Triaging Windows Event Logs for Ransomware Investigations

GIAC (GCIH) Gold Certification

Author: Perumal P S, perumal316@gmail.com
Advisor: Hamed Khiabani, Ph.D.
Accepted: June 12th 2022

Abstract

Ransomware attacks on organizations will disrupt their day-to-day operations causing significant inconvenience, especially if they provide critical services to the people. With the increasing number of ransomware attacks, it is of paramount importance to identify the ransomware characteristics during the preliminary investigation stage. This is critical in a heavily networked infrastructure where if the ransomware has been detected in one system, it could still spread to other systems in the network or continue residing in them. This has to be done in a fast and timely manner to prevent the spread or other similar attacks. Using the newest operating system, Windows 11 with its inbuilt Microsoft Defender Anti-Virus, 37 ransomware variants from the different families were tested. Windows Events logs generated and forwarded to a centralized log server were analyzed for logs generated during detection, removal or successful execution or other characteristics. In summary 28 out of 37 variants were detected by the Microsoft Defender and generated event logs with Event ID 1116 and 1117 containing critical information like signature name, path, detection name, and user. The remaining 9 variants were undetected and generated logs with Event ID 1, 1000 or 1109 where it either crashed (1 variant), could not run due to compatibility issues (4 variants), memory issue (1 variant), or executed and encrypted files successfully (3 variants). This is useful for forensics investigators during the triage period to focus on these event logs to get the necessary information to track down the origin and path of ransomware and also scanning the network where the ransomware could still be residing in other devices that may have failed execution. The info would also aid in the post-investigation phase where the necessary teams like Security Information and Event Management (SIEM) teams to get more information about the ransomware and build different use cases for early detection and prevention by the Security Operations Centers (SOCs).

1. Introduction

Close to 37% of organizations globally have been affected by ransomware in 2021 (Kerner, n.d.). Ransomware attacks could cause havoc in an organization as it could bring their operations to their knees if important files key to their day-to-day operations were rendered useless. To recover, organizations may choose to pay the ransom. These are business side decisions, but as an incident responder, it is essential at the triage level to isolate the key events that led to the attack to stop the spread of ransomware in the network if necessary and also to prevent it from being repeated.

In an organization with numerous computers deployed, most would have established a log forwarding mechanism to collect logs in a centralized server. Some may have dedicated personnel using log visualization software like Splunk to view the logs. In the event of a ransomware attack, incident responders at the triage stage could leverage on the collected logs to find key indicators of the ransomware and their characteristics. If a common ransomware like RAAS (ransomware-as-a-service) or attacker reusing code from a popular ransomware is being used there is even a possibility of the decryption software already being available thus eliminating the need to pay the ransom. But more importantly, the triage information can be used to prevent the spread of the ransomware which could be dormant in some computers or could have failed in the execution but still reside within the network.

This paper explores the common event logs generated by ransomware by executing actual ransomware samples on virtual machines mimicking an enterprise setup where there is a log forwarding setup and logs are being forwarded to a log server. By mapping the common event logs, it will help incident responders for their triage investigation into ransomware incidents.

2. Ransomware

2.1. Ransomware Attacks

Ransomware is a type of malware (Checkpoint, n.d.) designed to cause inconvenience to an organization by preventing them from continuing their day-to-day operation. This can

be achieved by either blocking access to their system or encrypting their files (Kaspersky, n.d.). In order to access their systems or decrypt the files, the organization would then have to pay a ransom to the perpetrators.

2.2. Types of Ransomware

As mentioned above, there are a few types of ransomware that can be used to achieve the purpose of getting ransom payments. The 2 main types are Crypto ransomware and Locker's ransomware. This causes actual damage to the system and affects the organizations directly. There are also other types like Scareware or Doxware that, without damaging the files, just flood the screen with pop-ups or threatening police-themed messages (Crowdstrike, 2021) to solicit payments.

2.2.1. Crypto Ransomware

For this paper, the focus is on Crypto ransomware. This type encrypts the key files within a system, thus making it unusable to the organization or user. If essential files like PDFs, Office documents, or database files are encrypted, then an organization or an individual may not be able to continue their day-to-day activities. It may be even more devastating if it leads to financial loss. To regain back the files, a decryptor or decryption key is required which can be obtained by paying the perpetrator in bitcoins thus the name Crypto ransomware. For this paper ransomware samples were downloaded from vx-underground, a popular website that hosts malware samples. Ransomware samples are also part of their database and various samples can be found in their website (vx-underground, n.d.). A total of 37 ransomware variants from the different families were downloaded. As there were multiple versions, the latest version is downloaded. If there are multiple latest versions, then the biggest size version was downloaded. The list is as below:

N/o	Ransomware Used	N/o	Ransomware Used
1	AvosLocker	21	LorenzRansomware
2	BandarChorRansomware	22	MagniberRansomware
3	BlackBastaRansomware	23	MementoRansomware
4	BlackCatRansomware	24	MidasRansomware

Perumal P S, perumal316@gmail.com

5	CerberRansomware	25	NightSkyRansomware
6	ClownicRansomware	26	NokoyawaRansomware
7	CubaRansomware	27	OnyxRansomware
8	CuratorRansomware	28	PandoraRansomware
9	DeadBoltRansomware	29	PhobosRansomware
10	DearCryRansomware	30	RansomExx
11	DecafRansomware	31	RookRansomware
12	DiavolRansomware	32	SFileRansomware
13	EvilNominatusRansomware	33	SamsamRansomware
14	HaronRansomware	34	SugarRansomware
15	HiveRansomware	35	SynAckRansomware
16	KoxicRansomware	36	WhiteRabbitRansomware
17	KrusRansomware	37	YanluowangRansomware
18	LockBitRansomware		
19	LockyRansomware		
20	LokiLockerRansomware		

3. Windows Event Logs

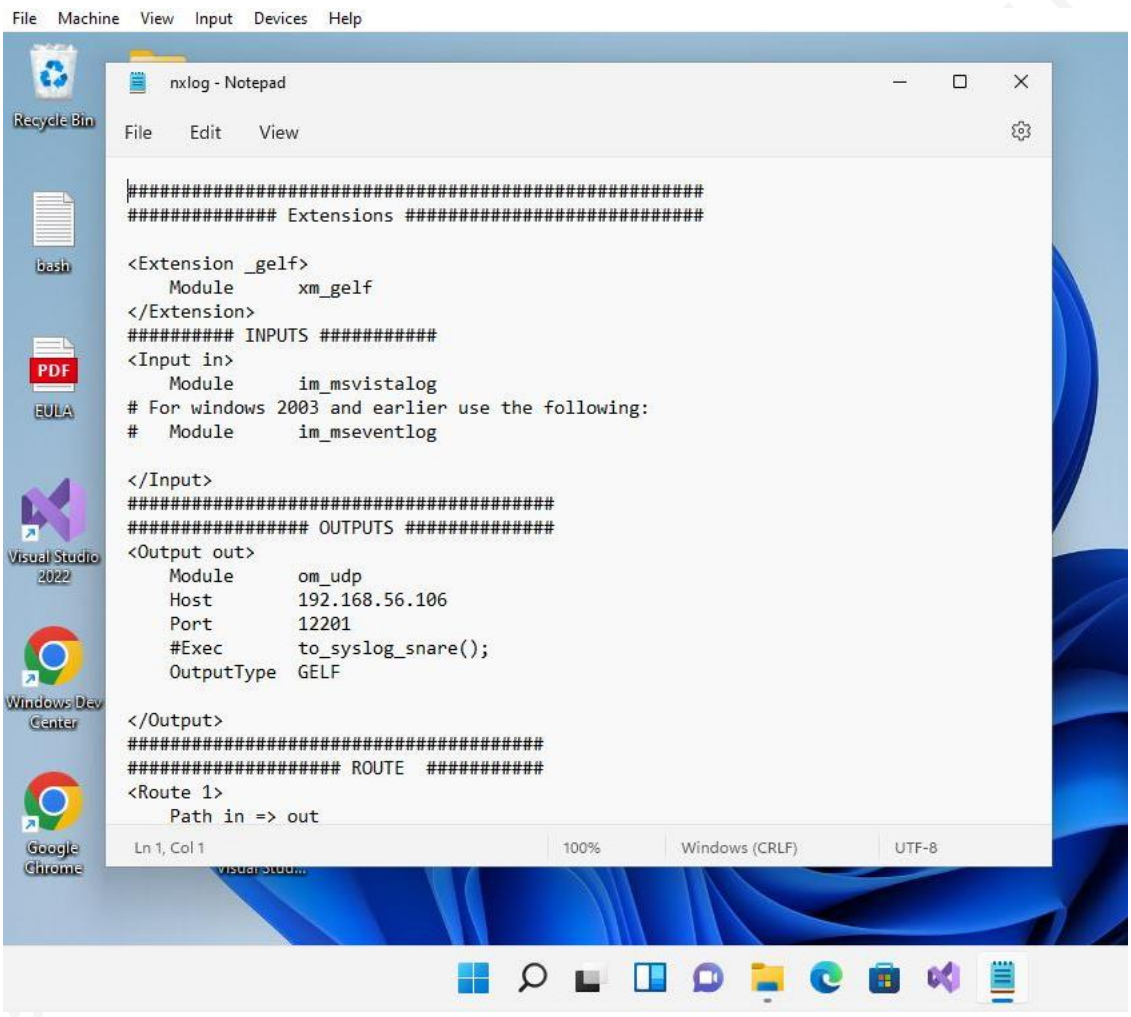
3.1. Windows Event Logs Forwarding

Windows Event logs are a comprehensive record of system, security, and application (Gillis, 2018) logs generated by the Windows Operating Systems or the applications running. In the event of forensic investigations, these logs can provide investigators with the necessary details like applications involved, login timestamps for users, and system events of interest (Fortuna, 2017) for analysis.

In the event of a ransomware attack, the system may become unstable thus making viewing of Windows Event Logs through the Event Viewer application infeasible. Thus, Windows Event Logs forwarder was set up to collect the Event Logs. SIEM (Security Information and Event Management) solutions are a popular choice for organizations (IBM, n.d.) for automated real-time data collection of logs for analysis and compliance from their various endpoints.

For this paper, GrayLog was used to collect the Windows Event Logs generated by the test machine. GrayLog server was set up on a Ubuntu 20.04.4 virtual machine. Further prerequisites like MongoDB and Elasticsearch were also installed and configured following instructions found online (Waderni, 2017). Subsequently, the GrayLog web interface can be accessed at http://127.0.0.1:9000. See Annex C for the GrayLog server login interface.

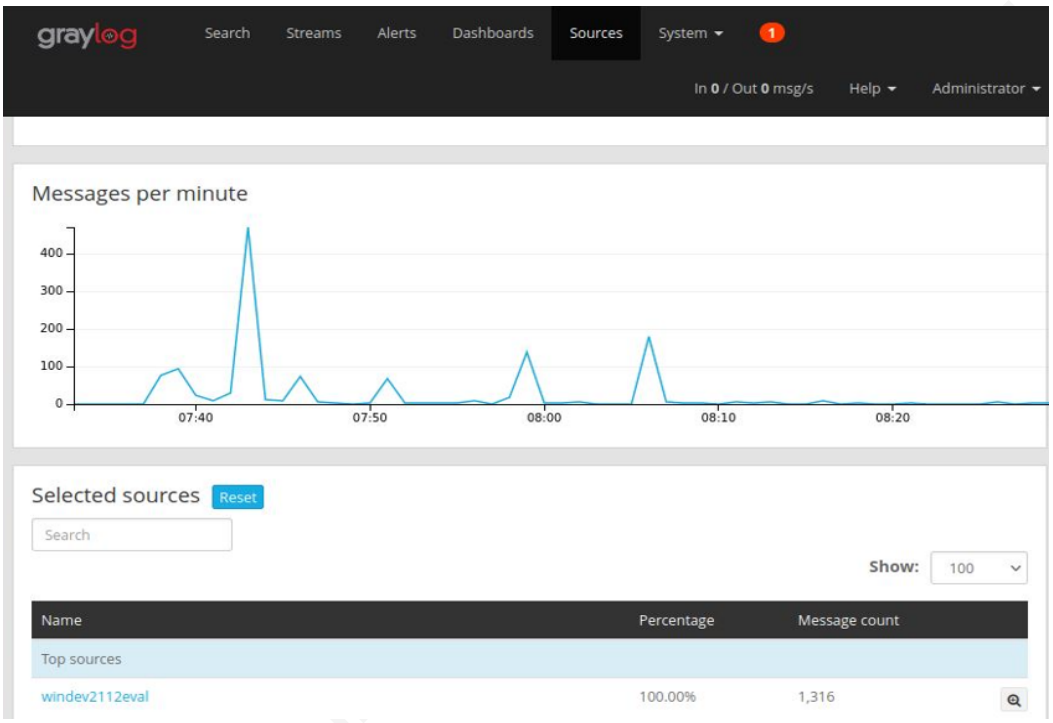
For the test machine that is the client, a Windows 11 Enterprise VM was downloaded from Microsoft's developer website (Microsoft, n.d.) used together with NXLog. It is an open-source log collection tool that is used as a log collector agent installed on the test machine. Below is the screenshot showing the nxlog agent configured to call back to the Graylog server. The im_msvistalog module reads all events from the local Windows Event Logs (Nxlog, n.d.).



