, the executed command and monitoring the event further gave us no leads, it could be a way for the trojan to establish persistence in the system.

Then, the system was checked further to find out any unusual changes. Inside windows explorer, many odd directories and files were discovered. The trojan had already installed backdoors.

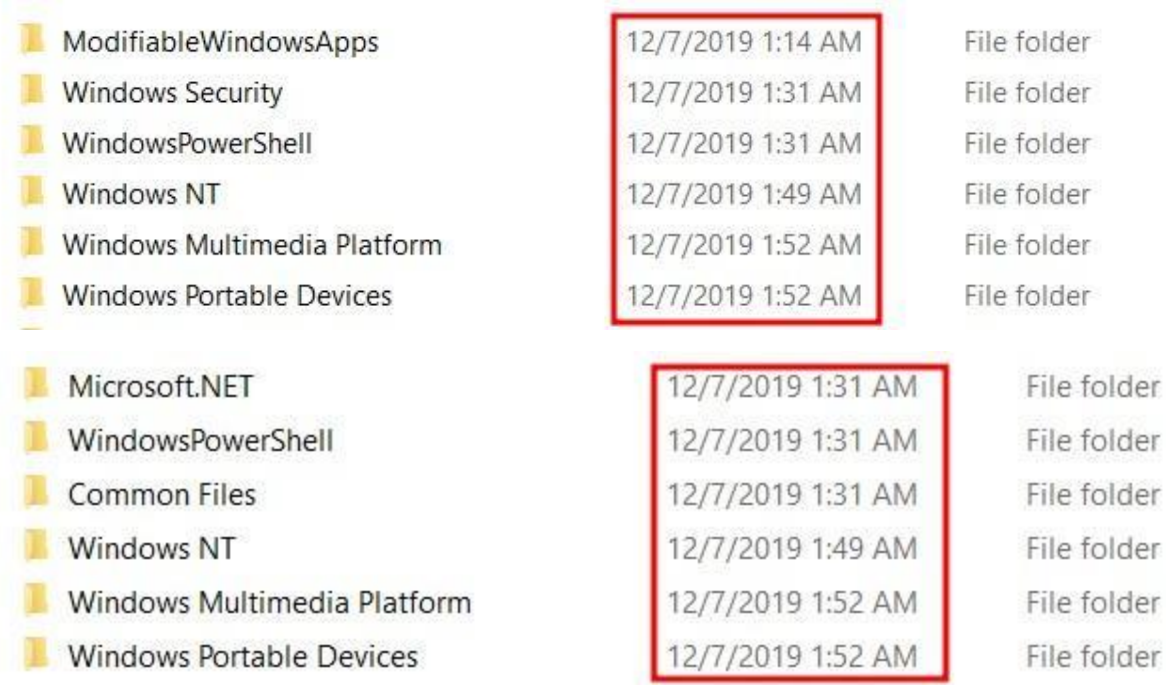


Figure 24 Suspicious Directories in the System

The discovered files were very suspicious because the date of creation of these files was earlier than that of the system itself. The files were created in 2019. Inside the files, were many .dll files which resembled the naming of normal windows file. Many of such files seemed legitimate and had verified signatures but they had been flagged previously as anomalies. This could have been done to potentially prevent detection.

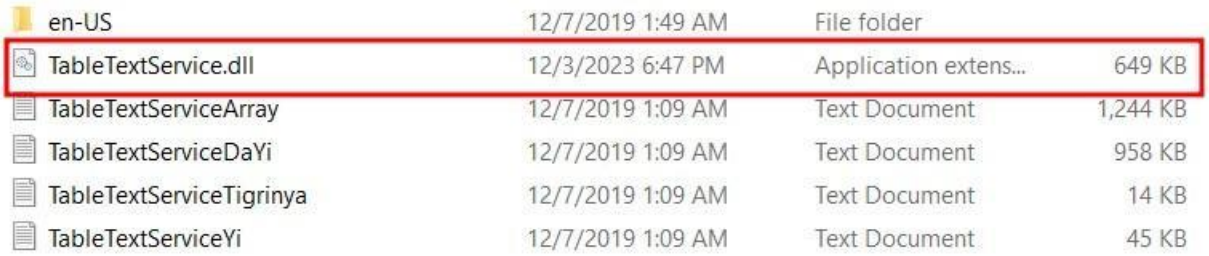


Figure 25 Example of malicious file disguised as legitimate files.

Upon, checking the file 'TableTextService.dll' using VirusTotal, it was discovered that it had been flagged as Trojan packed previously.

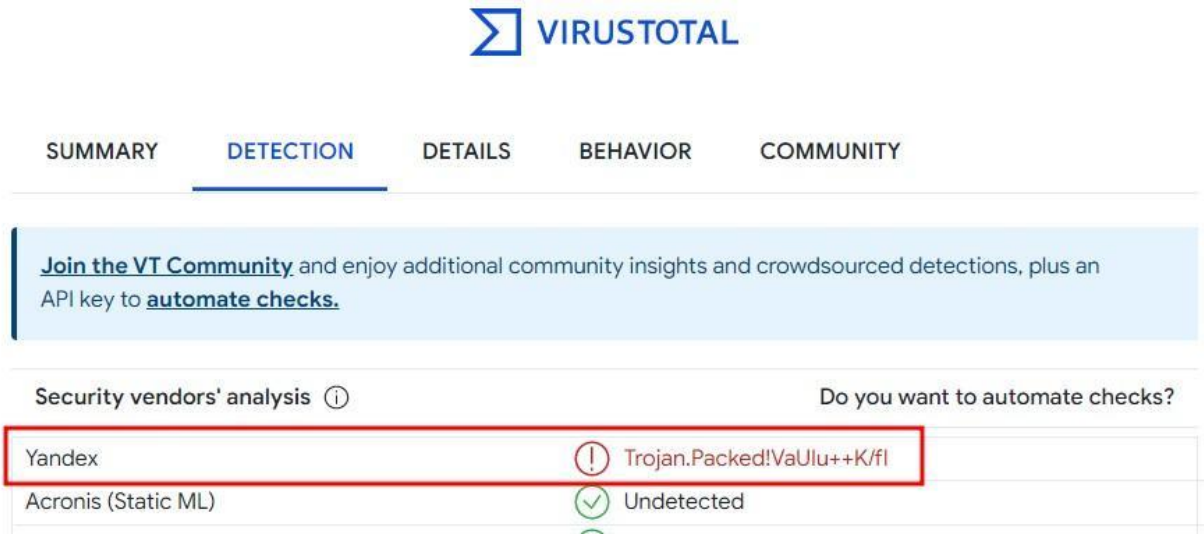


Figure 26 VirusTotal Output for TableTextService.dll

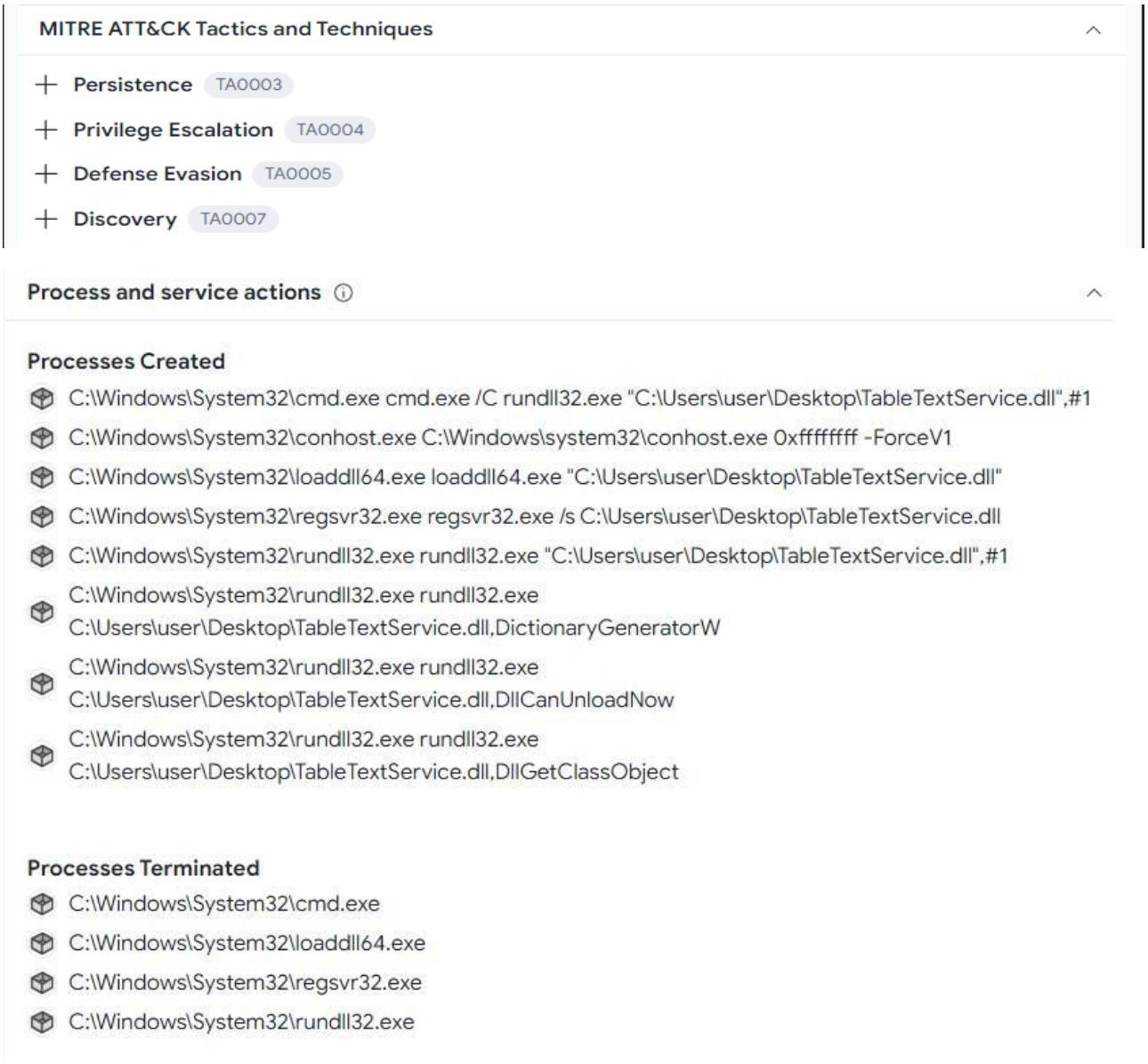


Figure 27 VirusTotal Details for TableTextService.dll

There were multiple backdoors like TableTextService.dll, having similar features to potentially attain persistence, escalate privileges, evade defenses and discovery. However, they were not creating any new processes. The directories also contained html pages to add authenticity, but the pages were oddly suspicious.

Microsoft Photos
Third Party Notices

This app contains source code developed by the third parties listed here.

Anderson, E. and Bai, Z. and Bischof, C. and Blackford, S. and Demmel, J. and Dongarra, J. and Du Croz, J. and Greenbaum, A. and Hammarling, S. and McKenney, A. and Sorensen, D., in LAPACK Users' Guide, third edition, published by Society for Industrial and Applied Mathematics, 1999, Philadelphia, PA, ISBN 0-89871-447-8

Newtonsoft.Json

The MIT License (MIT)

Copyright (c) 2007 James Newton-King

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

JsonCpp

The JsonCpp library's source code, including accompanying documentation, tests and demonstration applications, are licensed under the following conditions...

The author (Baptiste Lepilleur) explicitly disclaims copyright in all jurisdictions which recognize such a disclaimer. In such jurisdictions, this software is released into the Public Domain.

In jurisdictions which do not recognize Public Domain property (e.g. Germany as of 2010), this software is Copyright (c) 2007-2010 by Baptiste Lepilleur, and is released under the terms of the MIT License (see below).

In jurisdictions which recognize Public Domain property, the user of this software may choose to accept it either as 1) Public Domain, 2) under the conditions of the MIT License (see below), or 3) under the terms of dual Public Domain/MIT License conditions described here, as they choose.

The MIT License is about as close to Public Domain as a license can get, and is described in clear, concise terms at:

http://en.wikipedia.org/wiki/MIT_License

The full text of the MIT License follows:

Figure 28 Examples of Suspicious Webpages

After having no leads, the Procmon was rechecked to discover any new processes. Upon closer inspection a suspicious process was discovered. It was named “Microsoft.Photos.exe” and had no description and creator adding to the suspicion.

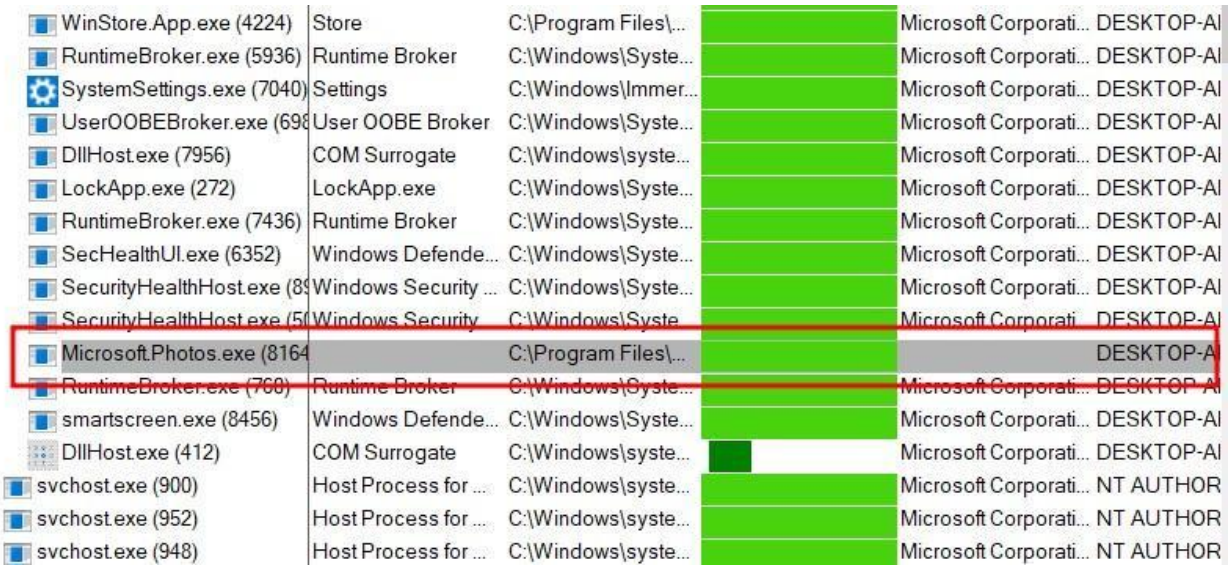


Figure 29 Microsoft.Photos.exe running in the background.

It was set to run at the start of Windows. Upon closer inspection, it had been running "Process Profiling" Operation continuously. Process profiling is a Procmon operation that generates and logs events for every process and thread on the system, recording kernel and user time, memory usage, and context switches (Microsoft, 2023).

Time o...	Process Name	PID	Operation	Path	Result	Detail
12:35:17...	Microsoft.Photo...	8164	Process Profiling		SUCCESS	User Time: 0.64062...
12:35:18...	Microsoft.Photo...	8164	Process Profiling		SUCCESS	User Time: 0.64062...
12:35:19...	Microsoft.Photo...	8164	Process Profiling		SUCCESS	User Time: 0.64062...
12:35:20...	Microsoft.Photo...	8164	Process Profiling		SUCCESS	User Time: 0.64062...
12:35:21...	Microsoft.Photo...	8164	Process Profiling		SUCCESS	User Time: 0.64062...
12:35:22...	Microsoft.Photo...	8164	Process Profiling		SUCCESS	User Time: 0.64062...
12:35:23...	Microsoft.Photo...	8164	Process Profiling		SUCCESS	User Time: 0.64062...
12:35:24...	Microsoft.Photo...	8164	Process Profiling		SUCCESS	User Time: 0.64062...
12:35:25...	Microsoft.Photo...	8164	Process Profiling		SUCCESS	User Time: 0.64062...
12:35:26...	Microsoft.Photo...	8164	Process Profiling		SUCCESS	User Time: 0.64062...
12:35:27...	Microsoft.Photo...	8164	Process Profiling		SUCCESS	User Time: 0.64062...
12:35:28...	Microsoft.Photo...	8164	Process Profiling		SUCCESS	User Time: 0.64062...
12:35:29...	Microsoft.Photo...	8164	Process Profiling		SUCCESS	User Time: 0.64062...
12:35:30...	Microsoft.Photo...	8164	Process Profiling		SUCCESS	User Time: 0.64062...
12:35:31...	Microsoft.Photo...	8164	Process Profiling		SUCCESS	User Time: 0.64062...
12:35:32...	Microsoft.Photo...	8164	Process Profiling		SUCCESS	User Time: 0.64062...
12:35:33...	Microsoft.Photo...	8164	Process Profiling		SUCCESS	User Time: 0.64062...
12:35:34...	Microsoft.Photo...	8164	Process Profiling		SUCCESS	User Time: 0.64062...
12:35:35...	Microsoft.Photo...	8164	Process Profiling		SUCCESS	User Time: 0.64062...
12:35:36...	Microsoft.Photo...	8164	Process Profiling		SUCCESS	User Time: 0.64062...
12:35:37...	Microsoft.Photo...	8164	Process Profiling		SUCCESS	User Time: 0.64062...