Windows 11 Enterprise VM with NXLog agent configured

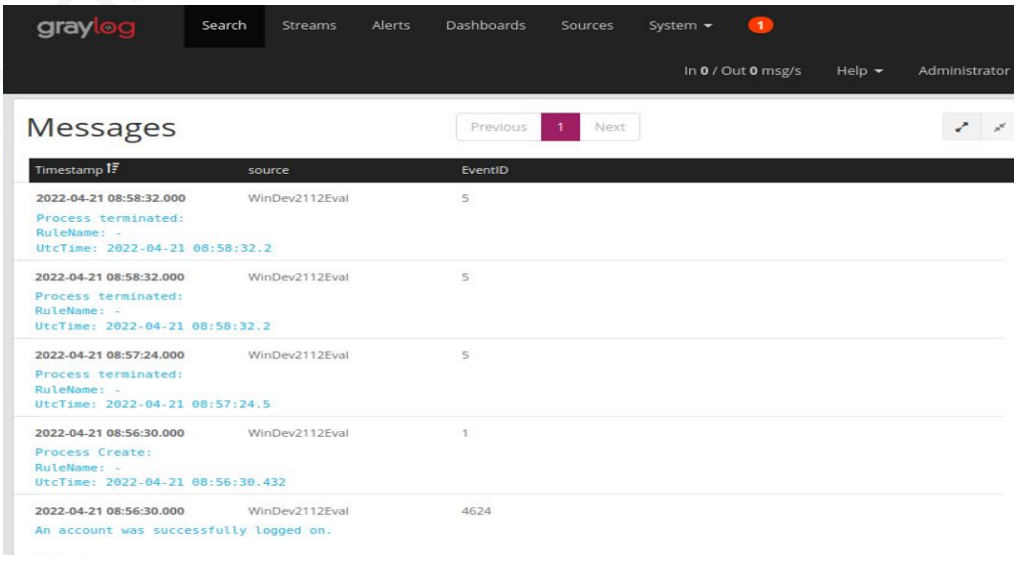
Below are the screenshots showing the callback from the Windows 11 VM back to the GrayLog server.

Perumal P S, perumal316@gmail.com



Windows 11 VM Callback

Individual event IDs and details can also be seen by choosing individual messages.



Individual Message with the Event ID and details

Perumal P S, perumal316@gmail.com

4. Scope

The scope of this paper is to focus on Windows Event logs generated when a ransomware was being executed. Microsoft Defender which is the default security software in Windows operating system is used as the Anti-Virus (AV) solution. There are numerous Anti-Virus solutions in the market, and Microsoft Defender is one of the prominent ones that comes together with the operating systems like Windows 10 and Windows 11. There has been increasing adoption of Microsoft Defender in enterprise environments where over 50% of Windows 10 devices are using it (Anderson, 2018).

Windows 11 is used to mimic an enterprise terminal as it is the newest operating system from Microsoft. Windows has a global market share of close to 75% (Statista, 2022) and enterprises adoption rate of Windows 11 is increasing with most estimated to go onboard by 2023 (Mearian, 2021). Annex C contains the screenshots showing the versions of Windows 11 and Microsoft Defender used for the testing. The default setting for the in-built Windows Exploit Protection was used together with the real-time protection in Microsoft Defender turned on. See Annex C for the screenshots.

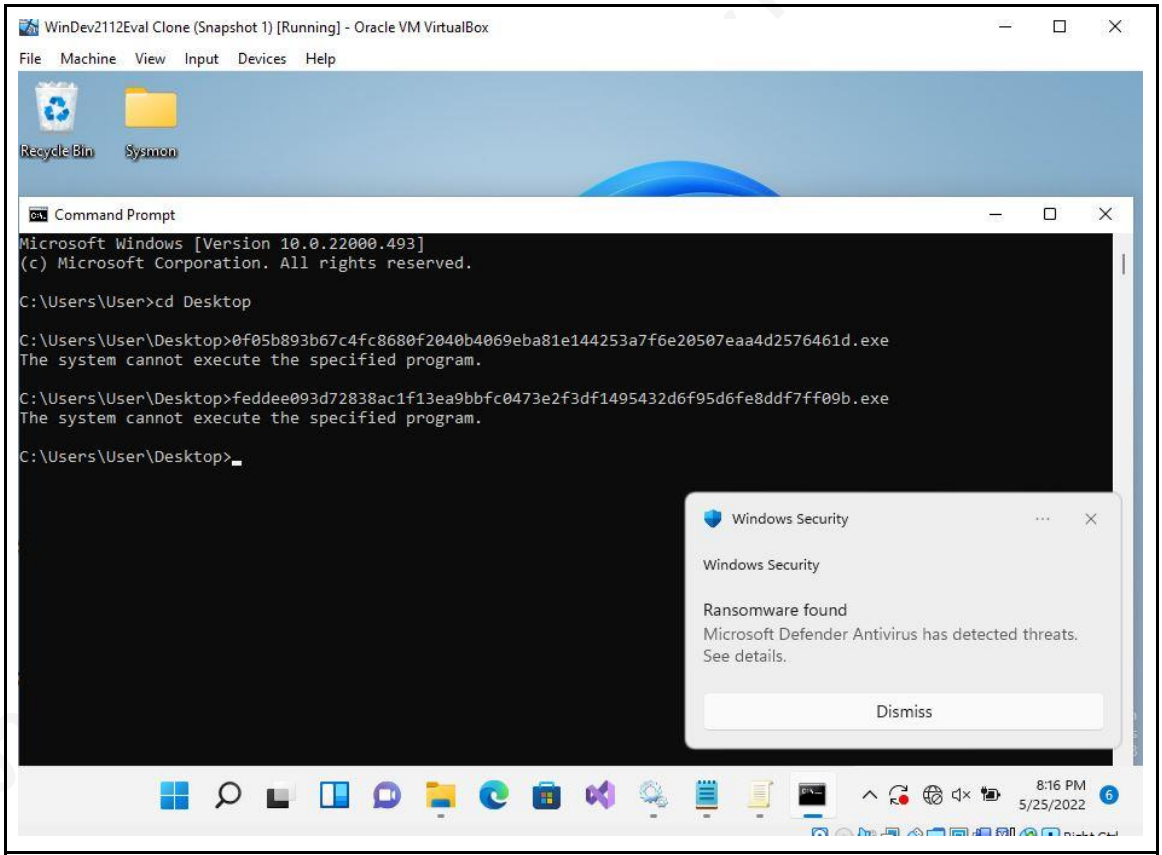
The testing follows the steps listed below:

1. Ransomware extracted and executed (through cmd: <name>.exe) on Windows 11 VM.
2. Take note of the behavior. Detected and removed by Defender? Files encrypted?
3. Take note of event logs forwarded to Graylog server.
4. Revert Windows 11 VM (using Snapshot taken before execution) if ransomware was successfully executed.
5. Repeat for all the 37 ransomware samples.

5. Findings

By following the five steps in the testing methodology as described above, five main occurrences were observed.

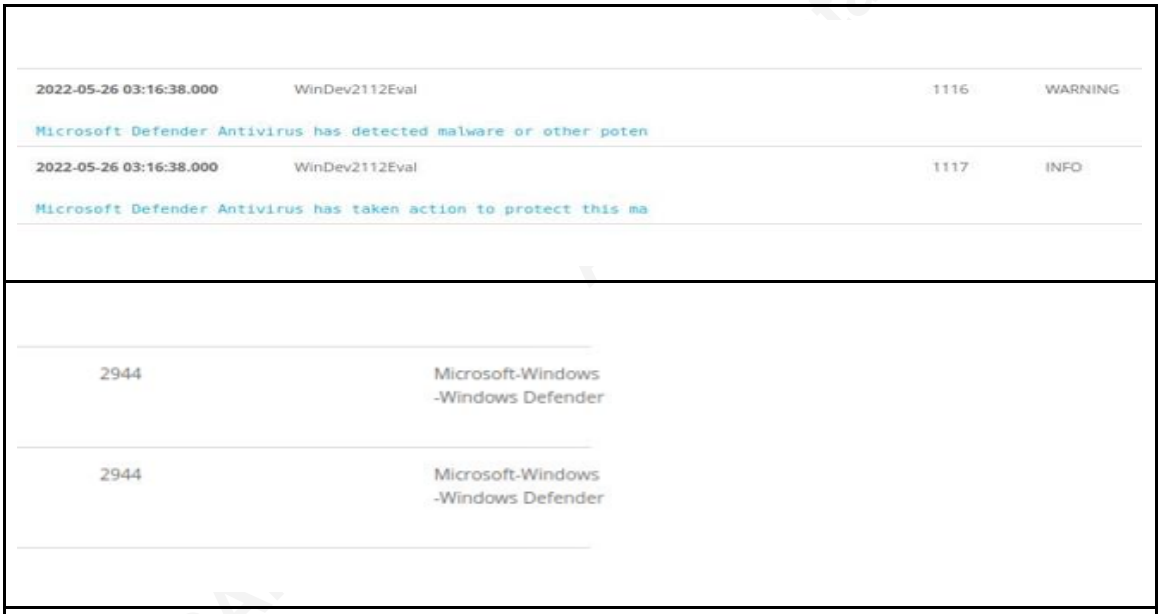
The first is Microsoft Defender successfully detects the ransomware and removes it from the system like shown in the screenshot below.



Microsoft Defender prompting that "Ransomware Found"

Two main Windows Event Logs were generated for this occurrence. Event ID 1116 and Event ID 1117. Event ID 1116's symbolic name is "MALWAREPROTECTION_STATE_MALWARE_DETECTED" and it means, "The antimalware platform detected malware or other potentially unwanted software." (Microsoft, 2022). Event ID 1117's symbolic name is "MALWAREPROTECTION_STATE_MALWARE_ACTION_TAKEN" and it means, "The antimalware platform performed an action to protect your system from malware or

other potentially unwanted software." (Microsoft, 2022). This is consistent with the observations from the Graylog server. Screenshot below shows the forwarded event logs after the sfile ransomware has been executed. The 3rd column shows the event IDs and the 5th column shows the process ID.

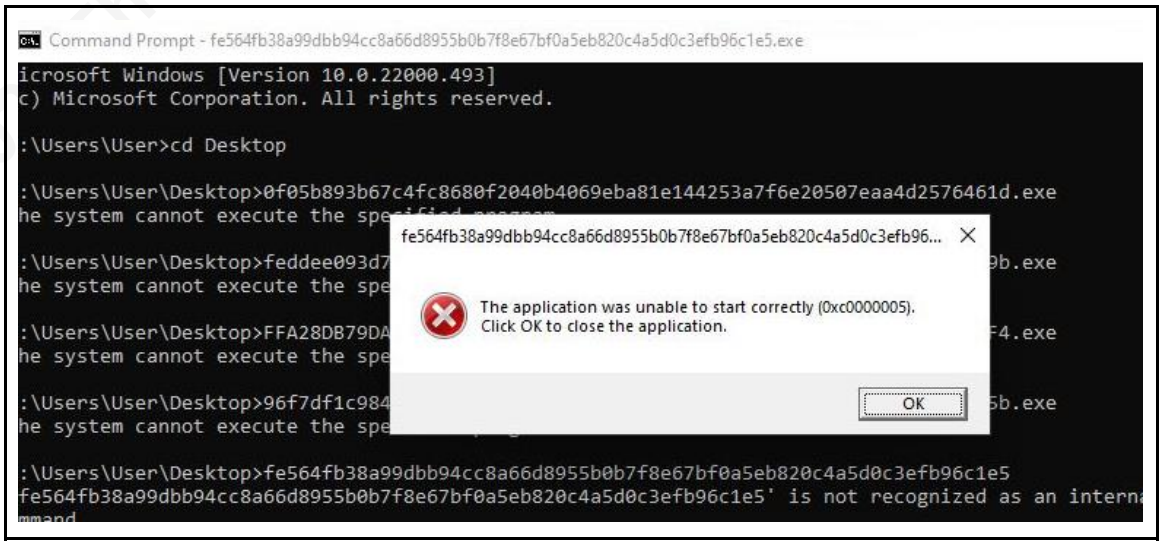


Received Event Logs in Graylog server

Upon clicking on the individual log more details are shown. A key detail is the full message field that explains about the ransomware quarantined like the name etc. The full message for sfile ransomware as shown below shows that it is the "Ransom:Win32/Morsp.ST!MTB" variant.

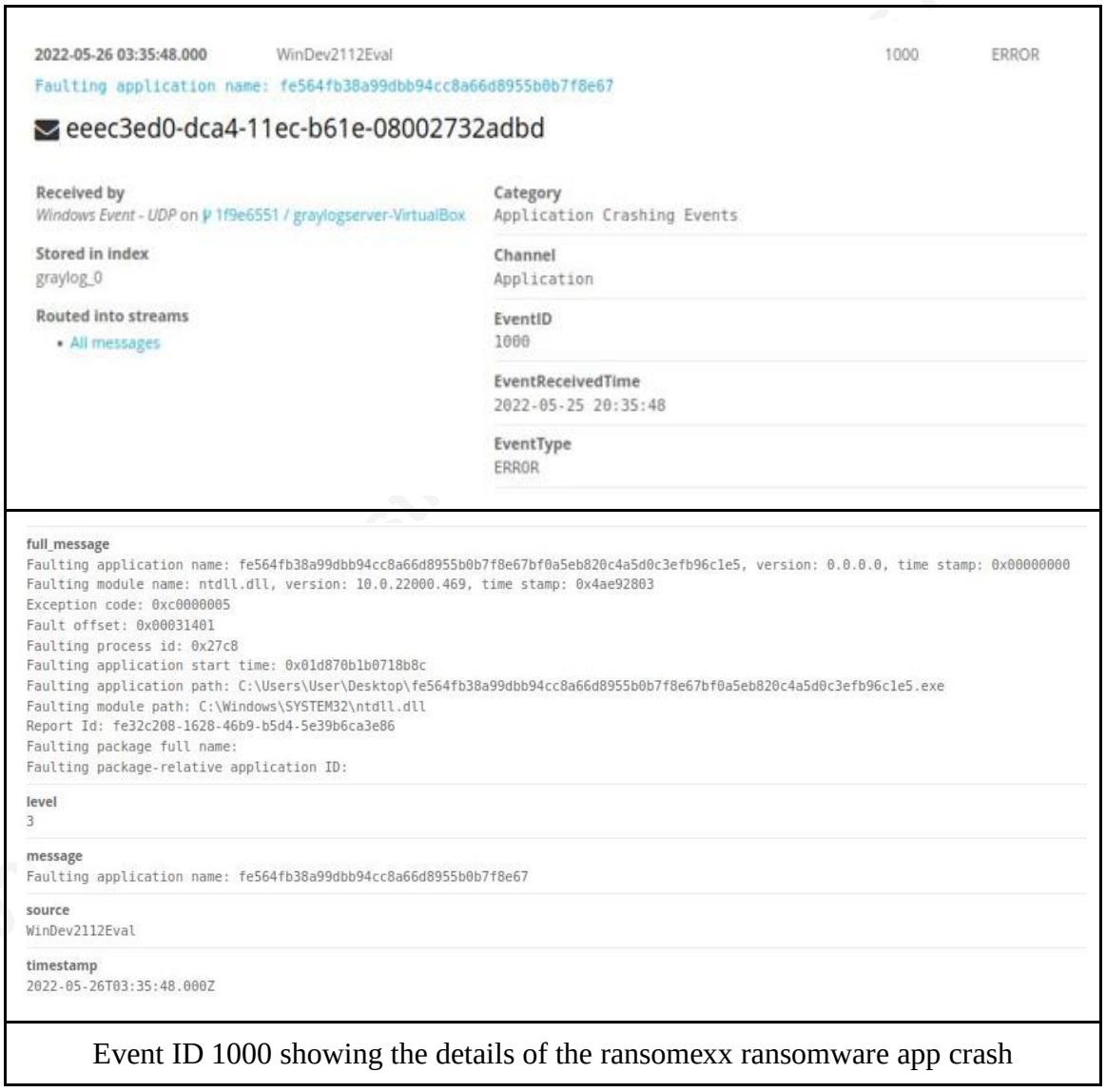
Full Message field from EventID 1117 for sfile ransomware

The second occurrence is the ransomware crashing and thus not being able to be executed. In an enterprise scenario, this is also a relevant scenario as even though the ransomware crashed being executed in that particular system it could be pivoted till it founds a suitable system and then being executed. The screenshot below shows such an occurrence where the ransomexx ransomware crashes when executed.



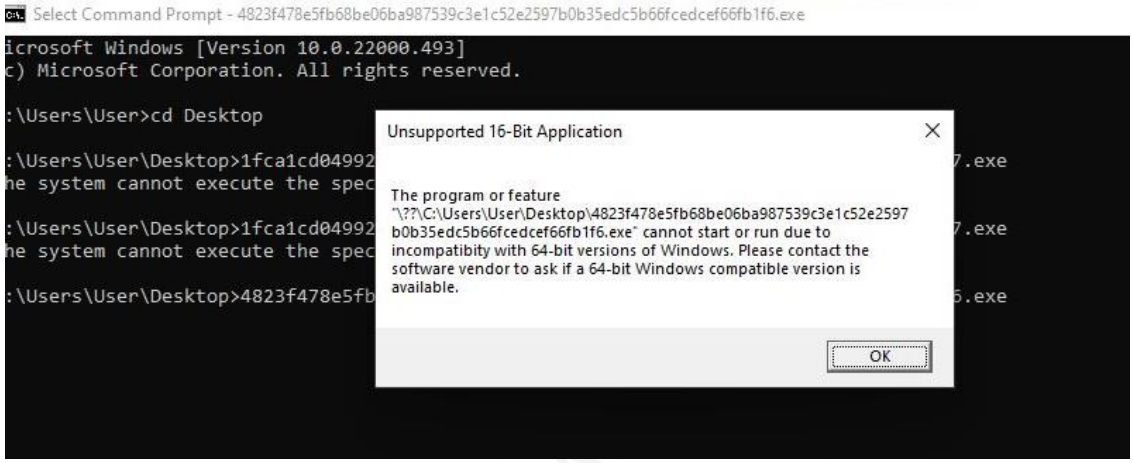
Ransomexx ransomware unable to start and crashes

The event log generated is Application Event ID 1000. Screenshots below show the event log and full message field containing details of the crash.



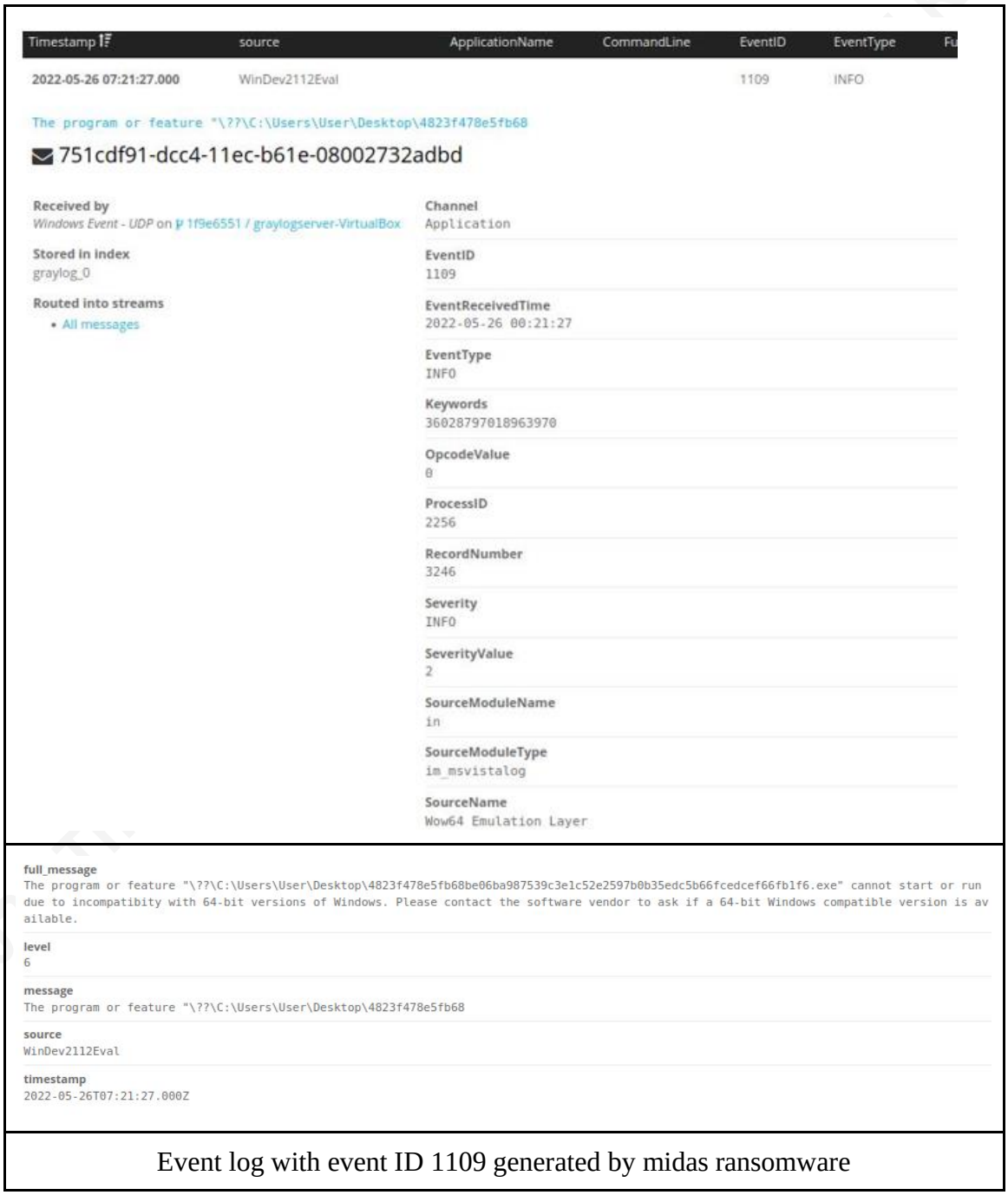
Event ID 1000 showing the details of the ransomexx ransomware app crash

The third occurrence is similar to the App crashing occurrence as above but in this case due to incompatibility issues like 16-bit application which is incompatible to run on a 64-bit system like the midas ransomware as shown in the screenshot below.