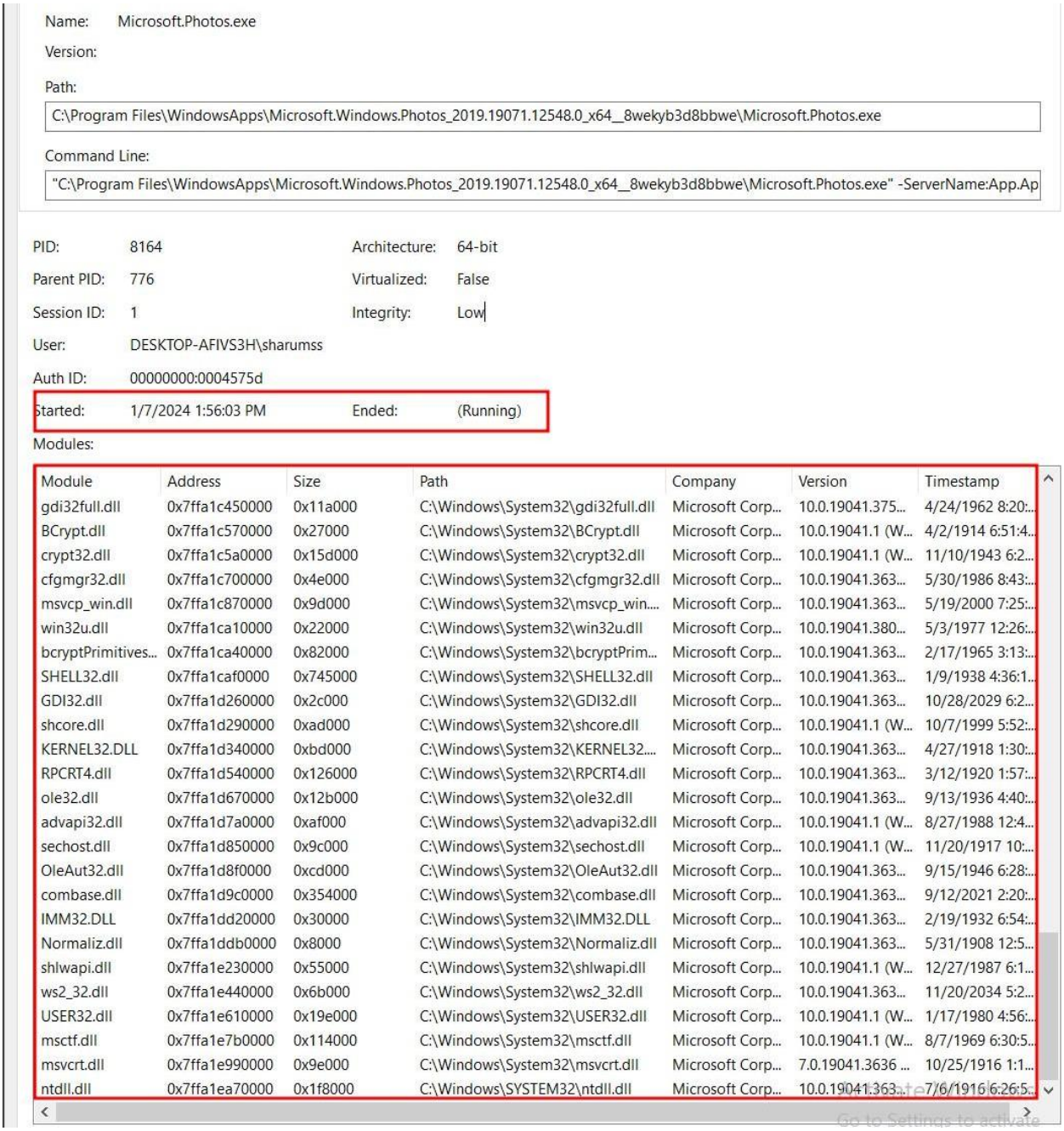
Figure 30 Microsoft.Photos.exe processes

Later, it was discovered that it had been continuously running in the background using modules like:

- **crypt32.dll and BCrypt.dll:**
  They handle cryptography, which can be potentially abused to encrypt stolen data/itself to evade detection, sign malicious code to appear legitimate, securing communication with a C2C server.
- **cfgmgr32.dll:**
  It manages system configuration, which can be potentially abused to facilitate data theft or hide processes, establish persistence by modifying system startup settings.
- **Core Windows modules (e.g., kernel32.dll, user32.dll):**
  These modules could be potentially abused for monitoring user activity like keystrokes, execute remote commands, take screenshots, etc.

- **gdi32full.dll:**

It is a graphic module which can be abused to launch DOS attacks against other systems.



Name: Microsoft.Photos.exe

Version:

Path:

C:\Program Files\WindowsApps\Microsoft.Windows.Photos_2019.19071.12548.0_x64__8wekyb3d8bbwe\Microsoft.Photos.exe

Command Line:

"C:\Program Files\WindowsApps\Microsoft.Windows.Photos_2019.19071.12548.0_x64__8wekyb3d8bbwe\Microsoft.Photos.exe" -ServerName:App.Ap

PID:	8164	Architecture:	64-bit
Parent PID:	776	Virtualized:	False
Session ID:	1	Integrity:	Low
User:	DESKTOP-AFIVS3H\sharumss		
Auth ID:	00000000:0004575d		
Started:	1/7/2024 1:56:03 PM	Ended:	(Running)

Modules:

Module	Address	Size	Path	Company	Version	Timestamp
gdi32full.dll	0x7ffa1c450000	0x11a000	C:\Windows\System32\gdi32full.dll	Microsoft Corp...	10.0.19041.375...	4/24/1962 8:20:...
BCrypt.dll	0x7ffa1c570000	0x27000	C:\Windows\System32\BCrypt.dll	Microsoft Corp...	10.0.19041.1 (W...	4/2/1914 6:51:4...
crypt32.dll	0x7ffa1c5a0000	0x15d000	C:\Windows\System32\crypt32.dll	Microsoft Corp...	10.0.19041.1 (W...	11/10/1943 6:2...
cfgmgr32.dll	0x7ffa1c700000	0x4e000	C:\Windows\System32\cfgmgr32.dll	Microsoft Corp...	10.0.19041.363...	5/30/1986 8:43:...
msvcp_win.dll	0x7ffa1c870000	0x9d000	C:\Windows\System32\msvcp_win....	Microsoft Corp...	10.0.19041.363...	5/19/2000 7:25:...
win32u.dll	0x7ffa1ca10000	0x22000	C:\Windows\System32\win32u.dll	Microsoft Corp...	10.0.19041.380...	5/3/1977 12:26:...
bcryptPrimitives...	0x7ffa1ca40000	0x82000	C:\Windows\System32\bcryptPrim...	Microsoft Corp...	10.0.19041.363...	2/17/1965 3:13:...
SHELL32.dll	0x7ffa1caf0000	0x745000	C:\Windows\System32\SHELL32.dll	Microsoft Corp...	10.0.19041.363...	1/9/1938 4:36:1...
GDI32.dll	0x7ffa1d260000	0x2c000	C:\Windows\System32\GDI32.dll	Microsoft Corp...	10.0.19041.363...	10/28/2029 6:2...
shcore.dll	0x7ffa1d290000	0xad000	C:\Windows\System32\shcore.dll	Microsoft Corp...	10.0.19041.1 (W...	10/7/1999 5:52:...
KERNEL32.DLL	0x7ffa1d340000	0xbd000	C:\Windows\System32\KERNEL32....	Microsoft Corp...	10.0.19041.363...	4/27/1918 1:30:...
RPCRT4.dll	0x7ffa1d540000	0x126000	C:\Windows\System32\RPCRT4.dll	Microsoft Corp...	10.0.19041.363...	3/12/1920 1:57:...
ole32.dll	0x7ffa1d670000	0x12b000	C:\Windows\System32\ole32.dll	Microsoft Corp...	10.0.19041.363...	9/13/1936 4:40:...
advapi32.dll	0x7ffa1d7a0000	0xaf000	C:\Windows\System32\advapi32.dll	Microsoft Corp...	10.0.19041.1 (W...	8/27/1988 12:4...
sechost.dll	0x7ffa1d850000	0x9c000	C:\Windows\System32\sechost.dll	Microsoft Corp...	10.0.19041.1 (W...	11/20/1917 10:...
OleAut32.dll	0x7ffa1d8f0000	0xcd000	C:\Windows\System32\OleAut32.dll	Microsoft Corp...	10.0.19041.363...	9/15/1946 6:28:...
combase.dll	0x7ffa1d9c0000	0x354000	C:\Windows\System32\combase.dll	Microsoft Corp...	10.0.19041.363...	9/12/2021 2:20:...
IMM32.DLL	0x7ffa1dd20000	0x30000	C:\Windows\System32\IMM32.DLL	Microsoft Corp...	10.0.19041.363...	2/19/1932 6:54:...
Normaliz.dll	0x7ffa1ddb0000	0x8000	C:\Windows\System32\Normaliz.dll	Microsoft Corp...	10.0.19041.363...	5/31/1908 12:5...
shlwapi.dll	0x7ffa1e230000	0x55000	C:\Windows\System32\shlwapi.dll	Microsoft Corp...	10.0.19041.1 (W...	12/27/1987 6:1...
ws2_32.dll	0x7ffa1e440000	0x6b000	C:\Windows\System32\ws2_32.dll	Microsoft Corp...	10.0.19041.363...	11/20/2034 5:2...
USER32.dll	0x7ffa1e610000	0x19e000	C:\Windows\System32\USER32.dll	Microsoft Corp...	10.0.19041.1 (W...	1/17/1980 4:56:...
msctf.dll	0x7ffa1e7b0000	0x114000	C:\Windows\System32\msctf.dll	Microsoft Corp...	10.0.19041.1 (W...	8/7/1969 6:30:5...
msvcrt.dll	0x7ffa1e990000	0x9e000	C:\Windows\System32\msvcrt.dll	Microsoft Corp...	7.0.19041.3636 ...	10/25/1916 1:1...
ntdll.dll	0x7ffa1ea70000	0x1f8000	C:\Windows\SYSTEM32\ntdll.dll	Microsoft Corp...	10.0.19041.363...	7/6/1916 6:26:5...

Figure 31 Event Properties of Microsoft.Photos.exe

To further explore, the path of Microsoft.Photos.exe was navigated. But the permission to the folder was denied, even as an administrator. Also, the directory wasn't listed in the parent directory, but it existed.

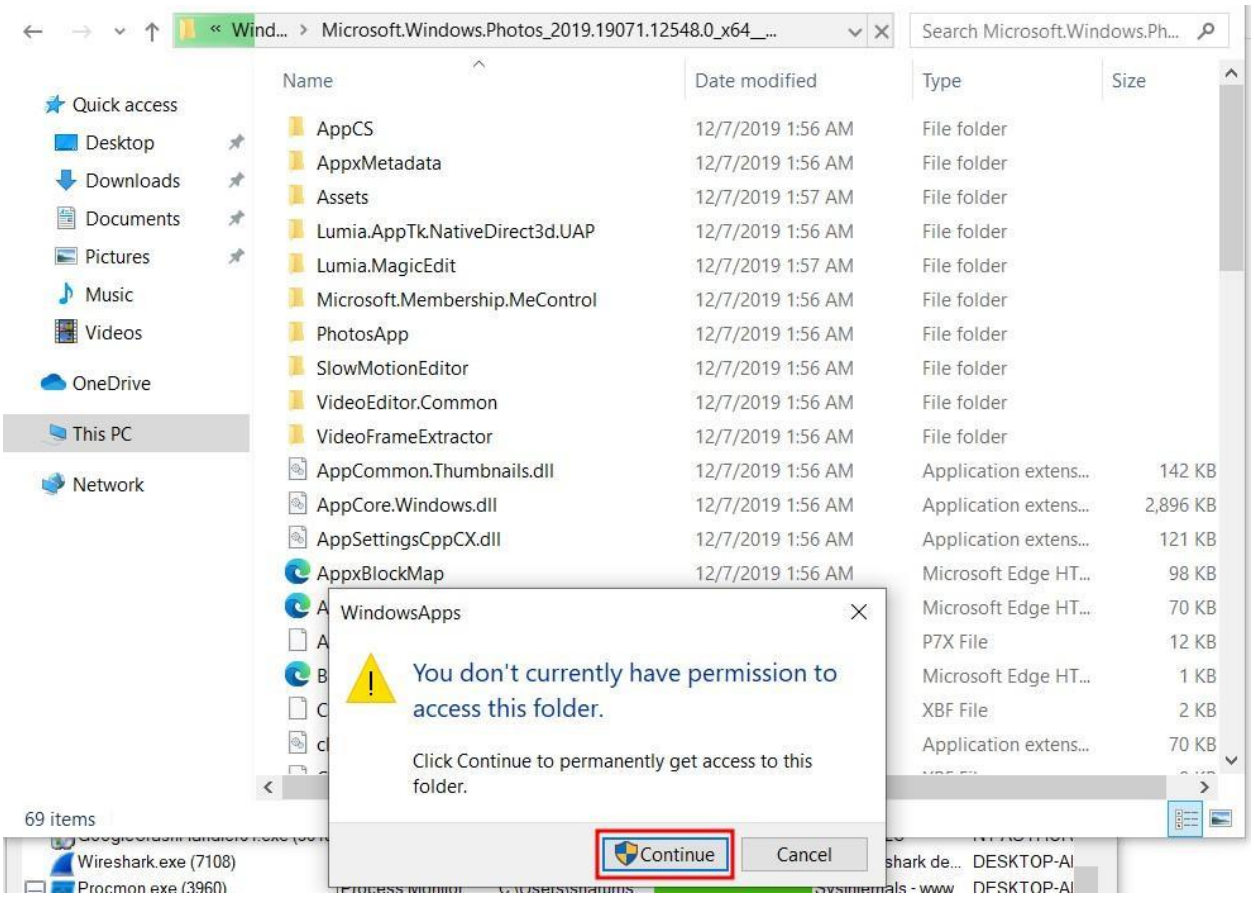


Figure 32 Permission denied to Microsoft.Photos.exe directory.

Following was the access control set up for the directory. An unidentified SID could be seen.

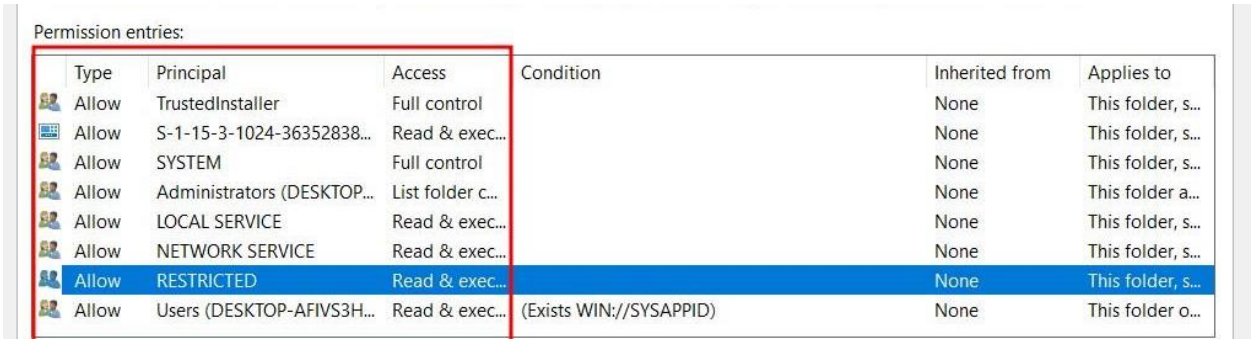


Figure 33 Permission Entries

Access Control entry for the USERS was corrupted.

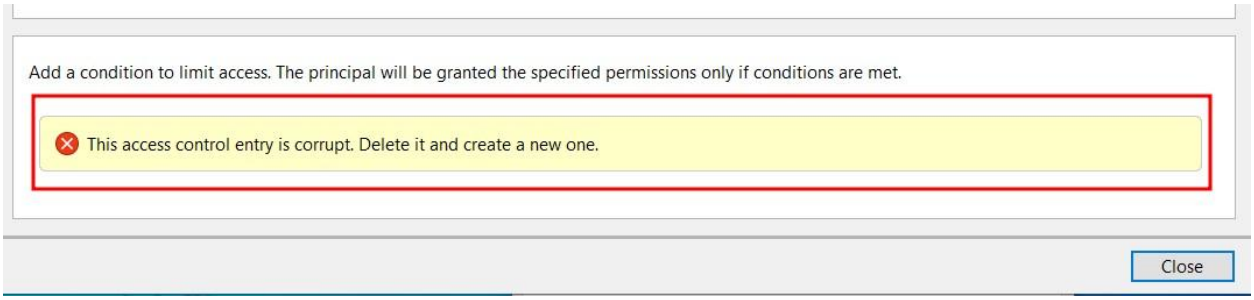


Figure 34 Corrupted Access List Entry

Also, access was denied on trying to edit the list by creating a new entry.

Figure 35 Error Applying Security

Since the folder wasn't accessible, Procmon was rechecked to discover any new processes. Suddenly, the background processes of Microsoft.Photos.exe had increased, it was seen making changes in the registry, and making changes/reading files it had downloaded and unlocking local files.

Time o...	Process Name	PID	Operation	Path	Result	Detail
2:22:13....	Microsoft.Photo...	8164	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
2:22:13....	Microsoft.Photo...	8164	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\...	NAME NOT FOUND	Desired Access: Q...
2:22:13....	Microsoft.Photo...	8164	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
2:22:13....	Microsoft.Photo...	8164	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\...	NAME NOT FOUND	Desired Access: Q...
2:22:13....	Microsoft.Photo...	8164	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
2:22:13....	Microsoft.Photo...	8164	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\...	NAME NOT FOUND	Desired Access: Q...
2:22:13....	Microsoft.Photo...	8164	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
2:22:13....	Microsoft.Photo...	8164	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\...	NAME NOT FOUND	Desired Access: Q...
2:22:13....	Microsoft.Photo...	8164	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
2:22:13.7562802 AM	ft.Photo...	8164	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\...	NAME NOT FOUND	Desired Access: Q...
2:22:13....	Microsoft.Photo...	8164	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
2:22:13....	Microsoft.Photo...	8164	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\...	NAME NOT FOUND	Desired Access: Q...
2:22:13....	Microsoft.Photo...	8164	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows...	NAME NOT FOUND	Desired Access: R...
2:22:13....	Microsoft.Photo...	8164	RegOpenKey	HKCR\ActivatableClasses\Package\Mic...	NAME NOT FOUND	Desired Access: R...
2:22:13....	Microsoft.Photo...	8164	RegOpenKey	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	SUCCESS	Desired Access: R...
2:22:13....	Microsoft.Photo...	8164	RegOpenKey	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	SUCCESS	Desired Access: R...
2:22:13....	Microsoft.Photo...	8164	RegQueryKey	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	SUCCESS	Query: Basic, Nam...
2:22:13....	Microsoft.Photo...	8164	RegQueryValue	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	SUCCESS	Type: REG_DWO...
2:22:13....	Microsoft.Photo...	8164	RegQueryValue	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	SUCCESS	Type: REG_SZ, Le...
2:22:13....	Microsoft.Photo...	8164	RegQueryValue	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	NAME NOT FOUND	Length: 144
2:22:13....	Microsoft.Photo...	8164	RegQueryValue	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	NAME NOT FOUND	Length: 16
2:22:13....	Microsoft.Photo...	8164	RegQueryValue	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	NAME NOT FOUND	Length: 16
2:22:13....	Microsoft.Photo...	8164	RegQueryKey	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	SUCCESS	Query: HandleTag...
2:22:13....	Microsoft.Photo...	8164	RegOpenKey	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	SUCCESS	Desired Access: R...
2:22:13....	Microsoft.Photo...	8164	RegSetInfoKey	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	SUCCESS	KeySetInformation...
2:22:13....	Microsoft.Photo...	8164	RegQueryValue	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	NAME NOT FOUND	Length: 16
2:22:13....	Microsoft.Photo...	8164	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows...	NAME NOT FOUND	Desired Access: R...
2:22:13....	Microsoft.Photo...	8164	RegOpenKey	HKCR\ActivatableClasses\Package\Mic...	NAME NOT FOUND	Desired Access: R...
2:22:13....	Microsoft.Photo...	8164	RegOpenKey	HKCR\ActivatableClasses\Package\Mic...	NAME NOT FOUND	Desired Access: R...
2:22:13....	Microsoft.Photo...	8164	RegOpenKey	HKCU\Software\Classes\ActivatableCla...	NAME NOT FOUND	Desired Access: R...
2:22:13....	Microsoft.Photo...	8164	RegOpenKey	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	SUCCESS	Desired Access: R...
2:22:13....	Microsoft.Photo...	8164	RegOpenKey	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	SUCCESS	Desired Access: R...
2:22:13....	Microsoft.Photo...	8164	RegQueryKey	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	SUCCESS	Query: Basic, Nam...
2:22:13....	Microsoft.Photo...	8164	RegQueryValue	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	SUCCESS	Type: REG_EXPA...
2:22:13....	Microsoft.Photo...	8164	RegQueryValue	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	NAME NOT FOUND	Length: 144
2:22:13....	Microsoft.Photo...	8164	RegQueryValue	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	SUCCESS	Type: REG_DWO...
2:22:13....	Microsoft.Photo...	8164	RegQueryValue	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	SUCCESS	Type: REG_SZ, Le...
2:22:13....	Microsoft.Photo...	8164	RegQueryValue	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	NAME NOT FOUND	Length: 144
2:22:13....	Microsoft.Photo...	8164	RegQueryValue	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	SUCCESS	Type: REG_DWO...
2:22:13....	Microsoft.Photo...	8164	RegQueryValue	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	SUCCESS	Type: REG_DWO...
2:22:13....	Microsoft.Photo...	8164	RegQueryValue	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	BUFFER OVERFL...	Length: 140
2:22:13....	Microsoft.Photo...	8164	RegQueryValue	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	BUFFER OVERFL...	Length: 144
2:22:13....	Microsoft.Photo...	8164	RegQueryValue	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	SUCCESS	Type: REG_BINAR...
2:22:13....	Microsoft.Photo...	8164	RegQueryValue	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	BUFFER OVERFL...	Length: 144
2:22:13....	Microsoft.Photo...	8164	RegQueryValue	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	BUFFER OVERFL...	Length: 144
2:22:13....	Microsoft.Photo...	8164	RegQueryValue	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	SUCCESS	Type: REG_MULTI...
2:22:13....	Microsoft.Photo...	8164	RegQueryValue	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	NAME NOT FOUND	Length: 16
2:22:13....	Microsoft.Photo...	8164	RegQueryValue	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	NAME NOT FOUND	Length: 16
2:22:13....	Microsoft.Photo...	8164	RegQueryValue	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	SUCCESS	Type: REG_DWO...
2:22:13....	Microsoft.Photo...	8164	RegQueryValue	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	SUCCESS	Type: REG_DWO...
2:22:13....	Microsoft.Photo...	8164	RegQueryValue	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	SUCCESS	Type: REG_DWO...
2:22:13....	Microsoft.Photo...	8164	RegQueryValue	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	NAME NOT FOUND	Length: 144
2:22:13....	Microsoft.Photo...	8164	RegQueryKey	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	SUCCESS	Query: HandleTag...
2:22:13....	Microsoft.Photo...	8164	RegOpenKey	\REGISTRY\A\{40D3A8C9-61E5-4600-B...	NAME NOT FOUND	Desired Access: R...
2:22:13....	Microsoft.Photo...	8164	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
2:22:13....	Microsoft.Photo...	8164	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\...	SUCCESS	Desired Access: R...
2:22:13....	Microsoft.Photo...	8164	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Windows\...	SUCCESS	KeySetInformation...
2:22:13....	Microsoft.Photo...	8164	RegQueryKey	HKLM\SOFTWARE\Microsoft\Windows\...	SUCCESS	Query: HandleTag...
2:22:13....	Microsoft.Photo...	8164	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\...	SUCCESS	Desired Access: R...
2:22:13....	Microsoft.Photo...	8164	RegQueryKey	HKLM\SOFTWARE\Microsoft\Windows\...	SUCCESS	Query: HandleTag...
2:22:13....	Microsoft.Photo...	8164	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\...	SUCCESS	Desired Access: R...
2:22:13....	Microsoft.Photo...	8164	RegEnumKey	HKLM\SOFTWARE\Microsoft\Windows\...	SUCCESS	Index: 0, Name: 70
2:22:13....	Microsoft.Photo...	8164	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\...	SUCCESS	
2:22:13....	Microsoft.Photo...	8164	RegQueryKey	HKLM\SOFTWARE\Microsoft\Windows\...	SUCCESS	Query: HandleTag...
2:22:13....	Microsoft.Photo...	8164	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\...	SUCCESS	Desired Access: R...
2:22:13....	Microsoft.Photo...	8164	RegEnumKey	HKLM\SOFTWARE\Microsoft\Windows\...	SUCCESS	Index: 0, Name: 3
2:22:13....	Microsoft.Photo...	8164	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\...	SUCCESS	
2:22:13....	Microsoft.Photo...	8164	RegQueryKey	HKLM\SOFTWARE\Microsoft\Windows\...	SUCCESS	Query: HandleTag...

Showing 3,465 of 3,865,776 events (0.089%) Backed by virtual memory

Figure 36 Changes in Registry

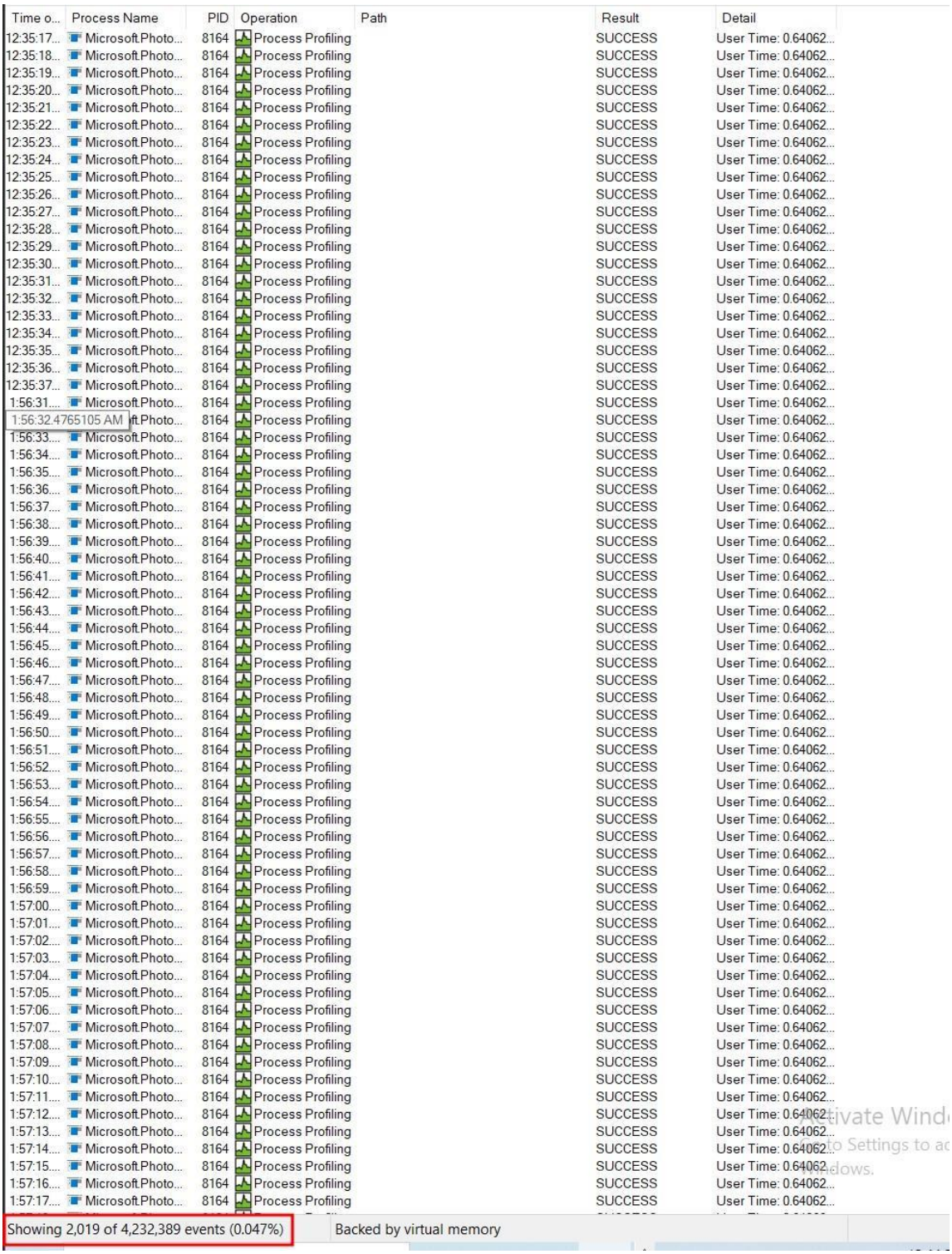
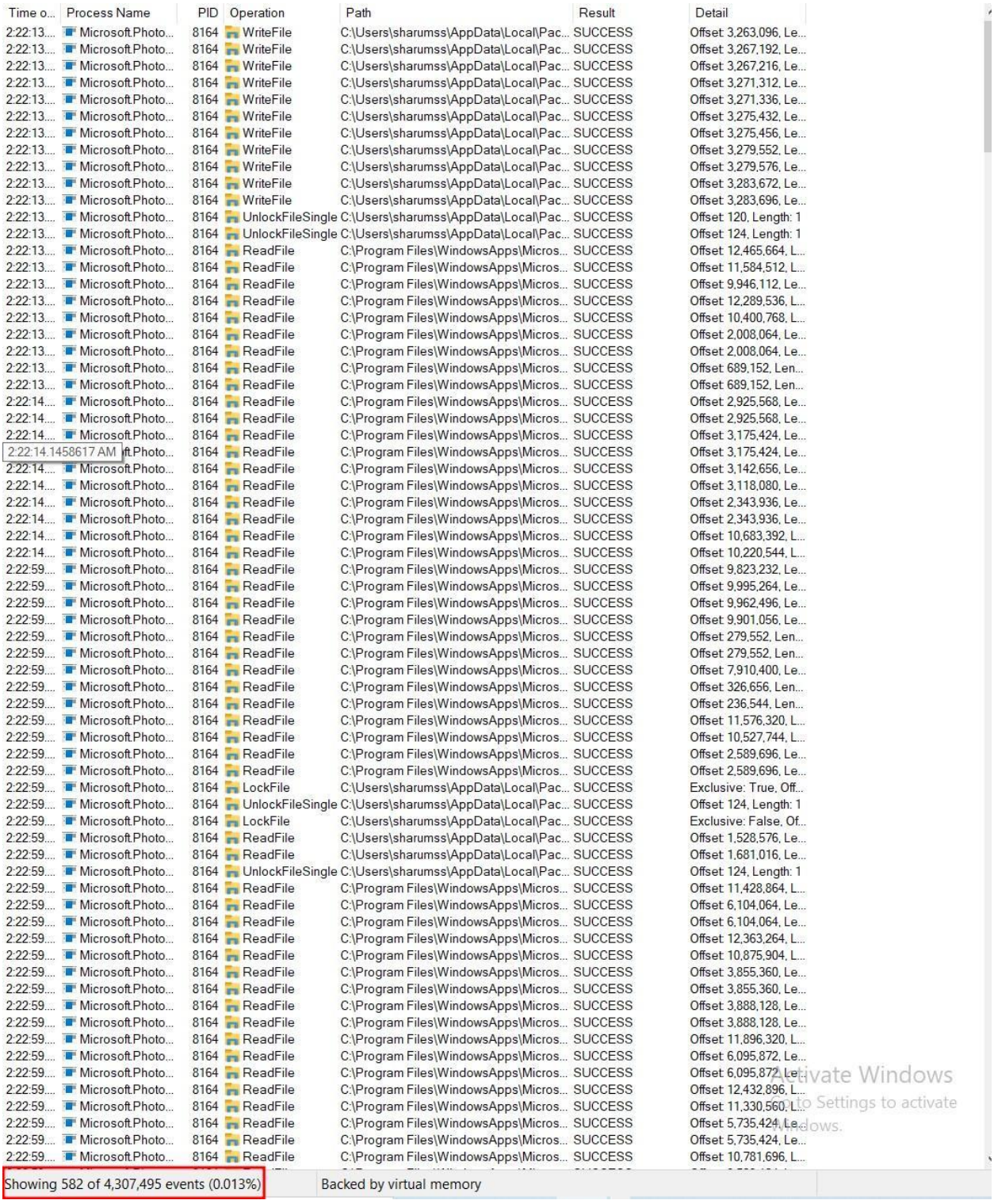