Midas ransomware incompatible to run

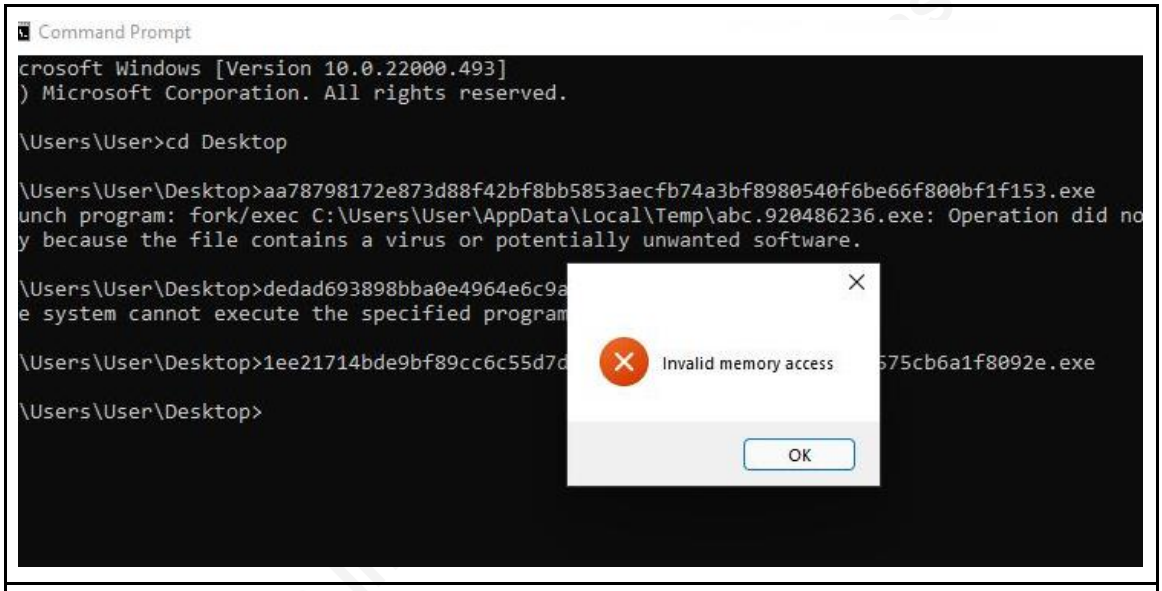
This is also a relevant occurrence as like in the second occurrence the ransomware could still pivot till it finds a compatible system to be executed. For incompatible apps, event log with event ID 1109 is generated as shown below.



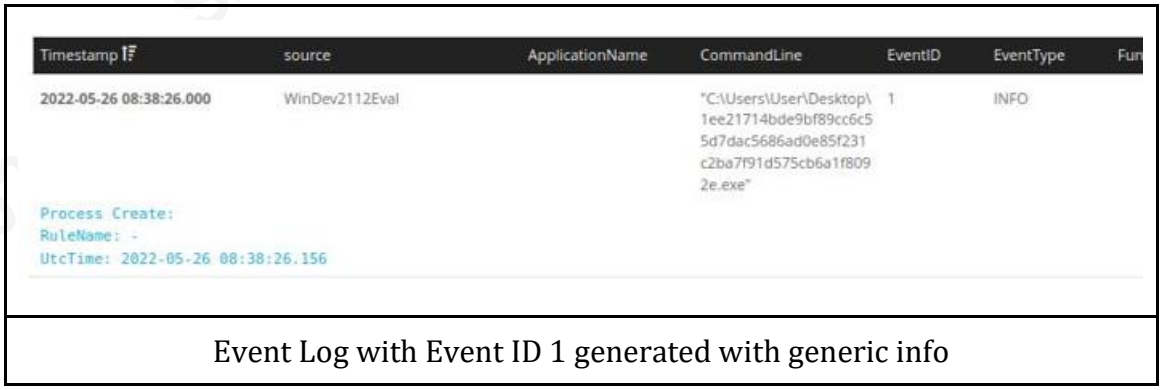
Event log with event ID 1109 generated by midas ransomware

The fourth occurrence is the ransomware not being able to run at all due to memory access error or could not be launched at all. These could be due to corrupted application thus even if it could pivot into other systems, it may not be able to be executed. In this scenario no logs were also generated other than the generic info event log with event ID 1 that shows

the execution of an application. See screenshot below for the evilnominatus ransomware that has memory access error and the event log generated.



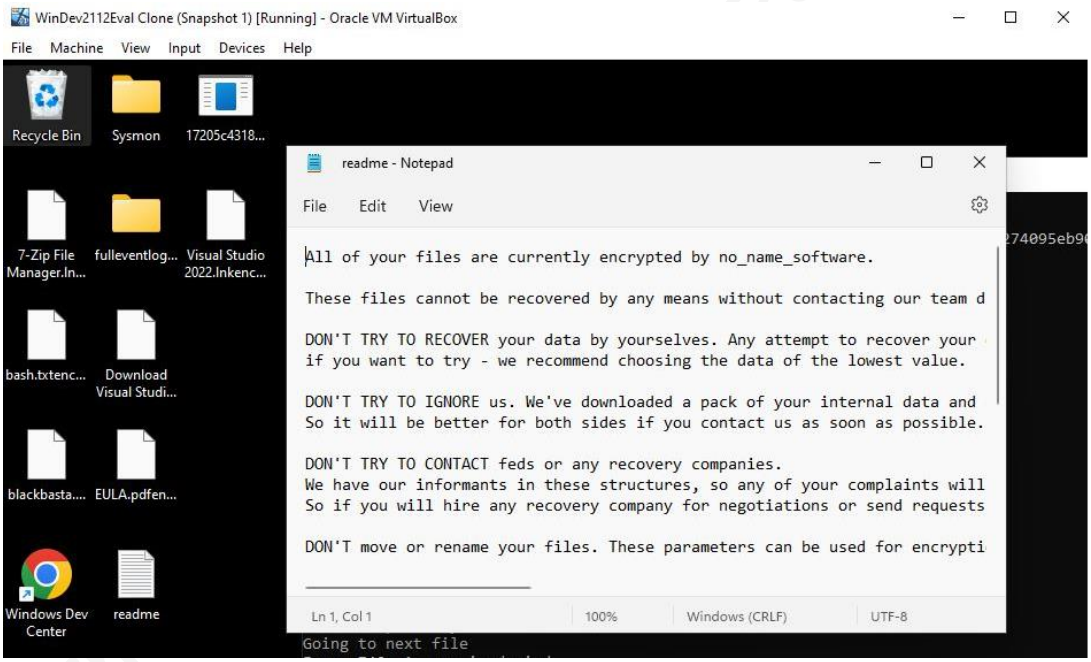
Evilnominatus ransomware with “Invalid memory access” error



Event Log with Event ID 1 generated with generic info

The fifth and the final observation is when the ransomware has been successfully executed and encrypts the user files with a ransom note. This shows that even when running the latest operating system like Windows 11 with the latest Microsoft Defender AV solution it is still possible to be affected by ransomware. Three ransomwares from the 37 tested were able to be executed. There are blackbasta, koxic and nokoyawa. Screenshots below showing the successful execution and display of ransom note from the three ransomwares. For blackbasta, Microsoft Defender was able to detect it as a ransomware due to the ransom

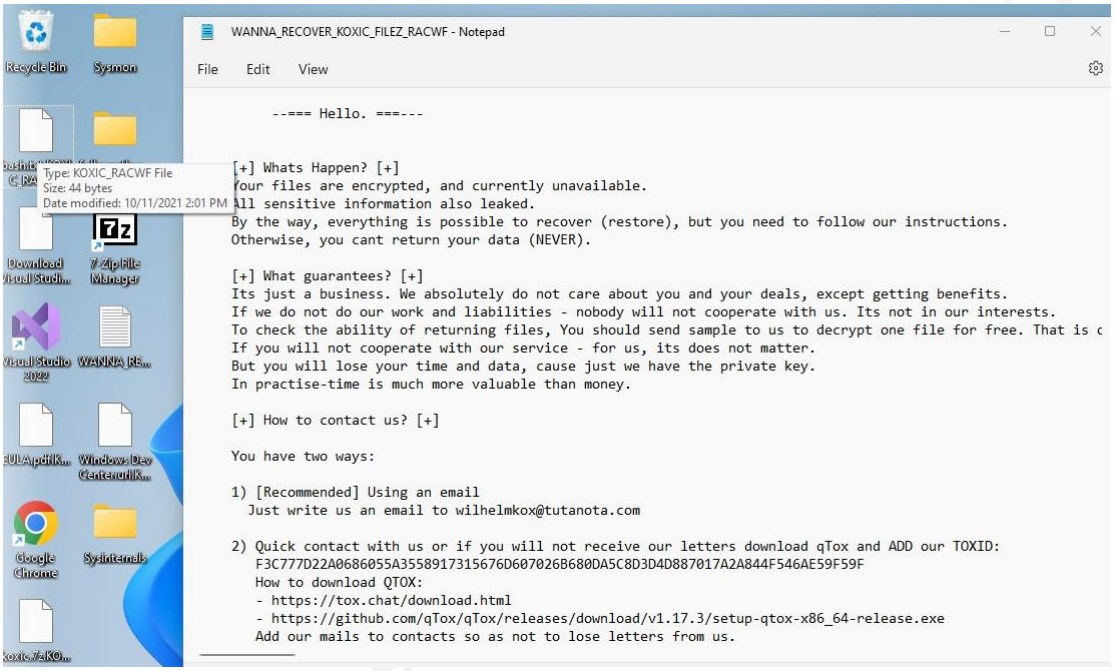
note created based on the full message content, thus it was after the ransomware was successfully executed but it didn't remove the ransomware nor prevent it from being executed. Thus, only the event log with event ID 1116 was detected. But for koxic and nokoyawa, these were also not detected.