Figure 37 Increase in Process Profiling Operation



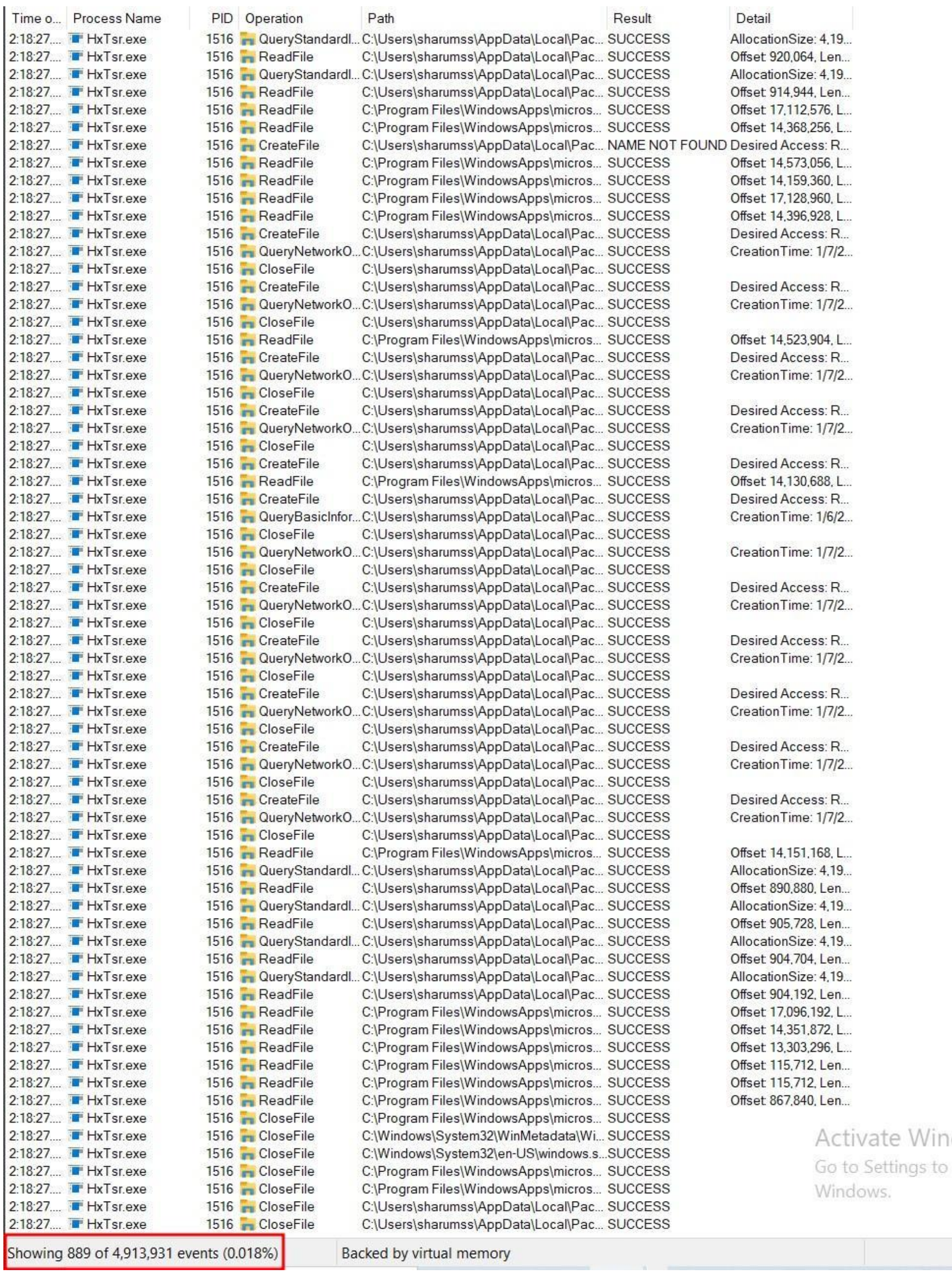
Time o...	Process Name	PID	Operation	Path	Result	Detail
2:22:13....	Microsoft.Photo...	8164	WriteFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Offset: 3,263,096, Le...
2:22:13....	Microsoft.Photo...	8164	WriteFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Offset: 3,267,192, Le...
2:22:13....	Microsoft.Photo...	8164	WriteFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Offset: 3,267,216, Le...
2:22:13....	Microsoft.Photo...	8164	WriteFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Offset: 3,271,312, Le...
2:22:13....	Microsoft.Photo...	8164	WriteFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Offset: 3,271,336, Le...
2:22:13....	Microsoft.Photo...	8164	WriteFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Offset: 3,275,432, Le...
2:22:13....	Microsoft.Photo...	8164	WriteFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Offset: 3,275,456, Le...
2:22:13....	Microsoft.Photo...	8164	WriteFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Offset: 3,279,552, Le...
2:22:13....	Microsoft.Photo...	8164	WriteFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Offset: 3,279,576, Le...
2:22:13....	Microsoft.Photo...	8164	WriteFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Offset: 3,283,672, Le...
2:22:13....	Microsoft.Photo...	8164	WriteFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Offset: 3,283,696, Le...
2:22:13....	Microsoft.Photo...	8164	UnlockFileSingle	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Offset: 120, Length: 1
2:22:13....	Microsoft.Photo...	8164	UnlockFileSingle	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Offset: 124, Length: 1
2:22:13....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 12,465,664, L...
2:22:13....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 11,584,512, L...
2:22:13....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 9,946,112, Le...
2:22:13....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 12,289,536, L...
2:22:13....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 10,400,768, L...
2:22:13....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 2,008,064, Le...
2:22:13....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 2,008,064, Le...
2:22:13....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 689,152, Len...
2:22:13....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 689,152, Len...
2:22:14....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 2,925,568, Le...
2:22:14....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 2,925,568, Le...
2:22:14....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 3,175,424, Le...
2:22:14.1458617 AM	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 3,175,424, Le...
2:22:14....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 3,142,656, Le...
2:22:14....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 3,118,080, Le...
2:22:14....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 2,343,936, Le...
2:22:14....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 2,343,936, Le...
2:22:14....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 10,683,392, L...
2:22:14....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 10,220,544, L...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 9,823,232, Le...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 9,995,264, Le...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 9,962,496, Le...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 9,901,056, Le...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 279,552, Len...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 279,552, Len...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 7,910,400, Le...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 326,656, Len...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 236,544, Len...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 11,576,320, L...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 10,527,744, L...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 2,589,696, Le...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 2,589,696, Le...
2:22:59....	Microsoft.Photo...	8164	LockFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Exclusive: True, Off...
2:22:59....	Microsoft.Photo...	8164	UnlockFileSingle	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Offset: 124, Length: 1
2:22:59....	Microsoft.Photo...	8164	LockFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Exclusive: False, Of...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Offset: 1,528,576, Le...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Offset: 1,681,016, Le...
2:22:59....	Microsoft.Photo...	8164	UnlockFileSingle	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Offset: 124, Length: 1
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 11,428,864, L...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 6,104,064, Le...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 6,104,064, Le...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 12,363,264, L...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 10,875,904, L...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 3,855,360, Le...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 3,855,360, Le...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 3,888,128, Le...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 3,888,128, Le...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 11,896,320, L...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 6,095,872, Le...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 6,095,872, Le...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 12,432,896, L...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 11,330,560, L...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 5,735,424, Le...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 5,735,424, Le...
2:22:59....	Microsoft.Photo...	8164	ReadFile	C:\Program Files\WindowsApps\Micros...	SUCCESS	Offset: 10,781,696, L...

Showing 582 of 4,307,495 events (0.013%) Backed by virtual memory

Figure 38 Reading/Writing backdoor files.

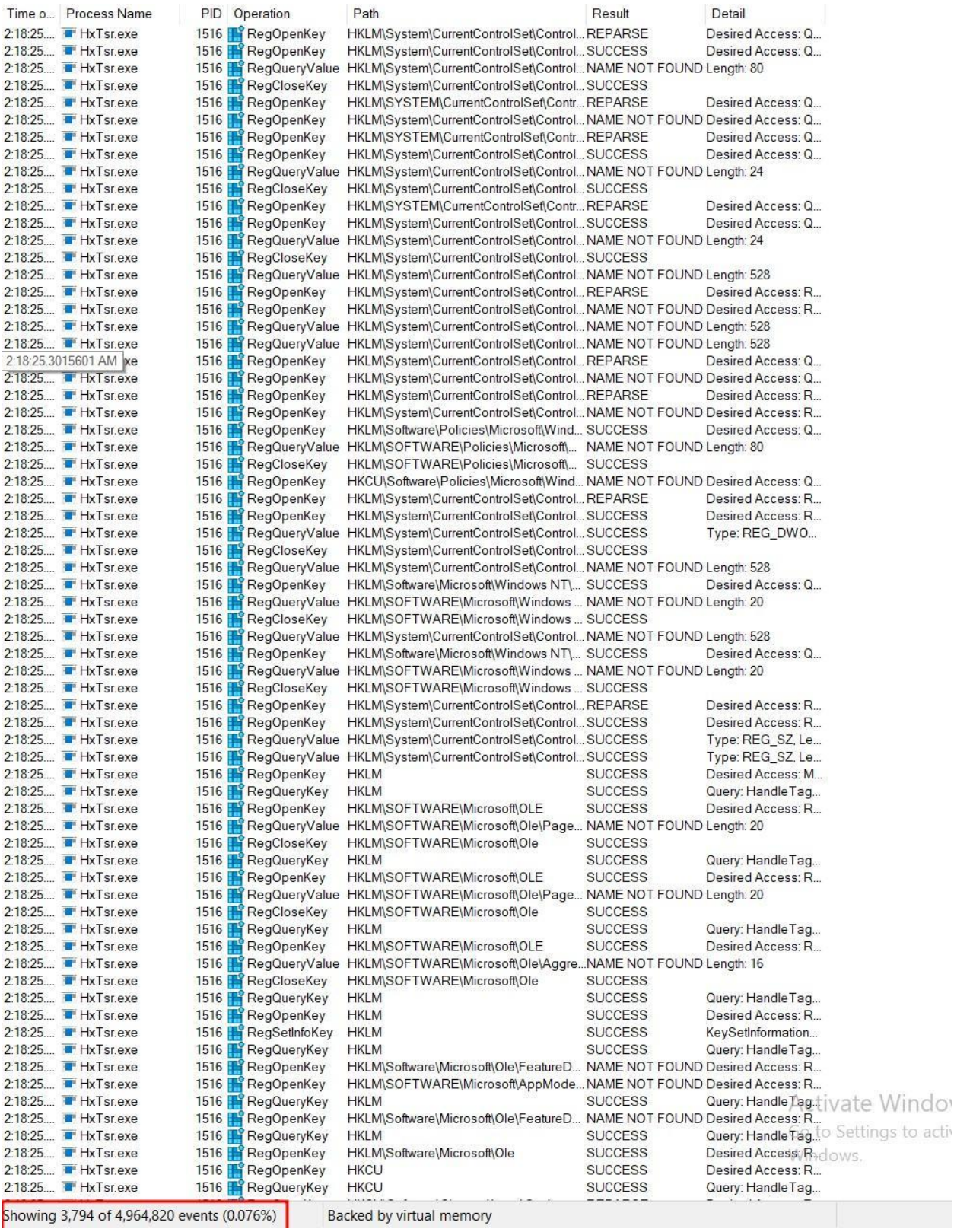
Procmon was rechecked to discover any new processes. On the course of it, many such process were found.

HxTsr.exe, which is a part of Microsoft Outlook, was running in the background, making changes to registry, reading initially discovered backdoors, querying networks, storage, keystrokes, etc.



Time o...	Process Name	PID	Operation	Path	Result	Detail
2:18:27....	HxTsr.exe	1516	QueryStandardI...	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	AllocationSize: 4,19...
2:18:27....	HxTsr.exe	1516	ReadFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Offset: 920,064, Len...
2:18:27....	HxTsr.exe	1516	QueryStandardI...	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	AllocationSize: 4,19...
2:18:27....	HxTsr.exe	1516	ReadFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Offset: 914,944, Len...
2:18:27....	HxTsr.exe	1516	ReadFile	C:\Program Files\WindowsApps\micros...	SUCCESS	Offset: 17,112,576, L...
2:18:27....	HxTsr.exe	1516	ReadFile	C:\Program Files\WindowsApps\micros...	SUCCESS	Offset: 14,368,256, L...
2:18:27....	HxTsr.exe	1516	CreateFile	C:\Users\sharumss\AppData\Local\Pac...	NAME NOT FOUND	Desired Access: R...
2:18:27....	HxTsr.exe	1516	ReadFile	C:\Program Files\WindowsApps\micros...	SUCCESS	Offset: 14,573,056, L...
2:18:27....	HxTsr.exe	1516	ReadFile	C:\Program Files\WindowsApps\micros...	SUCCESS	Offset: 14,159,360, L...
2:18:27....	HxTsr.exe	1516	ReadFile	C:\Program Files\WindowsApps\micros...	SUCCESS	Offset: 17,128,960, L...
2:18:27....	HxTsr.exe	1516	ReadFile	C:\Program Files\WindowsApps\micros...	SUCCESS	Offset: 14,396,928, L...
2:18:27....	HxTsr.exe	1516	CreateFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Desired Access: R...
2:18:27....	HxTsr.exe	1516	QueryNetworkO...	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	CreationTime: 1/7/2...
2:18:27....	HxTsr.exe	1516	CloseFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	
2:18:27....	HxTsr.exe	1516	CreateFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Desired Access: R...
2:18:27....	HxTsr.exe	1516	QueryNetworkO...	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	CreationTime: 1/7/2...
2:18:27....	HxTsr.exe	1516	CloseFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	
2:18:27....	HxTsr.exe	1516	ReadFile	C:\Program Files\WindowsApps\micros...	SUCCESS	Offset: 14,523,904, L...
2:18:27....	HxTsr.exe	1516	CreateFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Desired Access: R...
2:18:27....	HxTsr.exe	1516	QueryNetworkO...	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	CreationTime: 1/7/2...
2:18:27....	HxTsr.exe	1516	CloseFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	
2:18:27....	HxTsr.exe	1516	CreateFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Desired Access: R...
2:18:27....	HxTsr.exe	1516	QueryNetworkO...	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	CreationTime: 1/7/2...
2:18:27....	HxTsr.exe	1516	CloseFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	
2:18:27....	HxTsr.exe	1516	CreateFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Desired Access: R...
2:18:27....	HxTsr.exe	1516	ReadFile	C:\Program Files\WindowsApps\micros...	SUCCESS	Offset: 14,130,688, L...
2:18:27....	HxTsr.exe	1516	CreateFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Desired Access: R...
2:18:27....	HxTsr.exe	1516	QueryBasicInfor...	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	CreationTime: 1/6/2...
2:18:27....	HxTsr.exe	1516	CloseFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	
2:18:27....	HxTsr.exe	1516	QueryNetworkO...	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	CreationTime: 1/7/2...
2:18:27....	HxTsr.exe	1516	CloseFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	
2:18:27....	HxTsr.exe	1516	CreateFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Desired Access: R...
2:18:27....	HxTsr.exe	1516	QueryNetworkO...	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	CreationTime: 1/7/2...
2:18:27....	HxTsr.exe	1516	CloseFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	
2:18:27....	HxTsr.exe	1516	CreateFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Desired Access: R...
2:18:27....	HxTsr.exe	1516	QueryNetworkO...	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	CreationTime: 1/7/2...
2:18:27....	HxTsr.exe	1516	CloseFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	
2:18:27....	HxTsr.exe	1516	CreateFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Desired Access: R...
2:18:27....	HxTsr.exe	1516	QueryNetworkO...	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	CreationTime: 1/7/2...
2:18:27....	HxTsr.exe	1516	CloseFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	
2:18:27....	HxTsr.exe	1516	CreateFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Desired Access: R...
2:18:27....	HxTsr.exe	1516	QueryNetworkO...	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	CreationTime: 1/7/2...
2:18:27....	HxTsr.exe	1516	CloseFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	
2:18:27....	HxTsr.exe	1516	CreateFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Desired Access: R...
2:18:27....	HxTsr.exe	1516	QueryNetworkO...	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	CreationTime: 1/7/2...
2:18:27....	HxTsr.exe	1516	CloseFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	
2:18:27....	HxTsr.exe	1516	ReadFile	C:\Program Files\WindowsApps\micros...	SUCCESS	Offset: 14,151,168, L...
2:18:27....	HxTsr.exe	1516	QueryStandardI...	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	AllocationSize: 4,19...
2:18:27....	HxTsr.exe	1516	ReadFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Offset: 890,880, Len...
2:18:27....	HxTsr.exe	1516	QueryStandardI...	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	AllocationSize: 4,19...
2:18:27....	HxTsr.exe	1516	ReadFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Offset: 905,728, Len...
2:18:27....	HxTsr.exe	1516	QueryStandardI...	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	AllocationSize: 4,19...
2:18:27....	HxTsr.exe	1516	ReadFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Offset: 904,704, Len...
2:18:27....	HxTsr.exe	1516	QueryStandardI...	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	AllocationSize: 4,19...
2:18:27....	HxTsr.exe	1516	ReadFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	Offset: 904,192, Len...
2:18:27....	HxTsr.exe	1516	ReadFile	C:\Program Files\WindowsApps\micros...	SUCCESS	Offset: 17,096,192, L...
2:18:27....	HxTsr.exe	1516	ReadFile	C:\Program Files\WindowsApps\micros...	SUCCESS	Offset: 14,351,872, L...
2:18:27....	HxTsr.exe	1516	ReadFile	C:\Program Files\WindowsApps\micros...	SUCCESS	Offset: 13,303,296, L...
2:18:27....	HxTsr.exe	1516	ReadFile	C:\Program Files\WindowsApps\micros...	SUCCESS	Offset: 115,712, Len...
2:18:27....	HxTsr.exe	1516	ReadFile	C:\Program Files\WindowsApps\micros...	SUCCESS	Offset: 115,712, Len...
2:18:27....	HxTsr.exe	1516	ReadFile	C:\Program Files\WindowsApps\micros...	SUCCESS	Offset: 867,840, Len...
2:18:27....	HxTsr.exe	1516	CloseFile	C:\Program Files\WindowsApps\micros...	SUCCESS	
2:18:27....	HxTsr.exe	1516	CloseFile	C:\Windows\System32\WinMetadata\Wi...	SUCCESS	
2:18:27....	HxTsr.exe	1516	CloseFile	C:\Windows\System32\en-US\windows.s...	SUCCESS	
2:18:27....	HxTsr.exe	1516	CloseFile	C:\Program Files\WindowsApps\micros...	SUCCESS	
2:18:27....	HxTsr.exe	1516	CloseFile	C:\Program Files\WindowsApps\micros...	SUCCESS	
2:18:27....	HxTsr.exe	1516	CloseFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	
2:18:27....	HxTsr.exe	1516	CloseFile	C:\Users\sharumss\AppData\Local\Pac...	SUCCESS	