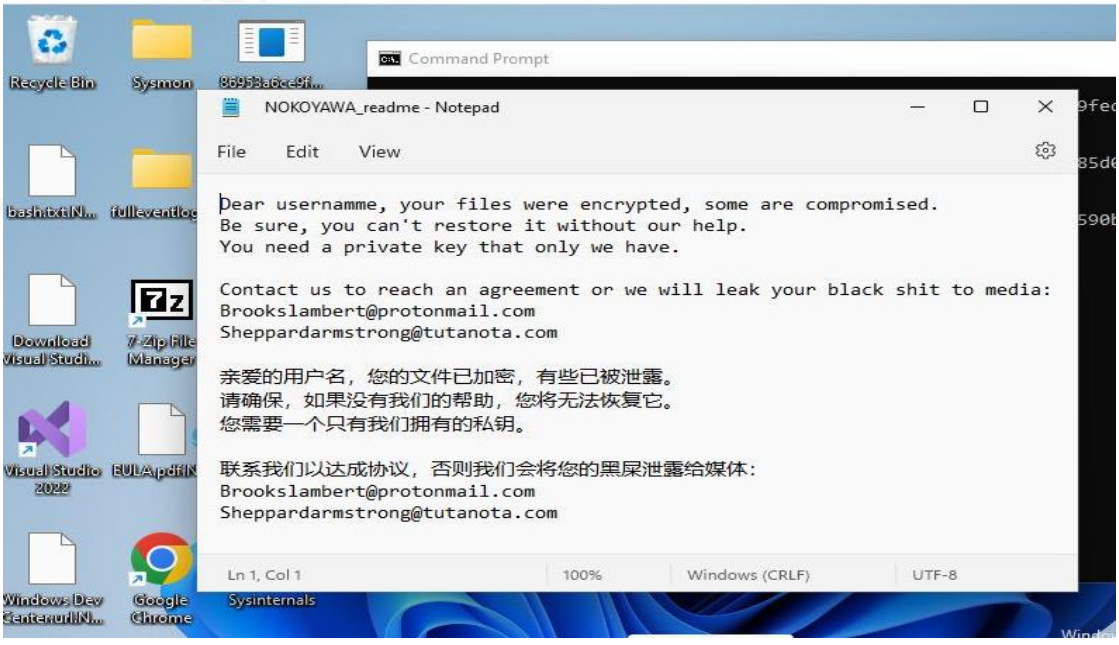
Blackbasta Ransomware

```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Behavior:Win32/Ransomware!Note.L&threatid=2147785254&enterprise=0
        Name: Behavior:Win32/Ransomware!Note.L
        ID: 2147785254
        Severity: Severe
        Category: Suspicious Behavior
        Path: behavior:_pid:9260:273448463567947; process:_pid:9260,ProcessStart:132980297900558793
        Detection Origin: Unknown
        Detection Type: Concrete
        Detection Source: Unknown
        User:
        Process Name: C:\Users\User\Desktop\17205c43189c22dfcb278f5cc45c2562f622b0b6280dcd43cc1d3c274095eb90.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

Blackbasta ransomware's event log (event ID 1116) triggered by the ransom note

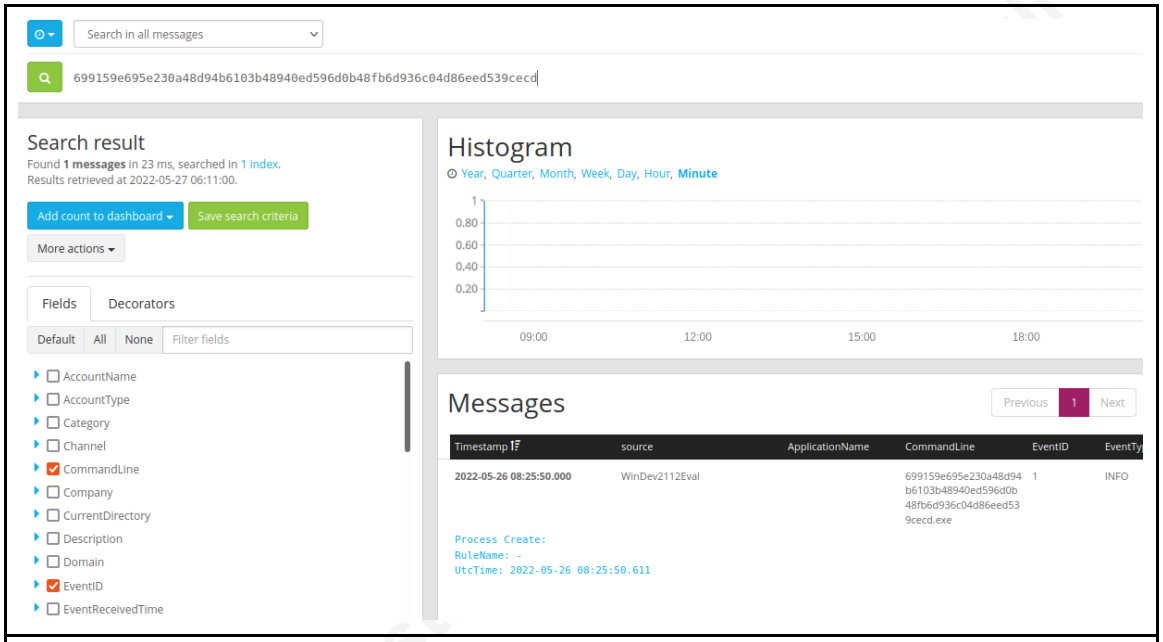


Koxic Ransomware



Nokoyawa Ransomware

In this scenario the only event log generated was the generic info event log with event ID 1 that shows the execution of an application as shown below.



Event log with event ID generated for koxic ransomware

6. Summary of Findings

The table below shows the 5 different occurrences and the corresponding event logs generated and their IDs as explained above. The threat name, threat ID and the file hash is also included as it will aid in the post investigation phase where the necessary team can get more information of the ransomware.

Ransomware Name & File Hash	Detection Type	Event Log	Threat Name	Threat ID
AvosLocker: f810deb1ba171cea5b595c6d3f816127fb182833f7a08a98de93226d4f6a336f	Concrete	1116, 1117	Ransom:Win32/AvosLocker.MBK!MTB	2147798265
BandarChorRansomware: B4362FCD75FD071FC8237C543C56DF5736B8E177	Concrete	1116, 1117	Ransom:Win32/Isda.A	2147689536
BlackBastaRansomware: 17205c43189c22dfcb278f5cc45c2562f622b0b6280dcd43cc1d3c274095eb90	Not Detected	1, 1116	Behavior:Win32/Ransomware!Note.L *1116 generated due to the ransom note.	NIL
BlackCatRansomware:	Concrete	1116,	Ransom:Win32/BlackCat.	2147809870

Perumal P S, perumal316@gmail.com

f837f1cd60e9941aa60f7be50a8f2aaaac380f560db8ee001408f35c1b7a97cb		1117	MK!MTB	
CerberRansomware: 772cad26853c7d8ea8f1023f6e3cba219cc9bb1db1cd31ad2b979e59d3d9c631	Concrete	1116, 1117	Ransom:Win32/Aicat.A!MTB	2147809789
ClownicRansomware: 880823dd9df0ca6047cd829a1031e8a167ccec0629fdeac40a097dd555debf7c	Concrete	1116, 1117	Ransom:MSIL/FileCryptor.AB!MTB	2147769543
CubaRansomware: f68cea99e6887739cd82865f9b973664117af14c1a25d4917eec25ce4b26a381	Concrete	1116, 1117	Trojan:Win32/KillAV.SA	2147808492
CuratorRansomware: 4d2c614ba98df43601b6d9551bd26684	Concrete	1116, 1117	Ransom:Win32/Filecoder.AA!MTB	2147774270
DeadBoltRansomware: 444e537f86cbeeea5a4fcf94c485cc9d286de0ccd91718362cecf415bf362bcf	Concrete	1116, 1117	Ransom:Linux/DeadBolt.A!MTB	2147811548
DearCryRansomware: 0e55ead3b8fd305d9a54f78c7b56741a	Concrete	1116, 1117	Ransom:Win32/DoejoCrypt.A	2147777392
DecafRansomware: 5da2a2ebe9959e6ac21683a8950055309eb34544962c02ed564e0deaf83c9477	Concrete	1116, 1117	Ransom:Win64/Deecaf.A!dha	2147797631
DiavolRansomware: ee13d59ae3601c948bd10560188447e6faaeef5336dcd605b52ee558ff2a8588	Concrete	1116, 1117	Ransom:Win32/Lovaid	2147797706
EvilNominatusRansomware: 1ee21714bde9bf89cc6c55d7dac5686ad0e85f231c2ba7f91d575cb6a1f8092e	Not Detected and Not Executed due to memory error	1	NIL	NIL
HaronRansomware: 5b9dee21841e1b6fd1477008b73729a0	Concrete	1116, 1117	Ransom:MacOS/Filecoder	2147768612

HiveRansomware: aa78798172e873d88f42bf8bb5853aecfb74a3bf8980540f6be66f800bf1f153	Concrete	1116, 1117	Ransom:Win64/Hive.E!MTB	2147816425
KoxicRansomware: 699159e695e230a48d94b6103b48940ed596d0b48fb6d936c04d86eed539cecd	Not detected and executed successfully	1	NIL	NIL
KrusRansomware: df109084e55980239d6d39a3a52afc372f5251653a3893497e3017e65c65e2a3	Not detected and not executed due to incompatibility	1109	NIL	NIL
LockBitRansomware: fc720ba95ab46e6a5f9fd7f6b1f240cd9b29cd96f6cb075f0459fac230f7de94	Concrete	1116, 1117	Ransom:Win32/Lockbit.STA	2147788196
LockyRansomware: E7AAD826559C8448CD8BA9F53F401182	Not detected and not executed due to incompatibility	1109	NIL	NIL
LokiLockerRansomware: 4215b5ce91deb97011cba2dd94d5bac1a745d6d55f6938b86e209eaaf8e655df	Concrete	1116, 1117	Ransom:MSIL/LokiLocker.MK!MTB	2147808650
LorenzRansomware: edc2070fd8116f1df5c8d419189331ec606d10062818c5f3de865cd0f7d6db84	Concrete	1116, 1117	Ransom:Win32/Lorenz!mclg	2147811807
MagniberRansomware: e2d3af7acd9bb440f9972b192cbfa83b07abdbb042f8bf1c2bb8f63944a4ae39	Not detected and not executed due to incompatibility	1109	NIL	NIL
MementoRansomware: 09a0caadc4df3d4278368f94f52007894c2b51d3785d985cb8e	Concrete	1116, 1117	Trojan:Win64/Malgent!MSR	2147782947

42646e8a33b68				
MidasRansomware: 4823f478e5fb68be06ba987539c3e1c52e2597b0b35edc5b66fcedcef66fb1f6	Not detected and not executed due to incompatibility	1109	NIL	NIL
NightSkyRansomware: 1fca1cd04992e0fcaa714d9dfa97323d81d7e3d43a024ec37d1c7a2767a17577	Concrete	1116, 1117	Ransom:Win64/NightSky!MTB	2147809814
NokoyawaRansomware: 86953a6ce9fb7bf8b7791b9c6b751120c35ee1df5590ba4ff447e21c29259e51	Not detected and executed successfully	1	NIL	NIL
OnyxRansomware: a7f09cfde433f3d47fc96502bf2b623ae5e7626da85d0a0130dcd19d1679af9b	Concrete	1116, 1117	Ransom:MSIL/FileCoder.AD!MTB	2147798231
PandoraRansomware: 5b56c5d86347e164c6e571c86dbf5b1535eae6b979fede6ed66b01e79ea33b7b	Concrete	1116, 1117	Ransom:Win64/FileCoder!MSR	2147764332
PhobosRansomware: a91491f45b851a07f91ba5a200967921bf796d38677786de51a4a8fe5ddeafd2	Concrete	1116, 1117	Ransom:Win32/Blocker	2147742143
RansomExx: fe564fb38a99dbb94cc8a66d8955b0b7f8e67bf0a5eb820c4a5d0c3efb96c1e5	Not detected and crashes	1000	NIL	NIL
RookRansomware: 96f7df1c984c1753289600f7f373f3a98a4f09f82acc1be8ecfd5790763a355b	Concrete	1116, 1117	Ransom:Win64/RookCrypt!MSR	2147805809
SamsamRansomWare: FFA28DB79DACA3B93A283CE2A6FF24791956A768CB5FC791C075B638416B51F4	Concrete	1116, 1117	HackTool:Win32/NLBrute	2147723627
SFileRansomware: feddee093d72838ac1f13ea9bbf	Concrete	1116, 1117	Ransom:Win32/Morsp.ST!MTB	2147762665

c0473e2f3df1495432d6f95d6fe8ddf7ff09b				
SugarRansomware: 0f05b893b67c4fc8680f2040b4069eba81e144253a7f6e20507eaa4d2576461d	Concrete	1116, 1117	Ransom:Win32/FileCryptor.MAK!MTB	2147810020
SynAckRansomware: 5b9dee21841e1b6fd1477008b73729a0	Concrete	1116, 1117	Ransom:MacOS/Filecoder	2147768612
WhiteRabbitRansomware: 03e8b29ad5055f1dda1b0e9353dc2c1421974eb3d0a115d0bb35c7d76f50de20	Concrete	1116, 1117	Trojan:Win32/Tnega!MSR	2147754624
YanluowangRansomware: d11793433065633b84567de403c1989640a07c9a399dd2753aaf118891ce791c	Concrete	1116, 1117	Ransom:Win32/Yanluow.STA	2147794251

Refer to Appendix A for the screenshots of the log details as forwarded to the GrayLog server.

7. Conclusion

Due to the Covid-19 pandemic where Work from Home (WFH) and Remote Work arrangements became common, it also fueled the 105% increase in ransomware attacks in 2021 (Taylor, 2022). In this paper, out of the 37 different ransomware variants tested, 28 variants were detected successfully by Microsoft Defender. The detection generated windows event logs with the event IDs 1116 and 1117. 1 variant was not detected and crashed generating an event log with event ID 1000. 4 variants were also not detected and it could not be executed due to compatibility issues and generated event log with event ID 1109. Another 1 variant could not be executed due to memory issues and also generated the event log with event ID 1. And 3 ransomware variants were able to be executed and could not be detected by Microsoft Defender running on the latest Windows 11 platform. These also generated the event logs with the event ID 1.

Thus, for incident responders doing triage investigations in a ransomware incident, they should look for event logs with the IDs, 1, 1000, 1109, 1116 and 1117. These will cover the different scenarios like successful execution, non-execution due to incompatibility issues but still residing in the system, non-execution due to memory issues or ransomware crashing and, in a scenario, where Microsoft Defender has detected the ransomware and have removed it. These will give them clues and necessary information to determine the next course of action to assist the affected organization in recovering from a ransomware attack.

Future work will include studying how the information from the windows event logs can be incorporated into detection rules like yara or sigma rules in an automated manner that can be used to prevent the spread of ransomware in a network. Similarly, the threat name, threat ID and the file hash will aid in the post investigation phase where the necessary Security Information and Event Management (SIEM) teams can get more information about the ransomware and build different use cases for early detection and prevention by the Security Operations Centers (SOCs) as it has been shown that even with the latest Microsoft Defender with the latest Windows 11 operating system is not immune to known ransomware variants.

References

Anderson, B. (2018, March 22). *Why Windows Defender Antivirus is the most deployed in the enterprise*. Microsoft. Retrieved May 27, 2022, from https://www.microsoft.com/security/blog/2018/03/22/why-windows-defender-antivirus-is-the-most-deployed-in-the-enterprise/

Checkpoint. (n.d.). *Ransomware Attack - What is it and How Does it Work?* Checkpoint. Retrieved April 21, 2022, from https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/

Crowdstrike. (2021, December 8). *Most Common Types of Ransomware*. CrowdStrike. Retrieved April 21, 2022, from https://www.crowdstrike.com/cybersecurity-101/ransomware/types-of-ransomware/

Fortuna, A. (2017, October 20). *Windows event logs in forensic analysis*. Andrea Fortuna. Retrieved April 21, 2022, from https://andreafortuna.org/2017/10/20/windows-event-logs-in-forensic-analysis/

Gillis, A. S. (2018, May 16). *What is Windows event log? - Definition from WhatIs.com*. TechTarget. Retrieved April 21, 2022, from https://www.techtarget.com/searchwindowsserver/definition/Windows-event-log

IBM. (n.d.). *What is Security Information and Event Management (SIEM)?* IBM. Retrieved April 21, 2022, from https://www.ibm.com/topics/siem

Kaspersky. (n.d.). *Ransomware Attacks and Types | How do Locky, Petya and other ransomware differ?* Kaspersky. Retrieved April 21, 2022, from https://www.kaspersky.com/resource-center/threats/ransomware-attacks-and-types

Perumal P S, perumal316@gmail.com

Kerner, S. M. (n.d.). *Ransomware Trends, Statistics and Facts in 2022*. TechTarget. Retrieved May 27, 2022, from https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts

Mearian, L. (2021, December 2). *Windows 11 adoption nears 9%, but businesses are waiting*. Computerworld. Retrieved May 27, 2022, from https://www.computerworld.com/article/3643074/windows-11-adoption-nears-9-but-businesses-are-waiting.html

Microsoft. (n.d.). *Download a Windows virtual machine - Windows app development*. Microsoft Developer. Retrieved April 21, 2022, from https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/

Microsoft. (2022, May 23). *Microsoft Defender Antivirus event IDs and error codes*. Microsoft Docs. Retrieved May 27, 2022, from https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/troubleshoot-microsoft-defender-antivirus?view=o365-worldwide

Nxlog. (n.d.). *About Windows Event Log*. NXLog Documentation. Retrieved June 6, 2022, from https://docs.nxlog.co/userguide/integrate/windows-eventlog.html

Ravindran, A. (2020, August 10). *Notable event IDs from Windows Event Logs – Digital Forensics and Incident Response*. Digital Forensics and Incident Response. Retrieved April 22, 2022, from https://digitalf0rensics.wordpress.com/2020/08/10/notable-event-ids-from-windows-event-logs/

Perumal P S, perumal316@gmail.com

SOPHOS. (2022, January 24). *Interesting Windows Event IDs - Malware/General Investigation*. Sophos Support Portal. Retrieved April 22, 2022, from https://support.sophos.com/support/s/article/KB-000038860?language=en_US

Statista. (2022, May 23). • *Desktop OS market share*. Statista. Retrieved May 27, 2022, from https://www.statista.com/statistics/218089/global-market-share-of-windows-7/

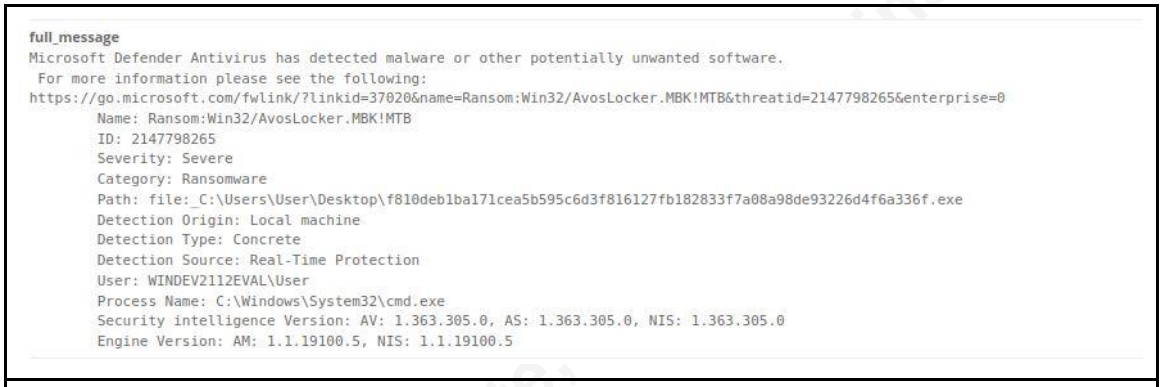
Taylor, A. (2022, February 17). *Ransomware cyberattacks surged in 2021 according to a new report*. Fortune. Retrieved June 6, 2022, from https://fortune.com/2022/02/17/ransomware-attacks-surge-2021-report/

vx-underground. (n.d.). *Directory: samples/Families*. vx-underground. Retrieved May 27, 2022, from https://samples.vx-underground.org/samples/Families/

Waderni, L. (2017, May 5). *How To Install and Configure Graylog Server on Ubuntu 16.04 LTS*. YallaLabs. Retrieved April 21, 2022, from https://yallalabs.com/linux/how-to-install-and-configure-graylog-server-on-ubuntu-16-04-lts/

Appendix A

Microsoft Defender Description of Detected Ransomware

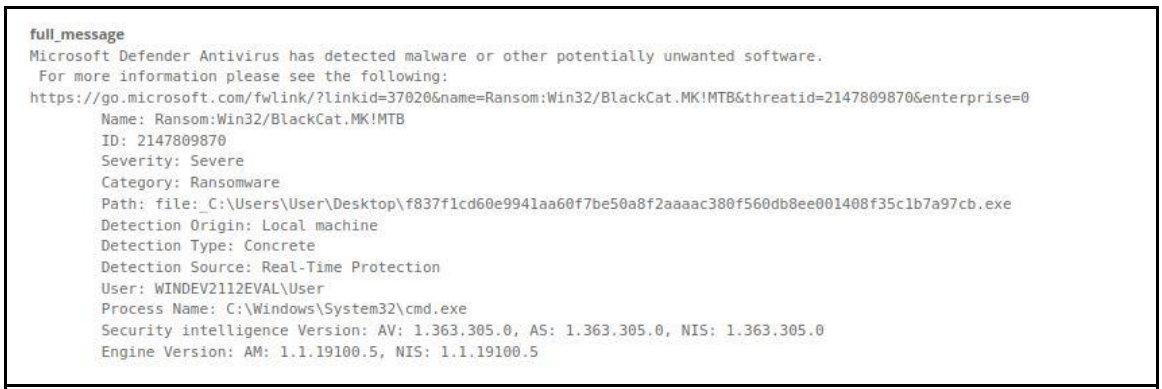


```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Ransom:Win32/AvosLocker.MBK!MTB&threatid=2147798265&enterprise=0
        Name: Ransom:Win32/AvosLocker.MBK!MTB
        ID: 2147798265
        Severity: Severe
        Category: Ransomware
        Path: file:_C:\Users\User\Desktop\f810deb1ba171cea5b595c6d3f816127fb182833f7a08a98de93226d4f6a336f.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: WINDEV2112EVAL\User
        Process Name: C:\Windows\System32\cmd.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

AvosLocker

```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Ransom:Win32/Isda.A&threatid=2147689536&enterprise=0
        Name: Ransom:Win32/Isda.A
        ID: 2147689536
        Severity: Severe
        Category: Ransomware
        Path: file:_C:\Users\User\Desktop\B4362FCD75FD071FC8237C543C56DF5736B8E177.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: WINDEV2112EVAL\User
        Process Name: C:\Windows\System32\cmd.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

Bandarchor



```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Ransom:Win32/BlackCat.MK!MTB&threatid=2147809870&enterprise=0
        Name: Ransom:Win32/BlackCat.MK!MTB
        ID: 2147809870
        Severity: Severe
        Category: Ransomware
        Path: file:_C:\Users\User\Desktop\f837f1cd60e9941aa60f7be50a8f2aaaac380f560db8ee001408f35c1b7a97cb.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: WINDEV2112EVAL\User
        Process Name: C:\Windows\System32\cmd.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

Blackcat

Perumal P S, perumal316@gmail.com

```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Ransom:Win32/Aicat.A!MTB&threatid=2147809789&enterprise=0
        Name: Ransom:Win32/Aicat.A!MTB
        ID: 2147809789
        Severity: Severe
        Category: Ransomware
        Path: file:_C:\Users\User\Desktop\772cad26853c7d8ea8f1023f6e3cba219cc9bb1db1cd31ad2b979e59d3d9c631.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: WINDEV2112EVAL\User
        Process Name: C:\Windows\System32\cmd.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

Cerber

```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Ransom:MSIL/FileCryptor.AB!MTB&threatid=2147769543&enterprise=0
        Name: Ransom:MSIL/FileCryptor.AB!MTB
        ID: 2147769543
        Severity: Severe
        Category: Ransomware
        Path: file:_C:\Users\User\Desktop\880823dd9df0ca6047cd829a1031e8a167ccec0629fdeac40a097dd555debf7c.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: WINDEV2112EVAL\User
        Process Name: C:\Windows\explorer.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

Clownic

```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win32/KillAV.SA&threatid=2147808492&enterprise=0
        Name: Trojan:Win32/KillAV.SA
        ID: 2147808492
        Severity: Severe
        Category: Trojan
        Path: file:_C:\Users\User\Desktop\f68cea99e6887739cd82865f9b973664117af14c1a25d4917eec25ce4b26a381.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: WINDEV2112EVAL\User
        Process Name: C:\Windows\explorer.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

Cuba

```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Ransom:Win32/Filecoder.AA!MTB&threatid=2147774270&enterprise=0
        Name: Ransom:Win32/Filecoder.AA!MTB
        ID: 2147774270
        Severity: Severe
        Category: Ransomware
        Path: file:_C:\Users\User\Desktop\4d2c614ba98df43601b6d9551bd26684.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: WINDEV2112EVAL\User
        Process Name: C:\Windows\explorer.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

Curator

```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Ransom:Linux/DeadBolt.A!MTB&threatid=2147811548&enterprise=0
        Name: Ransom:Linux/DeadBolt.A!MTB
        ID: 2147811548
        Severity: Severe
        Category: Ransomware
        Path: file:_C:\Users\User\Desktop\444e537f86cbeeea5a4fcf94c485cc9d286de0ccd91718362cecf415bf362bcf.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: WINDEV2112EVAL\User
        Process Name: C:\Windows\System32\cmd.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

Deadbolt

```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Ransom:Win32/DoejoCrypt.A&threatid=2147777392&enterprise=0
        Name: Ransom:Win32/DoejoCrypt.A
        ID: 2147777392
        Severity: Severe
        Category: Ransomware
        Path: file:_C:\Users\User\Desktop\0e55ead3b8fd305d9a54f78c7b56741a.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: WINDEV2112EVAL\User
        Process Name: C:\Windows\explorer.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

Dearcry

Perumal P S, perumal316@gmail.com

```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Ransom:Win64/Deecaf.A!dha&threatid=2147797631&enterprise=0
        Name: Ransom:Win64/Deecaf.A!dha
        ID: 2147797631
        Severity: Severe
        Category: Ransomware
        Path: file:_C:\Users\User\Desktop\5da2a2ebe9959e6ac21683a8950055309eb34544962c02ed564e0deaf83c9477.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: WINDEV2112EVAL\User
        Process Name: C:\Windows\explorer.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

Decaf

```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Ransom:Win32/Lovaid&threatid=2147797706&enterprise=0
        Name: Ransom:Win32/Lovaid
        ID: 2147797706
        Severity: Severe
        Category: Ransomware
        Path: file:_C:\Users\User\Desktop\ee13d59ae3601c948bd10560188447e6faaeef5336dcd605b52ee558ff2a8588.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: WINDEV2112EVAL\User
        Process Name: C:\Windows\System32\cmd.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