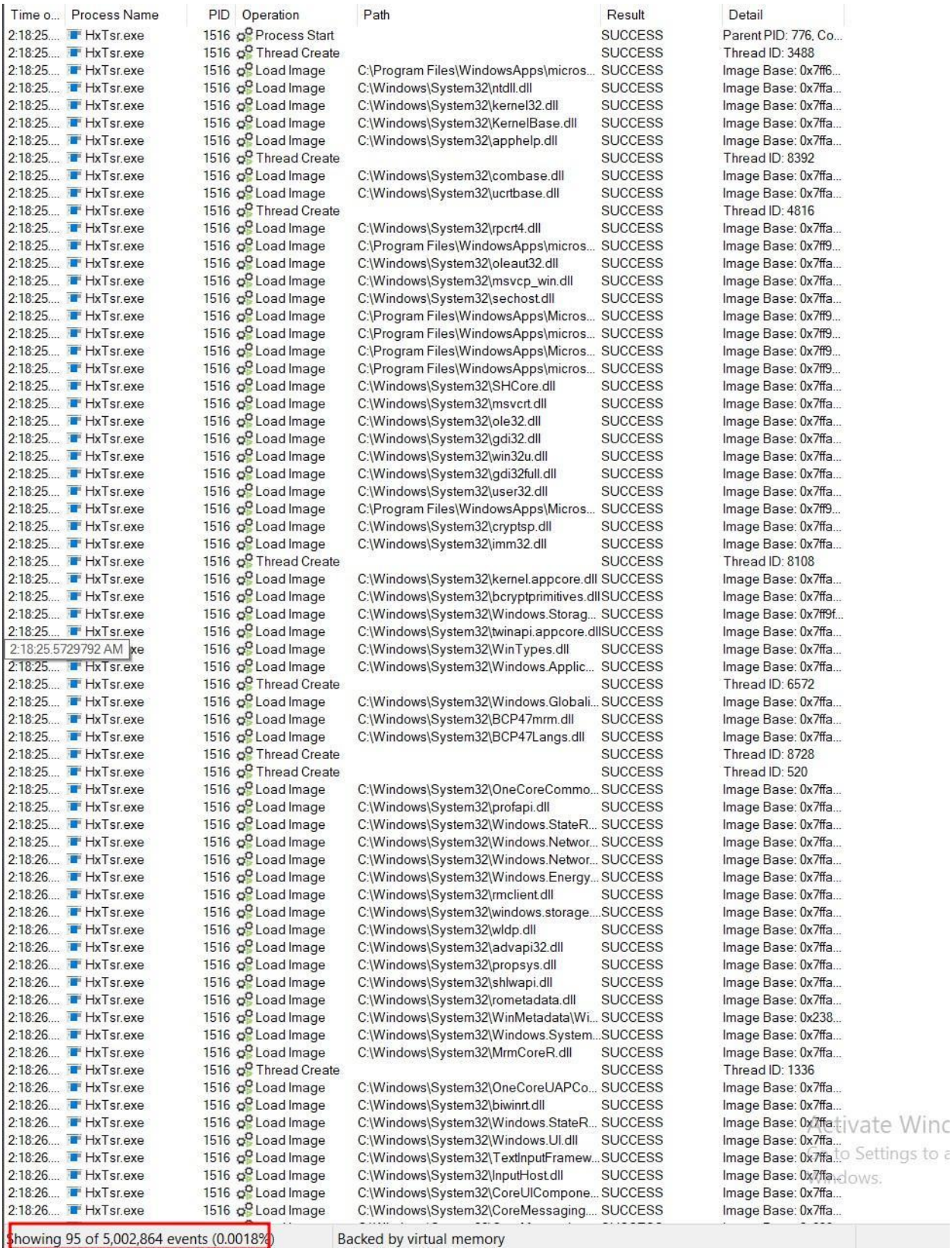
Figure 39 HxTsr making changes to system files.



Time o...	Process Name	PID	Operation	Path	Result	Detail
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\System\CurrentControlSet\Control...	REPARSE	Desired Access: Q...
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\System\CurrentControlSet\Control...	SUCCESS	Desired Access: Q...
2:18:25....	HxTsr.exe	1516	RegQueryValue	HKLM\System\CurrentControlSet\Control...	NAME NOT FOUND	Length: 80
2:18:25....	HxTsr.exe	1516	RegCloseKey	HKLM\System\CurrentControlSet\Control...	SUCCESS	
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\System\CurrentControlSet\Control...	NAME NOT FOUND	Desired Access: Q...
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\System\CurrentControlSet\Control...	SUCCESS	Desired Access: Q...
2:18:25....	HxTsr.exe	1516	RegQueryValue	HKLM\System\CurrentControlSet\Control...	NAME NOT FOUND	Length: 24
2:18:25....	HxTsr.exe	1516	RegCloseKey	HKLM\System\CurrentControlSet\Control...	SUCCESS	
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\System\CurrentControlSet\Control...	SUCCESS	Desired Access: Q...
2:18:25....	HxTsr.exe	1516	RegQueryValue	HKLM\System\CurrentControlSet\Control...	NAME NOT FOUND	Length: 24
2:18:25....	HxTsr.exe	1516	RegCloseKey	HKLM\System\CurrentControlSet\Control...	SUCCESS	
2:18:25....	HxTsr.exe	1516	RegQueryValue	HKLM\System\CurrentControlSet\Control...	NAME NOT FOUND	Length: 528
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\System\CurrentControlSet\Control...	REPARSE	Desired Access: R...
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\System\CurrentControlSet\Control...	NAME NOT FOUND	Desired Access: R...
2:18:25....	HxTsr.exe	1516	RegQueryValue	HKLM\System\CurrentControlSet\Control...	NAME NOT FOUND	Length: 528
2:18:25....	HxTsr.exe	1516	RegQueryValue	HKLM\System\CurrentControlSet\Control...	NAME NOT FOUND	Length: 528
2:18:25.3015601 AM	xe	1516	RegOpenKey	HKLM\System\CurrentControlSet\Control...	REPARSE	Desired Access: Q...
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\System\CurrentControlSet\Control...	NAME NOT FOUND	Desired Access: Q...
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\System\CurrentControlSet\Control...	REPARSE	Desired Access: R...
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\System\CurrentControlSet\Control...	NAME NOT FOUND	Desired Access: R...
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\Software\Policies\Microsoft\Wind...	SUCCESS	Desired Access: Q...
2:18:25....	HxTsr.exe	1516	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND	Length: 80
2:18:25....	HxTsr.exe	1516	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKCU\Software\Policies\Microsoft\Wind...	NAME NOT FOUND	Desired Access: Q...
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\System\CurrentControlSet\Control...	REPARSE	Desired Access: R...
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\System\CurrentControlSet\Control...	SUCCESS	Desired Access: R...
2:18:25....	HxTsr.exe	1516	RegQueryValue	HKLM\System\CurrentControlSet\Control...	SUCCESS	Type: REG_DWO...
2:18:25....	HxTsr.exe	1516	RegCloseKey	HKLM\System\CurrentControlSet\Control...	SUCCESS	
2:18:25....	HxTsr.exe	1516	RegQueryValue	HKLM\System\CurrentControlSet\Control...	NAME NOT FOUND	Length: 528
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\Software\Microsoft\Windows NT\...	SUCCESS	Desired Access: Q...
2:18:25....	HxTsr.exe	1516	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows ...	NAME NOT FOUND	Length: 20
2:18:25....	HxTsr.exe	1516	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows ...	SUCCESS	
2:18:25....	HxTsr.exe	1516	RegQueryValue	HKLM\System\CurrentControlSet\Control...	NAME NOT FOUND	Length: 528
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\Software\Microsoft\Windows NT\...	SUCCESS	Desired Access: Q...
2:18:25....	HxTsr.exe	1516	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows ...	NAME NOT FOUND	Length: 20
2:18:25....	HxTsr.exe	1516	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows ...	SUCCESS	
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\System\CurrentControlSet\Control...	REPARSE	Desired Access: R...
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\System\CurrentControlSet\Control...	SUCCESS	Desired Access: R...
2:18:25....	HxTsr.exe	1516	RegQueryValue	HKLM\System\CurrentControlSet\Control...	SUCCESS	Type: REG_SZ, Le...
2:18:25....	HxTsr.exe	1516	RegQueryValue	HKLM\System\CurrentControlSet\Control...	SUCCESS	Type: REG_SZ, Le...
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM	SUCCESS	Desired Access: M...
2:18:25....	HxTsr.exe	1516	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\SOFTWARE\Microsoft\OLE	SUCCESS	Desired Access: R...
2:18:25....	HxTsr.exe	1516	RegQueryValue	HKLM\SOFTWARE\Microsoft\Ole\Page...	NAME NOT FOUND	Length: 20
2:18:25....	HxTsr.exe	1516	RegCloseKey	HKLM\SOFTWARE\Microsoft\Ole	SUCCESS	
2:18:25....	HxTsr.exe	1516	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\SOFTWARE\Microsoft\OLE	SUCCESS	Desired Access: R...
2:18:25....	HxTsr.exe	1516	RegQueryValue	HKLM\SOFTWARE\Microsoft\Ole\Page...	NAME NOT FOUND	Length: 20
2:18:25....	HxTsr.exe	1516	RegCloseKey	HKLM\SOFTWARE\Microsoft\Ole	SUCCESS	
2:18:25....	HxTsr.exe	1516	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\SOFTWARE\Microsoft\OLE	SUCCESS	Desired Access: R...
2:18:25....	HxTsr.exe	1516	RegQueryValue	HKLM\SOFTWARE\Microsoft\Ole\Aggre...	NAME NOT FOUND	Length: 16
2:18:25....	HxTsr.exe	1516	RegCloseKey	HKLM\SOFTWARE\Microsoft\Ole	SUCCESS	
2:18:25....	HxTsr.exe	1516	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM	SUCCESS	Desired Access: R...
2:18:25....	HxTsr.exe	1516	RegSetInfoKey	HKLM	SUCCESS	KeySetInformation...
2:18:25....	HxTsr.exe	1516	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\Software\Microsoft\Ole\FeatureD...	NAME NOT FOUND	Desired Access: R...
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\SOFTWARE\Microsoft\AppMode...	NAME NOT FOUND	Desired Access: R...
2:18:25....	HxTsr.exe	1516	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\Software\Microsoft\Ole\FeatureD...	NAME NOT FOUND	Desired Access: R...
2:18:25....	HxTsr.exe	1516	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKLM\Software\Microsoft\Ole	SUCCESS	Desired Access: R...
2:18:25....	HxTsr.exe	1516	RegOpenKey	HKCU	SUCCESS	Desired Access: R...
2:18:25....	HxTsr.exe	1516	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...

Showing 3,794 of 4,964,820 events (0.076%) Backed by virtual memory

Figure 40 HxTsr making changes to registry.



Time o...	Process Name	PID	Operation	Path	Result	Detail
2:18:25....	HxTsr.exe	1516	Process Start		SUCCESS	Parent PID: 776, Co...
2:18:25....	HxTsr.exe	1516	Thread Create		SUCCESS	Thread ID: 3488
2:18:25....	HxTsr.exe	1516	Load Image	C:\Program Files\WindowsApps\micros...	SUCCESS	Image Base: 0x7ff6...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\KernelBase.dll	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\apphelp.dll	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Thread Create		SUCCESS	Thread ID: 8392
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\combase.dll	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\ucrtbase.dll	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Thread Create		SUCCESS	Thread ID: 4816
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\rpcrt4.dll	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Program Files\WindowsApps\micros...	SUCCESS	Image Base: 0x7ff9...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\oleaut32.dll	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\msvcp_win.dll	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\sechost.dll	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Program Files\WindowsApps\Micros...	SUCCESS	Image Base: 0x7ff9...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Program Files\WindowsApps\micros...	SUCCESS	Image Base: 0x7ff9...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Program Files\WindowsApps\Micros...	SUCCESS	Image Base: 0x7ff9...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Program Files\WindowsApps\micros...	SUCCESS	Image Base: 0x7ff9...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\SHCore.dll	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\msvcrt.dll	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\ole32.dll	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\gdi32.dll	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\win32u.dll	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\gdi32full.dll	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Program Files\WindowsApps\Micros...	SUCCESS	Image Base: 0x7ff9...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\cryptsp.dll	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\imm32.dll	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Thread Create		SUCCESS	Thread ID: 8108
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\kernel.appcore.dll	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\bcryptprimitives.dll	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\Windows.Storag...	SUCCESS	Image Base: 0x7ff9f...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\twinapi.appcore.dll	SUCCESS	Image Base: 0x7ffa...
2:18:25.5729792 AM	xe	1516	Load Image	C:\Windows\System32\WinTypes.dll	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\Windows.Applic...	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Thread Create		SUCCESS	Thread ID: 6572
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\Windows.Globali...	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\BCP47mrm.dll	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\BCP47Langs.dll	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Thread Create		SUCCESS	Thread ID: 8728
2:18:25....	HxTsr.exe	1516	Thread Create		SUCCESS	Thread ID: 520
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\OneCoreCommo...	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\profapi.dll	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\Windows.StateR...	SUCCESS	Image Base: 0x7ffa...
2:18:25....	HxTsr.exe	1516	Load Image	C:\Windows\System32\Windows.Networ...	SUCCESS	Image Base: 0x7ffa...
2:18:26....	HxTsr.exe	1516	Load Image	C:\Windows\System32\Windows.Networ...	SUCCESS	Image Base: 0x7ffa...
2:18:26....	HxTsr.exe	1516	Load Image	C:\Windows\System32\Windows.Energy...	SUCCESS	Image Base: 0x7ffa...
2:18:26....	HxTsr.exe	1516	Load Image	C:\Windows\System32\rmclient.dll	SUCCESS	Image Base: 0x7ffa...
2:18:26....	HxTsr.exe	1516	Load Image	C:\Windows\System32\windows.storage....	SUCCESS	Image Base: 0x7ffa...
2:18:26....	HxTsr.exe	1516	Load Image	C:\Windows\System32\wldp.dll	SUCCESS	Image Base: 0x7ffa...
2:18:26....	HxTsr.exe	1516	Load Image	C:\Windows\System32\advapi32.dll	SUCCESS	Image Base: 0x7ffa...
2:18:26....	HxTsr.exe	1516	Load Image	C:\Windows\System32\propsys.dll	SUCCESS	Image Base: 0x7ffa...
2:18:26....	HxTsr.exe	1516	Load Image	C:\Windows\System32\shlwapi.dll	SUCCESS	Image Base: 0x7ffa...
2:18:26....	HxTsr.exe	1516	Load Image	C:\Windows\System32\rometadata.dll	SUCCESS	Image Base: 0x7ffa...
2:18:26....	HxTsr.exe	1516	Load Image	C:\Windows\System32\WinMetadata\Wi...	SUCCESS	Image Base: 0x238...
2:18:26....	HxTsr.exe	1516	Load Image	C:\Windows\System32\Windows.System...	SUCCESS	Image Base: 0x7ffa...
2:18:26....	HxTsr.exe	1516	Load Image	C:\Windows\System32\MrmCoreR.dll	SUCCESS	Image Base: 0x7ffa...
2:18:26....	HxTsr.exe	1516	Thread Create		SUCCESS	Thread ID: 1336
2:18:26....	HxTsr.exe	1516	Load Image	C:\Windows\System32\OneCoreUAPCo...	SUCCESS	Image Base: 0x7ffa...
2:18:26....	HxTsr.exe	1516	Load Image	C:\Windows\System32\biwinrt.dll	SUCCESS	Image Base: 0x7ffa...
2:18:26....	HxTsr.exe	1516	Load Image	C:\Windows\System32\Windows.StateR...	SUCCESS	Image Base: 0x7ffa...
2:18:26....	HxTsr.exe	1516	Load Image	C:\Windows\System32\Windows.UI.dll	SUCCESS	Image Base: 0x7ffa...
2:18:26....	HxTsr.exe	1516	Load Image	C:\Windows\System32\TextInputFramew...	SUCCESS	Image Base: 0x7ffa...
2:18:26....	HxTsr.exe	1516	Load Image	C:\Windows\System32\InputHost.dll	SUCCESS	Image Base: 0x7ffa...
2:18:26....	HxTsr.exe	1516	Load Image	C:\Windows\System32\CoreUICompone...	SUCCESS	Image Base: 0x7ffa...
2:18:26....	HxTsr.exe	1516	Load Image	C:\Windows\System32\CoreMessaging....	SUCCESS	Image Base: 0x7ffa...

Showing 95 of 5,002,864 events (0.0018%) Backed by virtual memory

Figure 41 HxTsr loading images and creating threads.