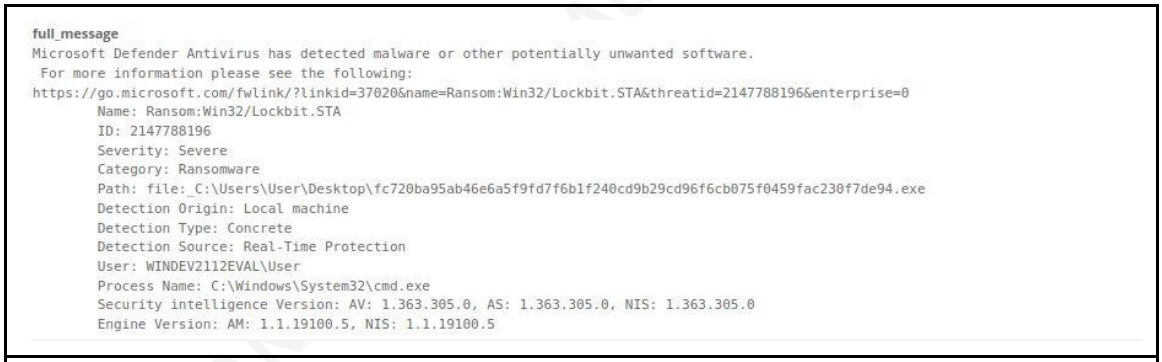
Diavol

```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Ransom:MacOS/Filecoder&threatid=2147768612&enterprise=0
        Name: Ransom:MacOS/Filecoder
        ID: 2147768612
        Severity: Severe
        Category: Ransomware
        Path: file:_C:\Users\User\Desktop\dedad693898bba0e4964e6c9a749d380.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: WINDEV2112EVAL\User
        Process Name: C:\Windows\System32\cmd.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

Haron

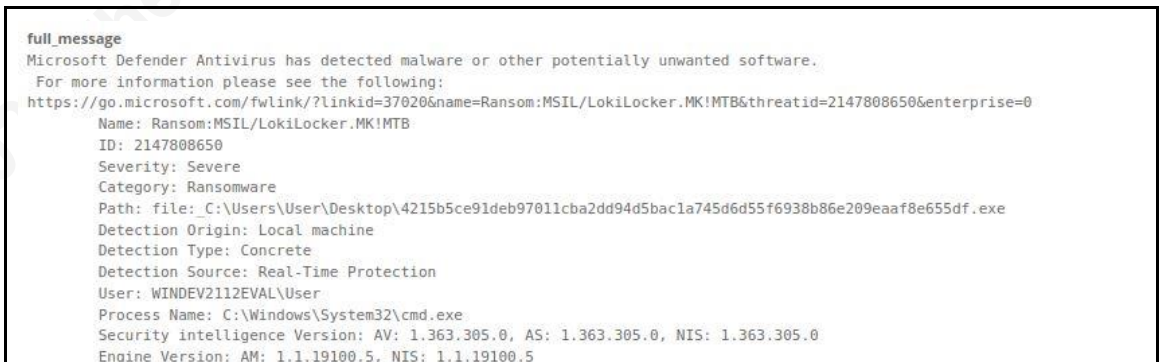
```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Ransom:Win64/Hive.E!MTB&threatid=2147816425&enterprise=0
        Name: Ransom:Win64/Hive.E!MTB
        ID: 2147816425
        Severity: Severe
        Category: Ransomware
        Path: file:_C:\Users\User\AppData\Local\Temp\abc.920486236.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: WINDEV2112EVAL\User
        Process Name: C:\Users\User\Desktop\aa78798172e873d88f42bf8bb5853aecfb74a3bf8980540f6be66f800bf1f153.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

Hive



```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Ransom:Win32/Lockbit.STA&threatid=2147788196&enterprise=0
        Name: Ransom:Win32/Lockbit.STA
        ID: 2147788196
        Severity: Severe
        Category: Ransomware
        Path: file:_C:\Users\User\Desktop\fc720ba95ab46e6a5f9fd7f6b1f240cd9b29cd96f6cb075f0459fac230f7de94.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: WINDEV2112EVAL\User
        Process Name: C:\Windows\System32\cmd.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

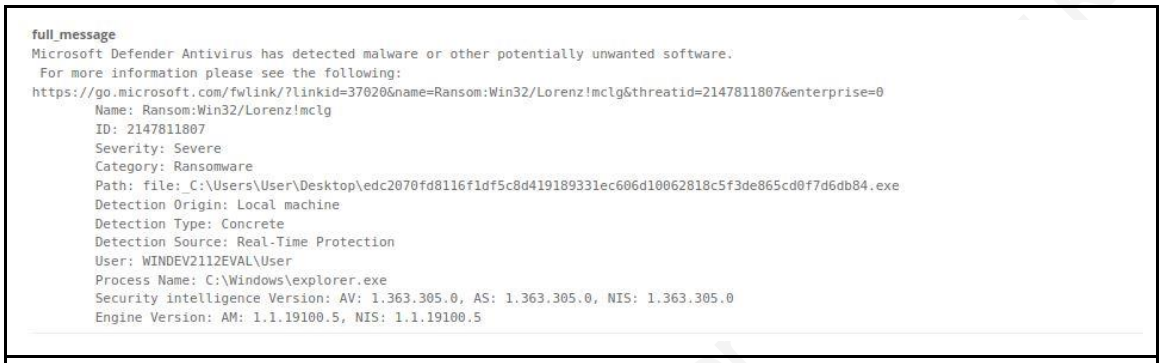
Lockbit



```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Ransom:MSIL/LokiLocker.MK!MTB&threatid=2147808650&enterprise=0
        Name: Ransom:MSIL/LokiLocker.MK!MTB
        ID: 2147808650
        Severity: Severe
        Category: Ransomware
        Path: file:_C:\Users\User\Desktop\4215b5ce91deb97011cba2dd94d5bac1a745d6d55f6938b86e209eaaf8e655df.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: WINDEV2112EVAL\User
        Process Name: C:\Windows\System32\cmd.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

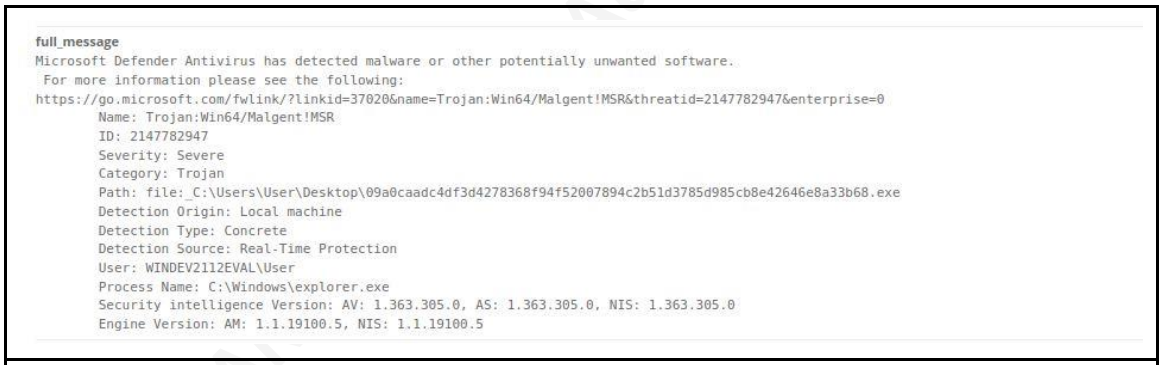
Lokilocker

Perumal P S, perumal316@gmail.com



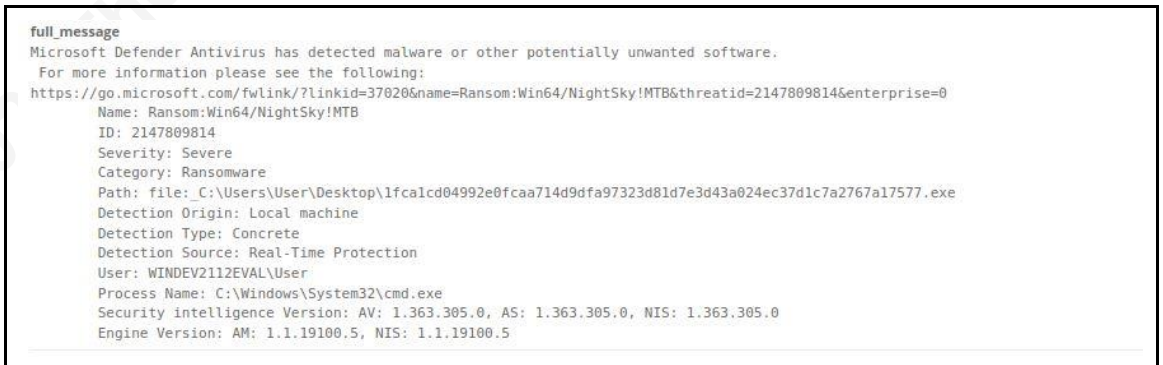
```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Ransom:Win32/Lorenz!mclg&threatid=2147811807&enterprise=0
        Name: Ransom:Win32/Lorenz!mclg
        ID: 2147811807
        Severity: Severe
        Category: Ransomware
        Path: file:_C:\Users\User\Desktop\edc2070fd8116f1df5c8d419189331ec606d10062818c5f3de865cd0f7d6db84.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: WINDEV2112EVAL\User
        Process Name: C:\Windows\explorer.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

Lorenz



```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win64/Malgent!MSR&threatid=2147782947&enterprise=0
        Name: Trojan:Win64/Malgent!MSR
        ID: 2147782947
        Severity: Severe
        Category: Trojan
        Path: file:_C:\Users\User\Desktop\09a0caadc4df3d4278368f94f52007894c2b51d3785d985cb8e42646e8a33b68.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: WINDEV2112EVAL\User
        Process Name: C:\Windows\explorer.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

Memento

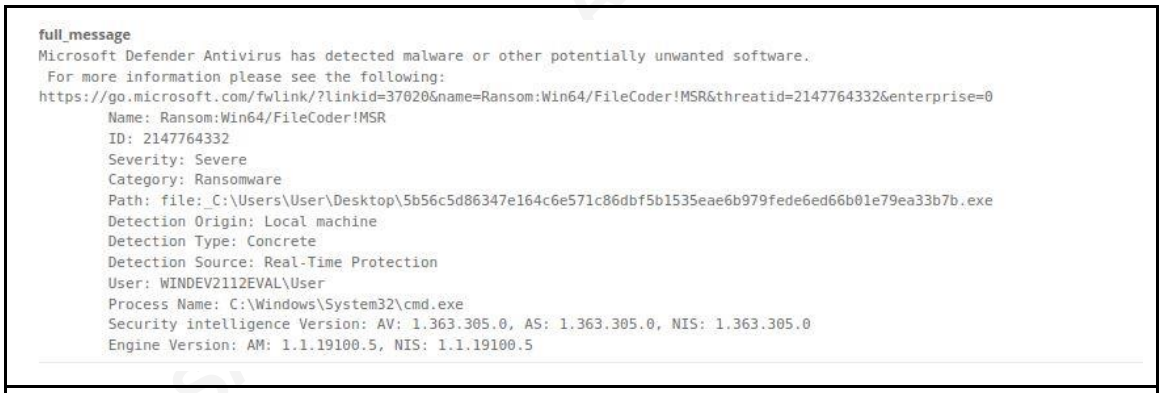


```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Ransom:Win64/NightSky!MTB&threatid=2147809814&enterprise=0
        Name: Ransom:Win64/NightSky!MTB
        ID: 2147809814
        Severity: Severe
        Category: Ransomware
        Path: file:_C:\Users\User\Desktop\1fca1cd04992e0fcaa714d9dfa97323d81d7e3d43a024ec37d1c7a2767a17577.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: WINDEV2112EVAL\User
        Process Name: C:\Windows\System32\cmd.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

Nightsky

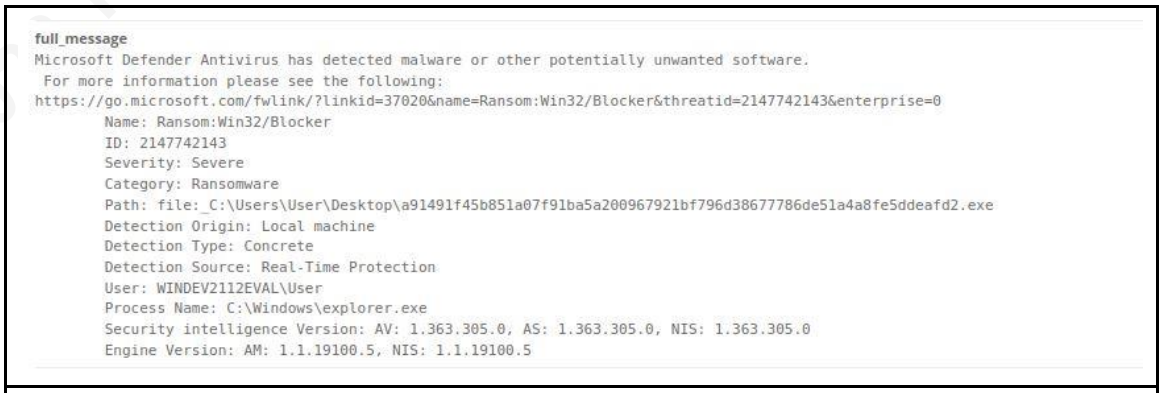
```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Ransom:MSIL/FileCoder.AD!MTB&threatid=2147798231&enterprise=0
        Name: Ransom:MSIL/FileCoder.AD!MTB
        ID: 2147798231
        Severity: Severe
        Category: Ransomware
        Path: file:_C:\Users\User\Desktop\a7f09cfde433f3d47fc96502bf2b623ae5e7626da85d0a0130dcd19d1679af9b.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: WINDEV2112EVAL\User
        Process Name: C:\Windows\System32\cmd.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