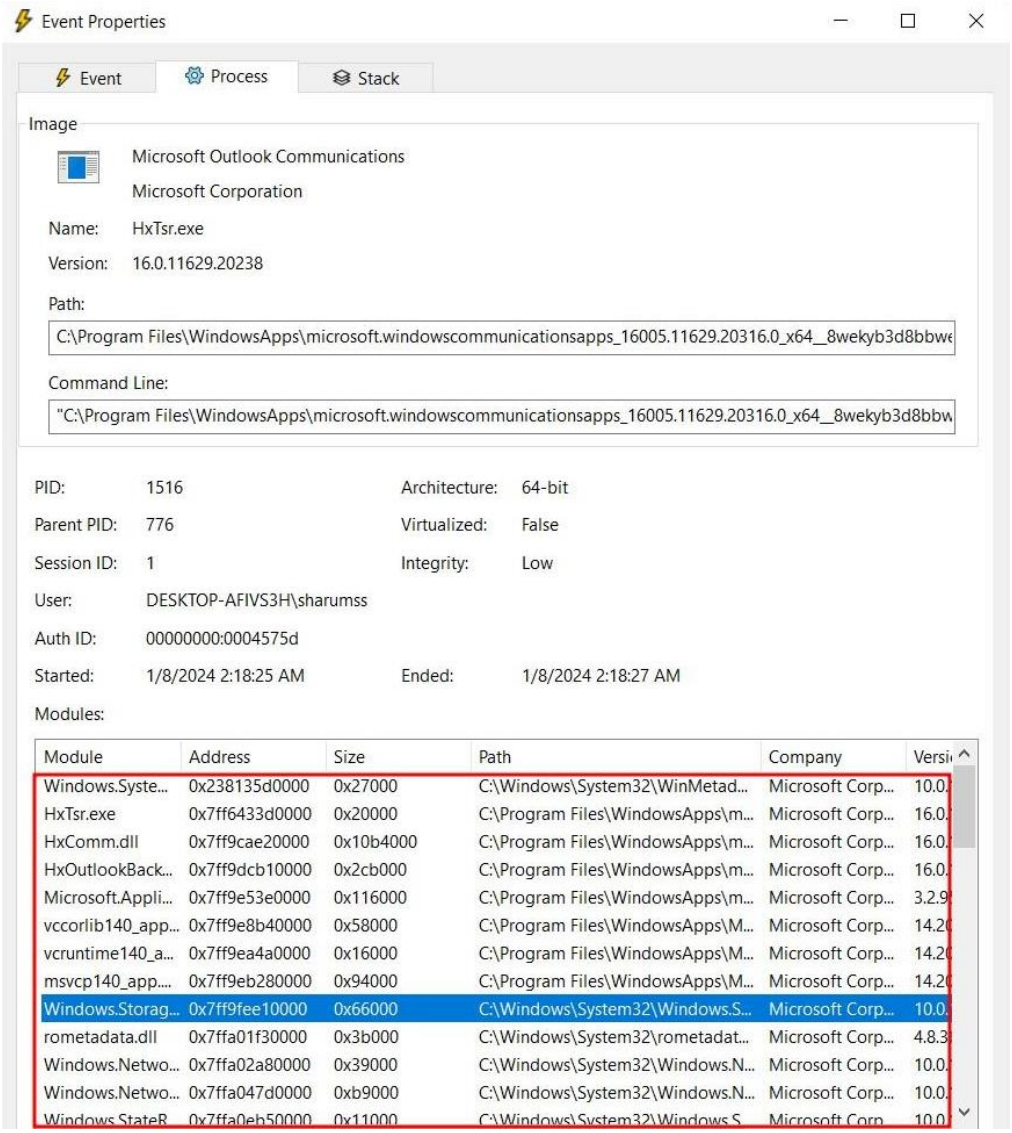


Figure 42 Event Properties of HxTsr

The process ran for only two seconds and ran with “low” integrity and the other process is created right after that, which is very malicious. Also, MS Outlook is not a default application and wasn’t previously installed in the victim’s PC. This process was potentially triggered by another process, like Microsoft.Photos.exe. Malware could have disguised itself as a Microsoft Outlook process to evade detection. The short execution time could be part of a stealthy operation to inject malicious code or perform reconnaissance.

Based on modules it loaded, it could be

- **(HxOutlookBackingStore.dll, Windows.Storage.Server.dll)**
  stealing email messages, contacts, and calendar data from / Accessing files stored in OneDrive/ exfiltrating sensitive data to a remote server.
- **(Windows Network Connectivity Manager, Windows Network Connections)**
  Establishing a backdoor for remote control by the attacker/ Downloading additional malware or tools/ Exfiltrating data over the network
- **(Windows State Repository, romemetadata.dll)**
  Modifying system settings to ensure malware persistence after reboots/ Hiding files or registry entries to evade detection/ Creating scheduled tasks or startup entries to maintain presence.
- **(Windows.Networking.ConnectivityManager, Windows.Networking.Connectivity.dll)**
  Gathering system information (OS version, installed software, network configuration)/Identifying potential vulnerabilities for further exploitation/Mapping the network for valuable targets.
- **HxComm.dll**
  Intercepting and stealing user credentials for email accounts or other services/ Using stolen credentials for lateral movement or data exfiltration

Similarly, other malicious processes were also discovered running suspicious commands.

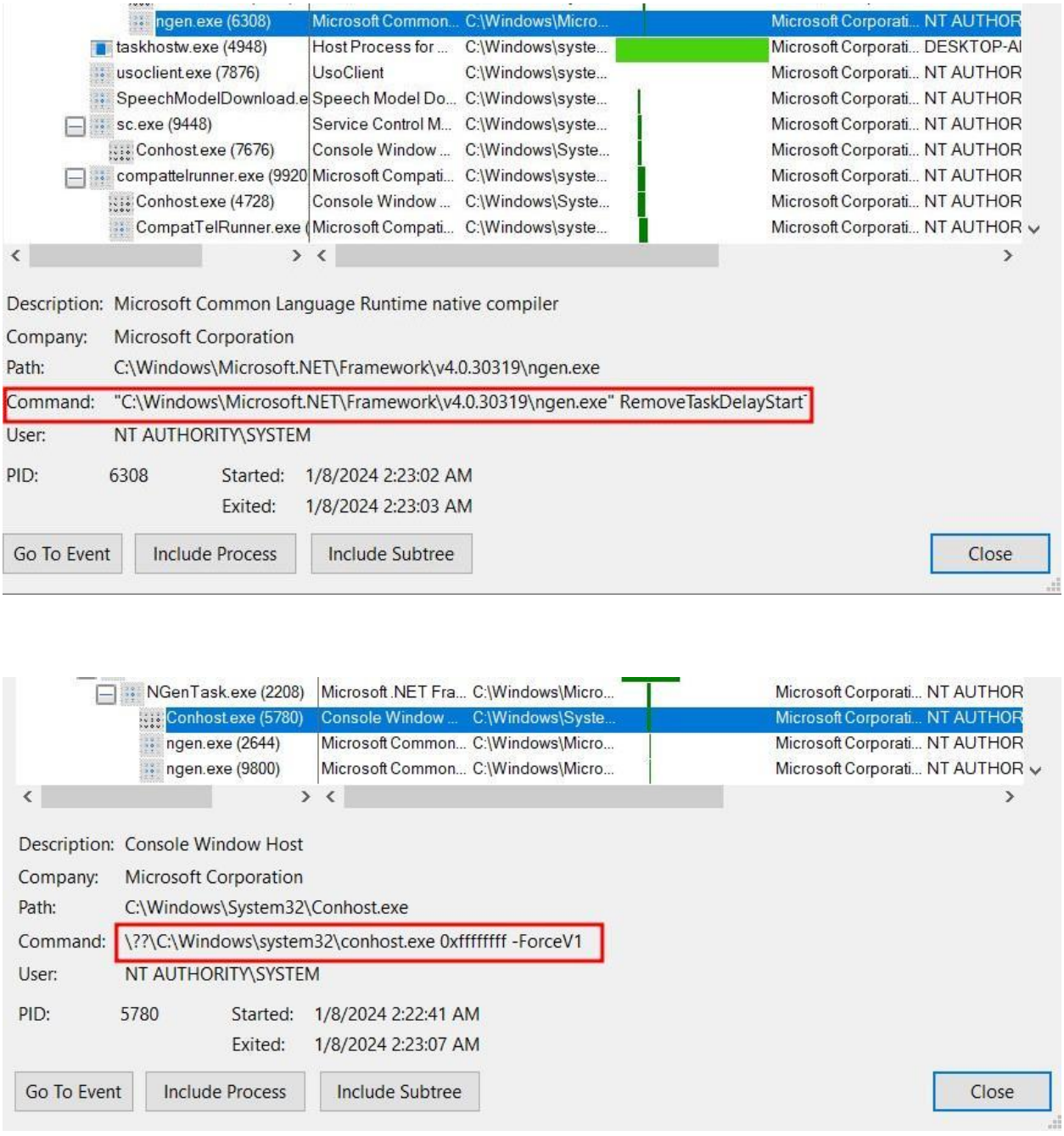


Figure 43 Malicious Process of 'NGenTask.exe'

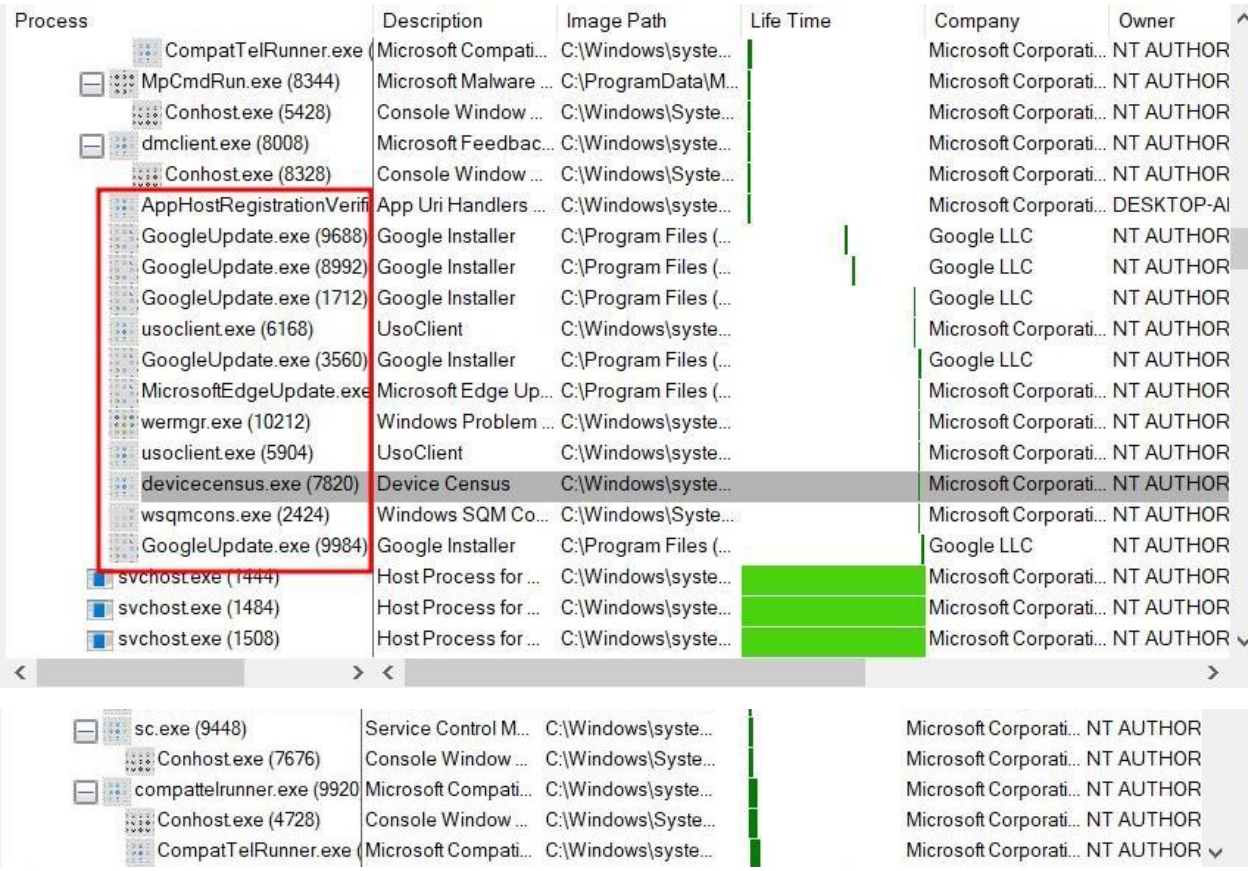


Figure 44 Other Malicious Processes

VirusTotal Checks on other Malicious Processes:

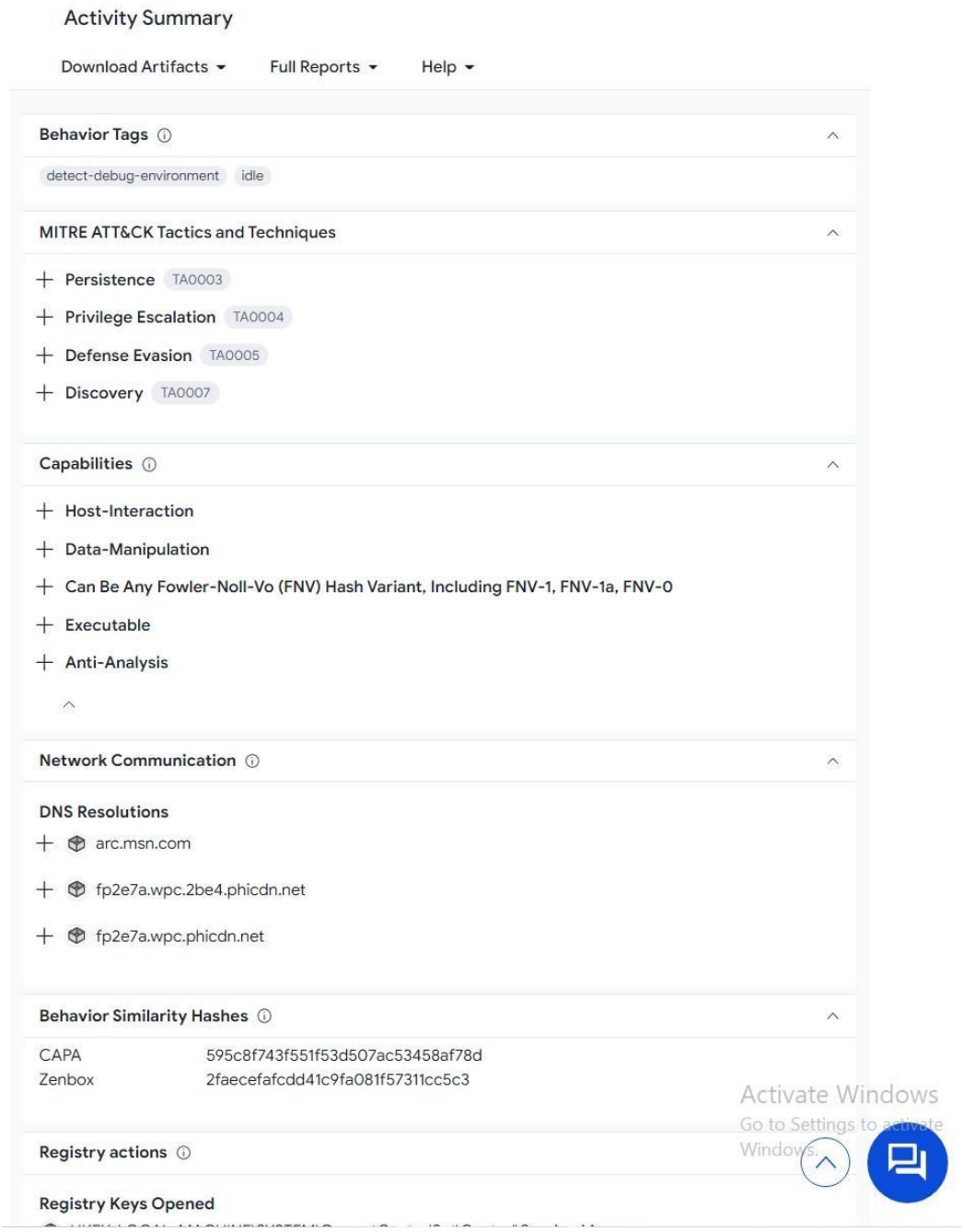


Figure 45 VirusTotal Checks – MpSigStub.exe (Activity Summary)

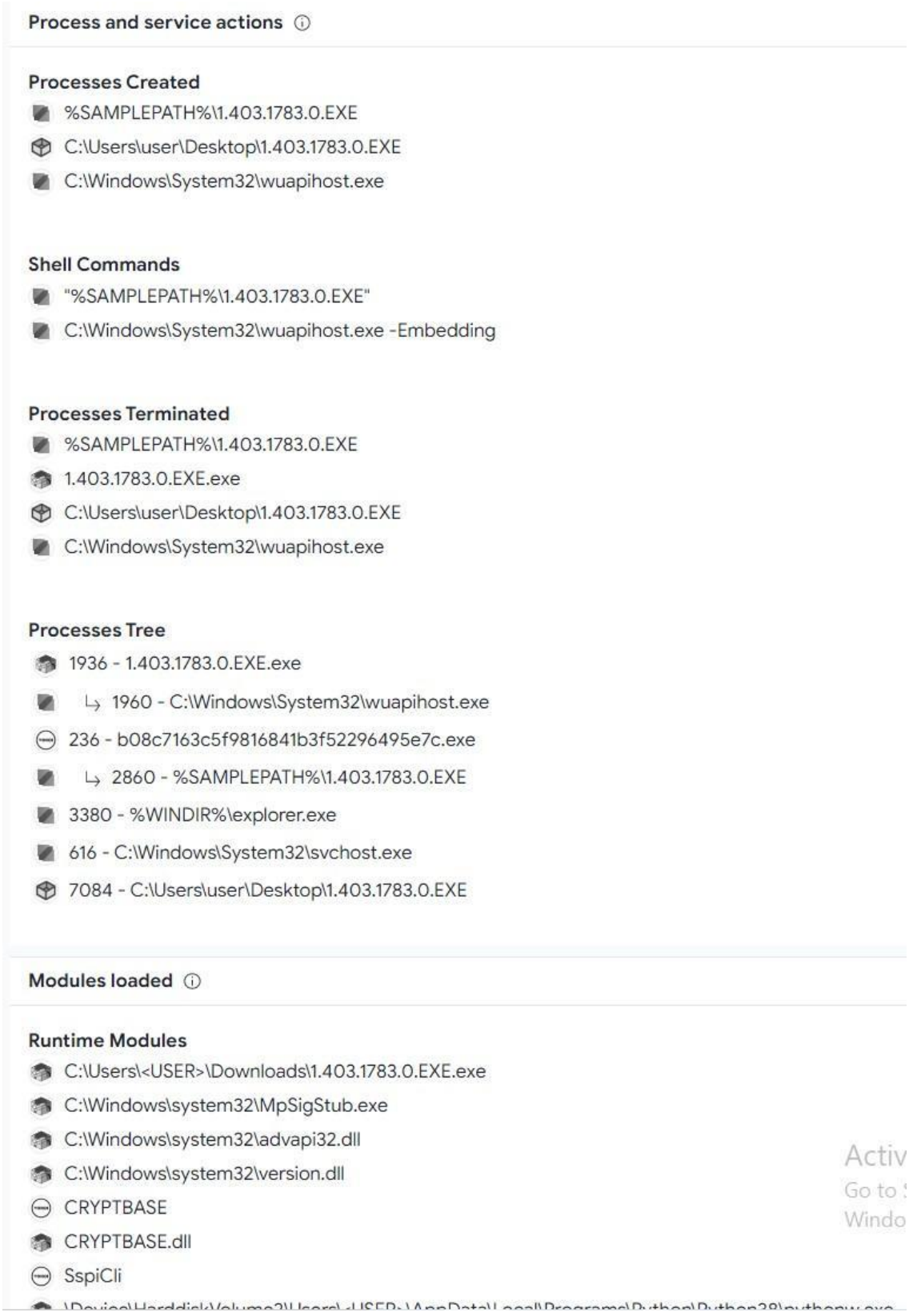


Figure 46 VirusTotal Check - MpSigStub.exe (Processes)

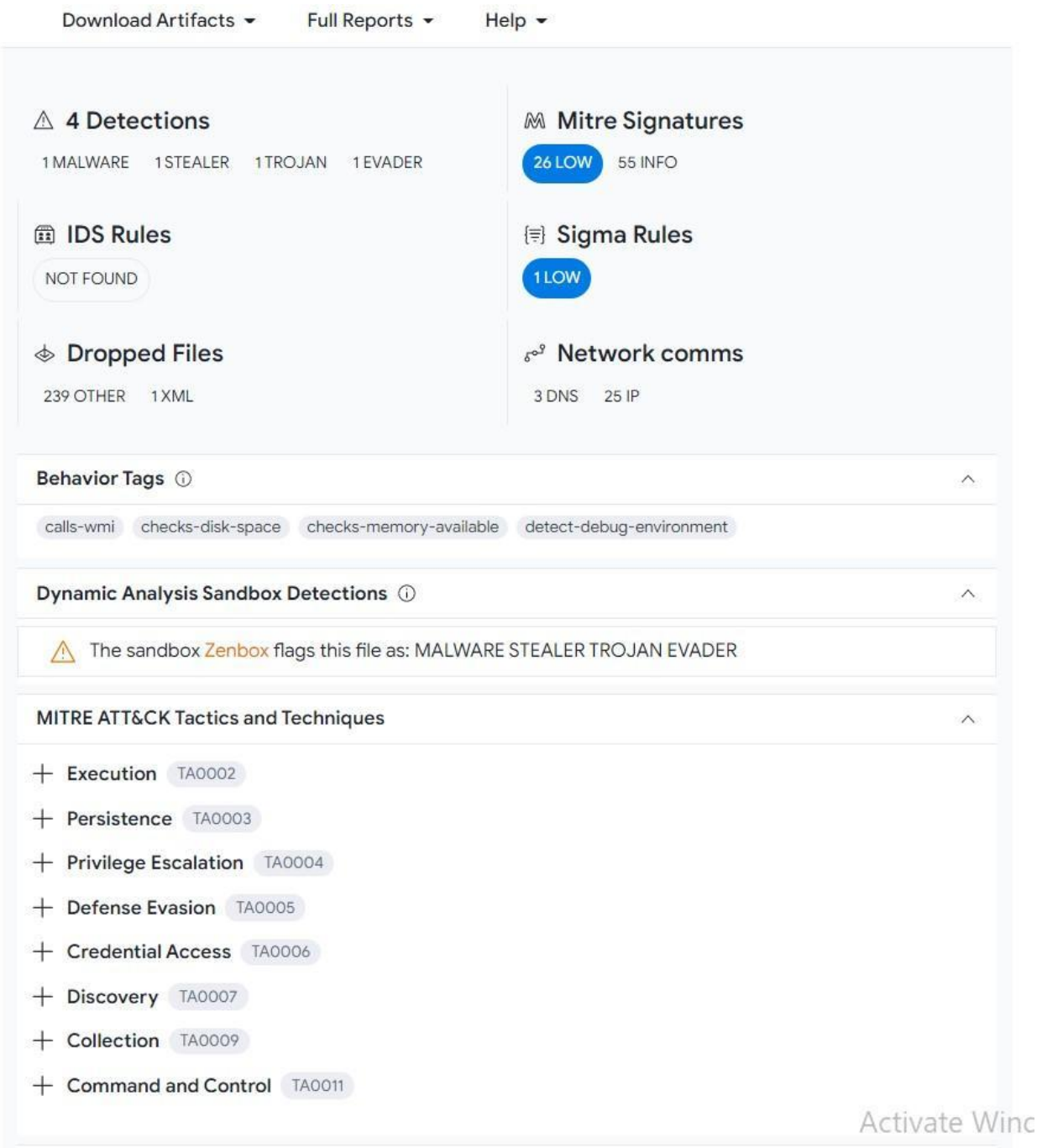


Figure 47 VirusTotal Check - CompaTelRunner.exe (Summary)

login.live.com	1 / 89	1994-12-28	CSC CORPORATE DOMAINS, INC.
query.prod.cms.rt.microsoft.com	0 / 89	1991-05-02	MarkMonitor Inc.

Contacted IP addresses (15)

IP	Detections	Autonomous System	Country
104.90.121.87	0 / 89	16625	US
192.229.211.108	2 / 89	15133	US

Figure 48 VirusTotal Check - CompaTelRunner.exe (Contacted Domains)

Contacted Domains (1)

Domain	Detections	Created	Registrar
query.prod.cms.rt.microsoft.com	0 / 89	1991-05-02	MarkMonitor Inc.

Contacted IP addresses (8)

IP	Detections	Autonomous System	Country
104.86.182.8	1 / 89	20940	US
192.229.211.108	2 / 89	15133	US
20.22.113.133	0 / 89	8075	US
20.99.133.109	3 / 89	8075	US
20.99.185.48	0 / 89	8075	US
20.99.186.246	1 / 89	8075	US
23.198.146.35	0 / 89	16625	US
23.216.147.76	2 / 89	20940	US

Execution Parents (23.8 K)

Scanned	Detections	Type	Name
2023-12-15	54 / 72	Win32 EXE	w64.exe
2024-01-04	49 / 68	Win32 EXE	wininst-14.0.exe
2023-12-17	53 / 72	Win32 EXE	armsvc.exe
2023-12-31	54 / 74	Win32 EXE	mscorsvw.exe
2024-01-07	0 / 69	Win32 EXE	Google Update Setup
2023-12-31	48 / 70	Win32 EXE	Wextract
2023-12-25	55 / 72	Win32 EXE	Aut2Exe.exe
2023-12-30	55 / 74	Win32 EXE	Zoom Installer
2023-12-27	48 / 72	Win32 EXE	llvm-symbolizer
2023-12-30	56 / 72	Win32 EXE	armsvc.exe

Figure 49 VirusTotal Check - wsqmcons.exe (Contacted Domains and Execution Parents)

Figure 50 VirusTotal Check - devicecensus.exe (Crowdsourced Context)

Execution Parents (23.8 K)

Scanned	Detections	Type	Name
2023-12-15	54 / 72	Win32 EXE	w64.exe
2024-01-04	49 / 68	Win32 EXE	wininst-14.0.exe
2023-12-17	53 / 72	Win32 EXE	armsvc.exe
2023-12-31	54 / 74	Win32 EXE	mscorsvw.exe
2024-01-07	0 / 69	Win32 EXE	Google Update Setup
2023-12-31	48 / 70	Win32 EXE	Wextract
2023-12-25	55 / 72	Win32 EXE	Aut2Exe.exe
2023-12-30	55 / 74	Win32 EXE	Zoom Installer
2023-12-27	48 / 72	Win32 EXE	llvm-symbolizer
2023-12-30	56 / 72	Win32 EXE	armsvc.exe
2023-12-23	52 / 71	Win32 EXE	Aut2Exe.exe
2024-01-02	48 / 72	Win32 EXE	wininst-14.0-amd64.exe
2023-12-28	53 / 72	Win32 EXE	Java(TM) Web Start Launcher
2023-12-29	54 / 72	Win32 EXE	Java(TM) Web Start Launcher
2024-01-01	49 / 70	Win32 EXE	armsvc.exe
2023-12-17	53 / 72	Win32 EXE	chrome_pwa_launcher
2023-12-27	54 / 72	Win32 EXE	Java(TM) Web Start Launcher
2023-12-26	55 / 72	Win32 EXE	mscorsvw.exe
2023-12-27	55 / 72	Win32 EXE	LogTransport2
2023-12-14	49 / 70	Win32 EXE	mscorsvw.exe

Figure 51 VirusTotal Check - devicecensus.exe (Execution Parents)

9.4.1.2 Network Analysis

Looking at the network activity, it can be seen making requests to fetch client metadata.

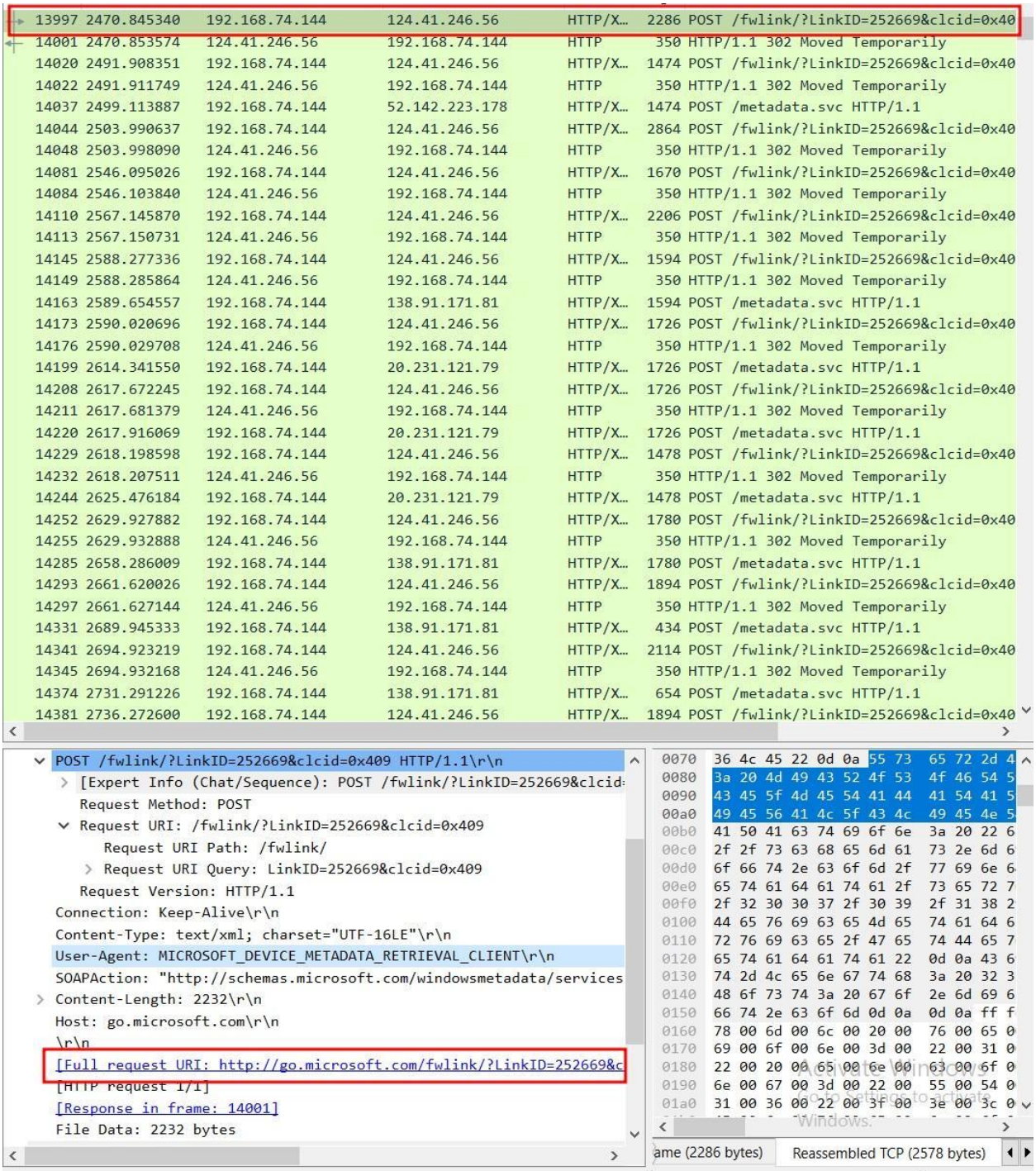


Figure 52 Request to fetch client metadata.

Also, it can be seen making request for the status of a certificate with the serial number MFEwTzBNMESwSTAJBgUrDgMCGgUABBQ500tx.

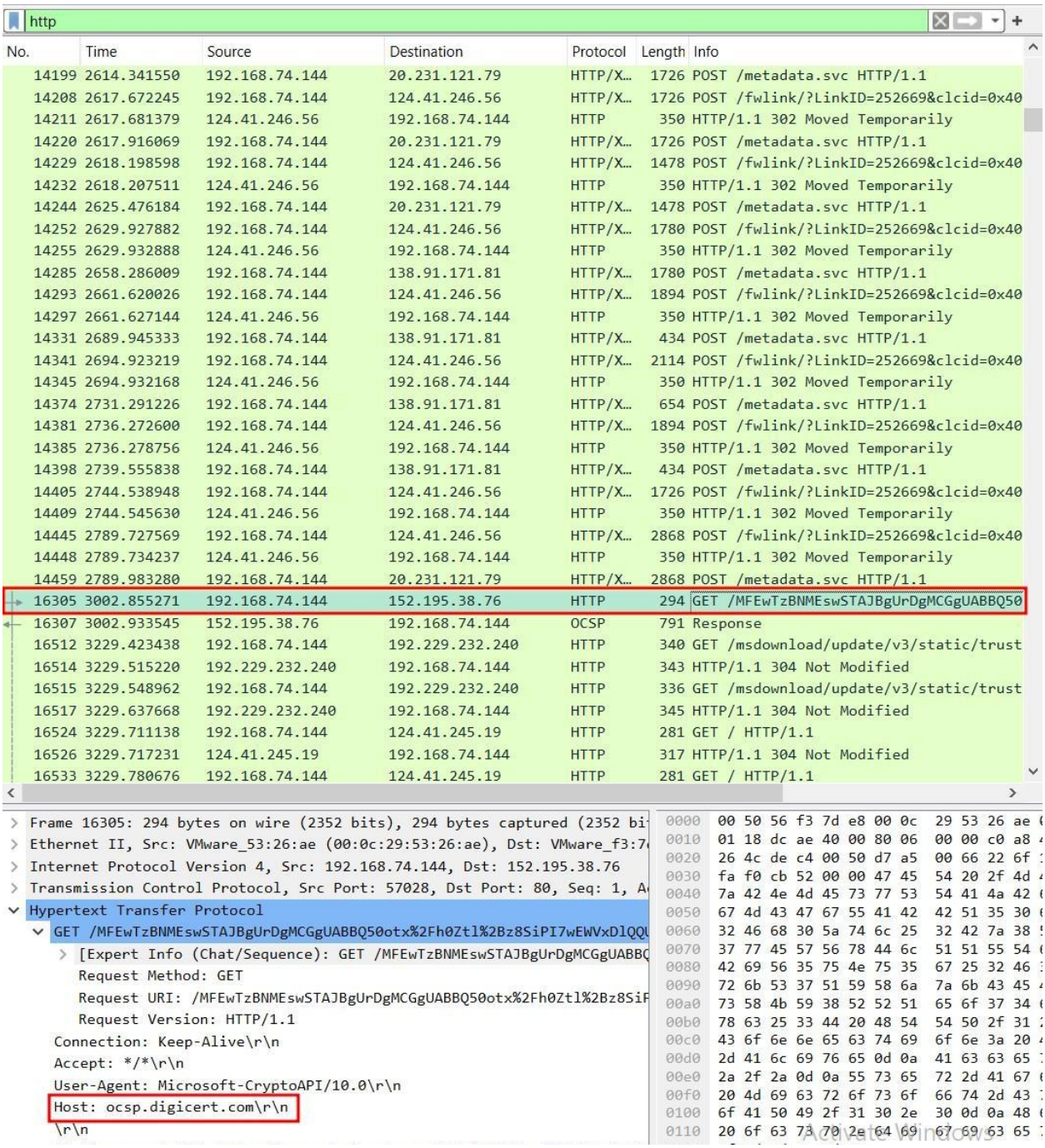


Figure 53 Making request for certificate validation.

It also makes request for a file named "disallowedcertstl.cab" located on the Windows Update server. This file likely contains a list of revoked or untrusted certificates.

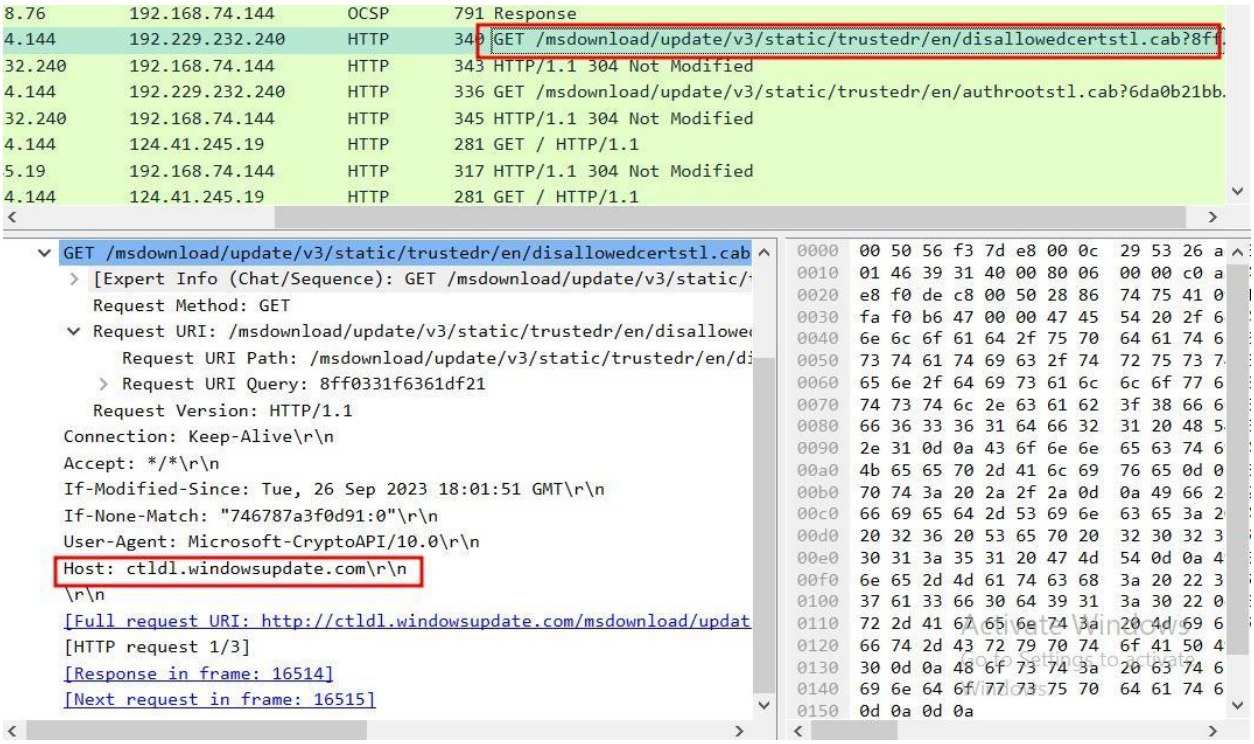


Figure 54 Malware checking for disallowed certificates.

HTTP GET request for a resource called /en-US/livetile/preinstall on the server "tile-service.weather.microsoft.com". The request includes parameters specifying the region ("US") and app ID ("C98EA5B0842DBB9405BBF07").

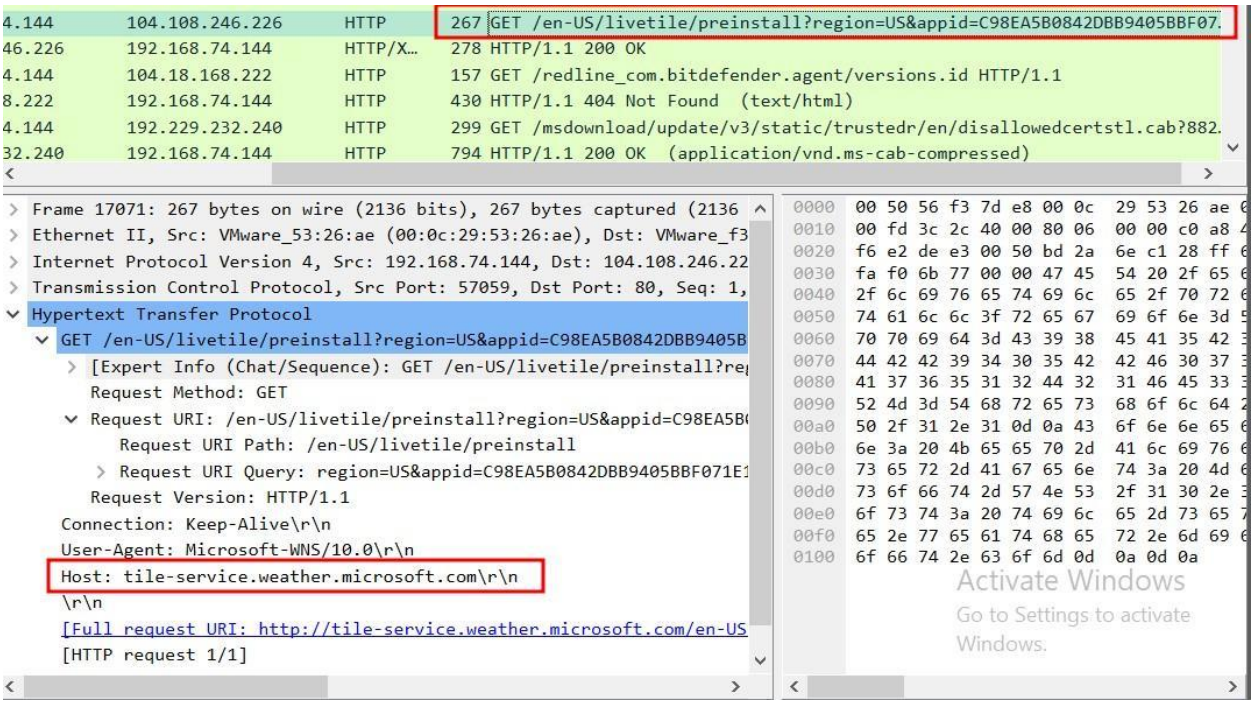


Figure 55 Suspicious HTTP request

After that, it can be seen that the Windows Update Agent on the machine is trying to download a file named "40462833_b065241af2f8fa25e" as part of the Windows Update process. However, the server redirects the client to another file named "40461964_5f72c1e3e80aa4c8a1387" instead.

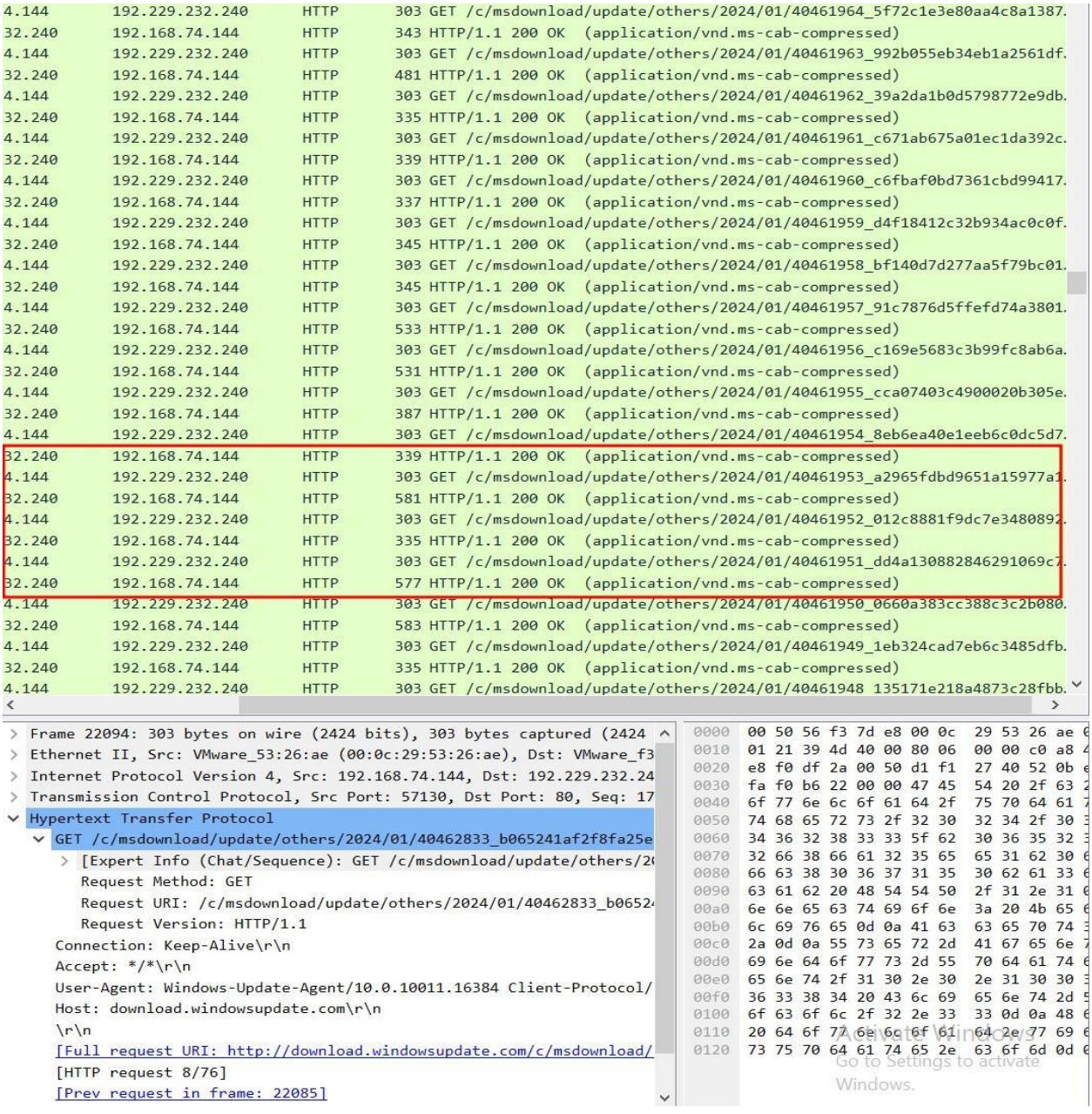
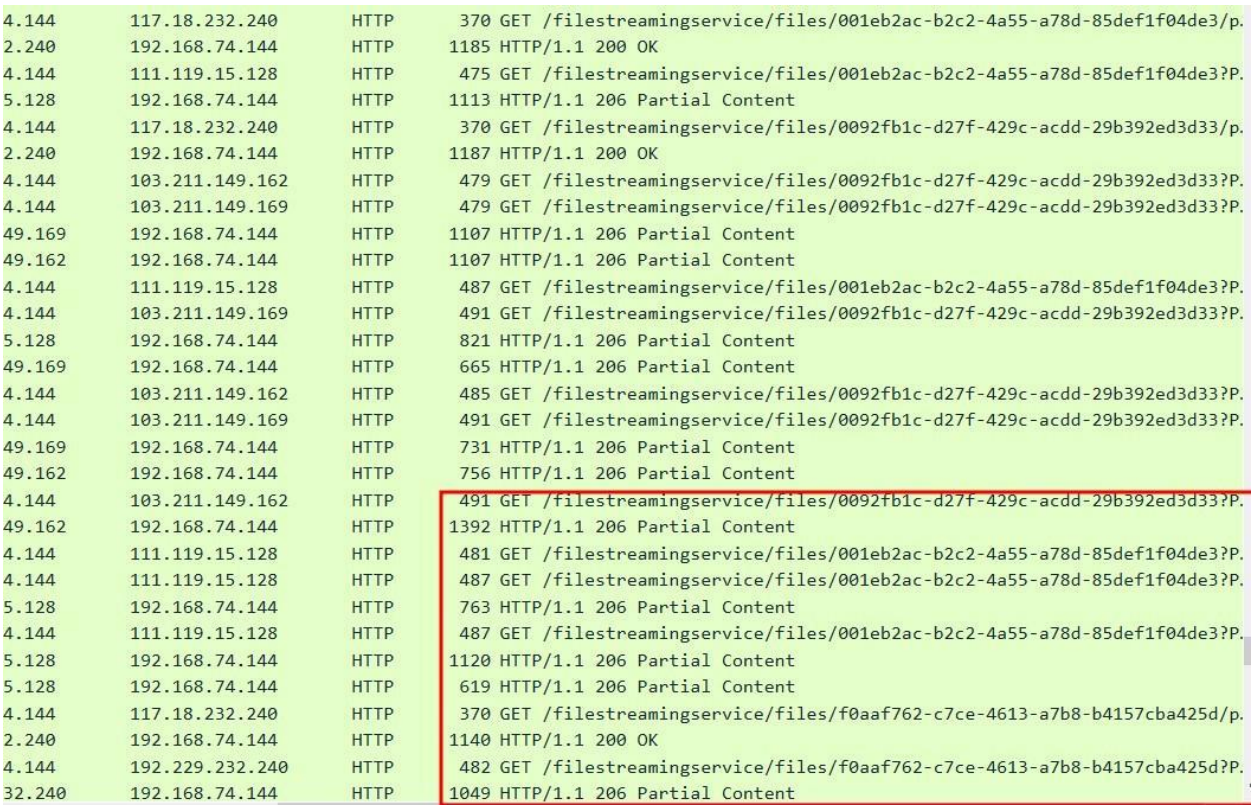


Figure 56 Redirected HTTP request.

After that it can be seen making request to suspicious server, on which running virustotal checks gave no leads and downloading multiple files.



4.144	117.18.232.240	HTTP	370	GET /filestreamingservice/files/001eb2ac-b2c2-4a55-a78d-85def1f04de3/p.
2.240	192.168.74.144	HTTP	1185	HTTP/1.1 200 OK
4.144	111.119.15.128	HTTP	475	GET /filestreamingservice/files/001eb2ac-b2c2-4a55-a78d-85def1f04de3?P.
5.128	192.168.74.144	HTTP	1113	HTTP/1.1 206 Partial Content
4.144	117.18.232.240	HTTP	370	GET /filestreamingservice/files/0092fb1c-d27f-429c-acdd-29b392ed3d33/p.
2.240	192.168.74.144	HTTP	1187	HTTP/1.1 200 OK
4.144	103.211.149.162	HTTP	479	GET /filestreamingservice/files/0092fb1c-d27f-429c-acdd-29b392ed3d33?P.
4.144	103.211.149.169	HTTP	479	GET /filestreamingservice/files/0092fb1c-d27f-429c-acdd-29b392ed3d33?P.
49.169	192.168.74.144	HTTP	1107	HTTP/1.1 206 Partial Content
49.162	192.168.74.144	HTTP	1107	HTTP/1.1 206 Partial Content
4.144	111.119.15.128	HTTP	487	GET /filestreamingservice/files/001eb2ac-b2c2-4a55-a78d-85def1f04de3?P.
4.144	103.211.149.169	HTTP	491	GET /filestreamingservice/files/0092fb1c-d27f-429c-acdd-29b392ed3d33?P.
5.128	192.168.74.144	HTTP	821	HTTP/1.1 206 Partial Content
49.169	192.168.74.144	HTTP	665	HTTP/1.1 206 Partial Content
4.144	103.211.149.162	HTTP	485	GET /filestreamingservice/files/0092fb1c-d27f-429c-acdd-29b392ed3d33?P.
4.144	103.211.149.169	HTTP	491	GET /filestreamingservice/files/0092fb1c-d27f-429c-acdd-29b392ed3d33?P.
49.169	192.168.74.144	HTTP	731	HTTP/1.1 206 Partial Content
49.162	192.168.74.144	HTTP	756	HTTP/1.1 206 Partial Content
4.144	103.211.149.162	HTTP	491	GET /filestreamingservice/files/0092fb1c-d27f-429c-acdd-29b392ed3d33?P.
49.162	192.168.74.144	HTTP	1392	HTTP/1.1 206 Partial Content
4.144	111.119.15.128	HTTP	481	GET /filestreamingservice/files/001eb2ac-b2c2-4a55-a78d-85def1f04de3?P.
4.144	111.119.15.128	HTTP	487	GET /filestreamingservice/files/001eb2ac-b2c2-4a55-a78d-85def1f04de3?P.
5.128	192.168.74.144	HTTP	763	HTTP/1.1 206 Partial Content
4.144	111.119.15.128	HTTP	487	GET /filestreamingservice/files/001eb2ac-b2c2-4a55-a78d-85def1f04de3?P.
5.128	192.168.74.144	HTTP	1120	HTTP/1.1 206 Partial Content
5.128	192.168.74.144	HTTP	619	HTTP/1.1 206 Partial Content
4.144	117.18.232.240	HTTP	370	GET /filestreamingservice/files/f0aaf762-c7ce-4613-a7b8-b4157cba425d/p.
2.240	192.168.74.144	HTTP	1140	HTTP/1.1 200 OK
4.144	192.229.232.240	HTTP	482	GET /filestreamingservice/files/f0aaf762-c7ce-4613-a7b8-b4157cba425d?P.
32.240	192.168.74.144	HTTP	1049	HTTP/1.1 206 Partial Content

Figure 57 Requests to unknown server

The request is wrapped in a custom TCP payload that appears obfuscated or encrypted, suggesting an attempt to bypass security measures that might be based on traditional HTTP traffic inspection and attempting to hide their activities from network security measures.

Back to Report

9.5 Appendix 5: Preventive Measures/ Recommendation

- **Secure Browsing Habits:**

  Use secure, encrypted connections (HTTPS) when browsing untrusted or suspicious websites, especially those offering pirated software or illegal content.

- **Network Segmentation:**

  Network segmentation can help contain malware's impact and prevent its spread across the network by restricting lateral movement in case of a successful infection.

- **Behavioural Analysis and Anomaly Detection:**

  Implement security solutions that utilize behavioural analysis and anomaly detection to detect and block suspicious activities, even if they don't match known malware signatures.

- **Access Controls and Least Privilege Principle:**

  Regularly review and update user access permissions to minimize the risk of unauthorized access and ensure job functions are properly performed.

- **Regular Backups:**

  Regularly back up critical data and store them securely to prevent malware infection and ensure system restoration without significant data loss.

- **Disable Unnecessary Services:**

  Disable unnecessary services and protocols on systems to reduce the attack surface.

- **Incident Response Plan:**

  Develop and update an incident response plan to effectively handle malware infections, including system isolation, stakeholder communication, and service restoration (Avast, 2024), (Baker, 2023), (Fortra's Digital Defense, 2024), (Proofpoint, 2024).

Back to Report