Onyx



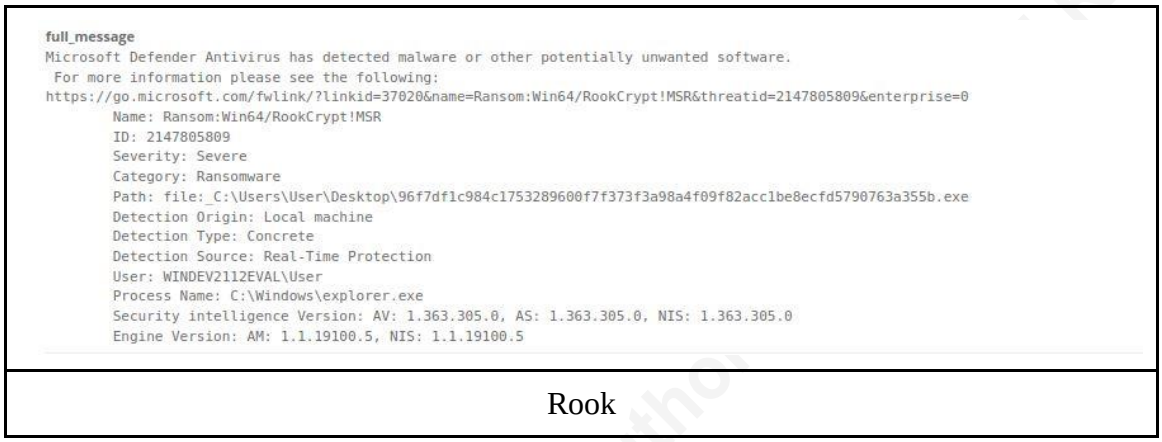
```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Ransom:Win64/FileCoder!MSR&threatid=2147764332&enterprise=0
        Name: Ransom:Win64/FileCoder!MSR
        ID: 2147764332
        Severity: Severe
        Category: Ransomware
        Path: file:_C:\Users\User\Desktop\5b56c5d86347e164c6e571c86dbf5b1535eae6b979fede6ed66b01e79ea33b7b.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: WINDEV2112EVAL\User
        Process Name: C:\Windows\System32\cmd.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

Pandora



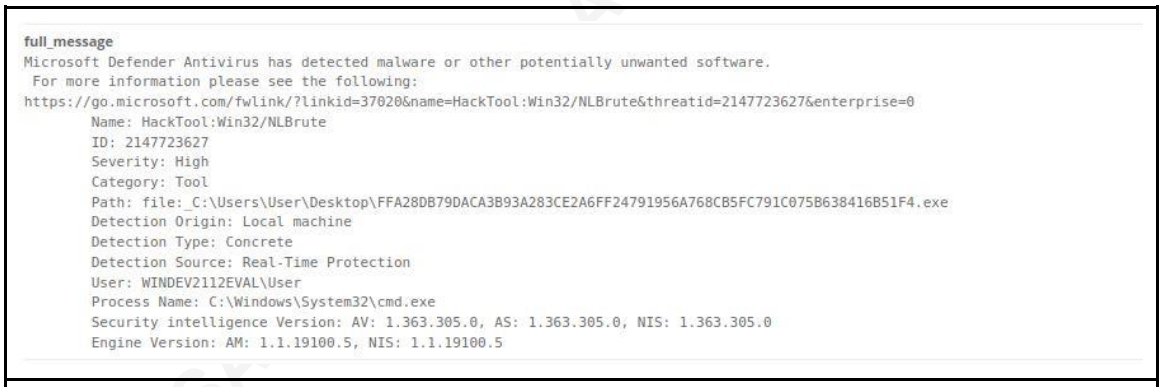
```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Ransom:Win32/Blocker&threatid=2147742143&enterprise=0
        Name: Ransom:Win32/Blocker
        ID: 2147742143
        Severity: Severe
        Category: Ransomware
        Path: file:_C:\Users\User\Desktop\a91491f45b851a07f91ba5a200967921bf796d38677786de51a4a8fe5ddeafd2.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: WINDEV2112EVAL\User
        Process Name: C:\Windows\explorer.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

Phobos



```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Ransom:Win64/RookCrypt!MSR&threatid=2147805809&enterprise=0
        Name: Ransom:Win64/RookCrypt!MSR
        ID: 2147805809
        Severity: Severe
        Category: Ransomware
        Path: file:_C:\Users\User\Desktop\96f7df1c984c1753289600f7f373f3a98a4f09f82acc1be8ecfd5790763a355b.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: WINDEV2112EVAL\User
        Process Name: C:\Windows\explorer.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

Rook



```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=HackTool:Win32/NLBrute&threatid=2147723627&enterprise=0
        Name: HackTool:Win32/NLBrute
        ID: 2147723627
        Severity: High
        Category: Tool
        Path: file:_C:\Users\User\Desktop\FFA28DB79DACA3B93A283CE2A6FF24791956A768CB5FC791C075B638416B51F4.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: WINDEV2112EVAL\User
        Process Name: C:\Windows\System32\cmd.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

Samsam

```
full_message
Microsoft Defender Antivirus has taken action to protect this machine from malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Ransom:Win32/Morsp.ST!MTB&threatid=2147762665&enterprise=0
        Name: Ransom:Win32/Morsp.ST!MTB
        ID: 2147762665
        Severity: Severe
        Category: Ransomware
        Path: file:_C:\Users\User\Desktop\feddee093d72838ac1f13ea9bbfc0473e2f3df1495432d6f95d6fe8ddf7ff09b.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: NT AUTHORITY\SYSTEM
        Process Name: C:\Windows\explorer.exe
        Action: Quarantine
        Action Status:  No additional actions required
        Error Code: 0x00000000
        Error description: The operation completed successfully.
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

Sfile

```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Ransom:Win32/FileCryptor.MAK!MTB&threatid=2147810020&enterprise=0
        Name: Ransom:Win32/FileCryptor.MAK!MTB
        ID: 2147810020
        Severity: Severe
        Category: Ransomware
        Path: file:_C:\Users\User\Desktop\0f05b893b67c4fc8680f2040b4069eba81e144253a7f6e20507eaa4d2576461d.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: WINDEV2112EVAL\User
        Process Name: C:\Windows\explorer.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

Sugar

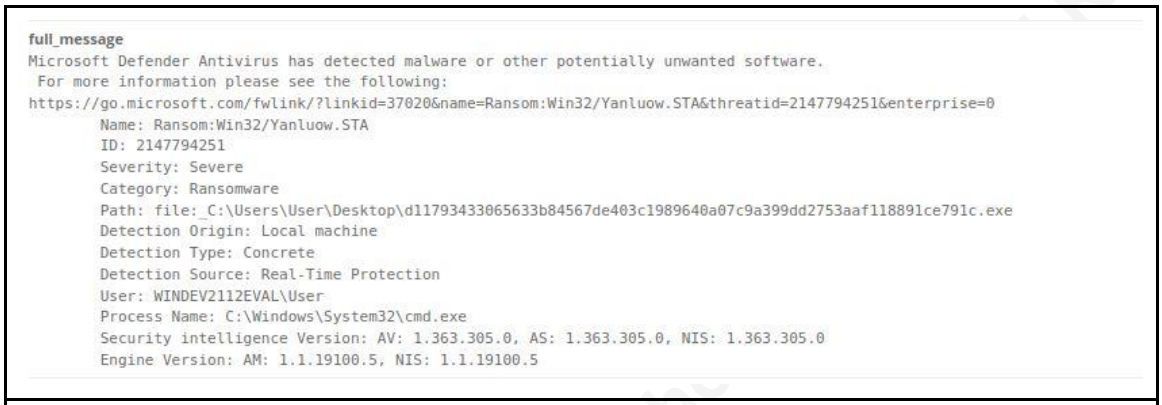
```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Ransom:MacOS/Filecoder&threatid=2147768612&enterprise=0
        Name: Ransom:MacOS/Filecoder
        ID: 2147768612
        Severity: Severe
        Category: Ransomware
        Path: file:_C:\Users\User\Desktop\5b9dee21841e1b6fd1477008b73729a0.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: WINDEV2112EVAL\User
        Process Name: C:\Windows\System32\cmd.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

Synack

```
full_message
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win32/Tnega!MSR&threatid=2147754624&enterprise=0
        Name: Trojan:Win32/Tnega!MSR
        ID: 2147754624
        Severity: Severe
        Category: Trojan
        Path: file:_C:\Users\User\Desktop\03e8b29ad5055f1dda1b0e9353dc2c1421974eb3d0a115d0bb35c7d76f50de20.exe
        Detection Origin: Local machine
        Detection Type: Concrete
        Detection Source: Real-Time Protection
        User: WINDEV2112EVAL\User
        Process Name: C:\Windows\System32\cmd.exe
        Security intelligence Version: AV: 1.363.305.0, AS: 1.363.305.0, NIS: 1.363.305.0
        Engine Version: AM: 1.1.19100.5, NIS: 1.1.19100.5
```

Whiterabbit

Perumal P S, perumal316@gmail.com



Yanluowang

Appendix B

Ransomware tested and their download links

N/o	Ransomware Name	Link to download
1	AvosLocker	https://samples.vx-underground.org/samples/Families/AvosLockerRansomware/Windows/Encryptor/f810deb1ba171cea5b595c6d3f816127fb182833f7a08a98de93226d4f6a336f.7z
2	BandarChorRansomware	https://samples.vx-underground.org/samples/Families/BandarChorRansomware/B4362FCD75FD071FC8237C543C56DF5736B8E177.7z
3	BlackBastaRansomware	https://samples.vx-underground.org/samples/Families/BlackBastaRansomware/Samples/17205c43189c22dfcb278f5cc45c2562f622b0b6280dcd43cc1d3c274095eb90.7z
4	BlackCatRansomware	https://samples.vx-underground.org/samples/Families/BlackCatRansomware/Samples/win/f837f1cd60e9941aa60f7be50a8f2aaaac380f560db8ee001408f35c1b7a97cb.7z
5	CerberRansomware	https://samples.vx-underground.org/samples/Families/CerberRansomware/772cad26853c7d8ea8f1023f6e3cba219cc9bb1db1cd31ad2b979e59d3d9c631.7z
6	ClownicRansomware	https://samples.vx-underground.org/samples/Families/ClownicRansomware/880823dd9df0ca6047cd829a1031e8a167ccec0629fdeac40a097dd555debf7c.7z
7	CubaRansomware	https://samples.vx-underground.org/samples/Families/CubaRansomware/Samples/f68cea99e6887739cd82865f9b973664117af14c1a25d4917eec25ce4b26a381.7z
8	CuratorRansomware	https://samples.vx-underground.org/samples/Families/CuratorRansomware/4d2c614ba98df43601b6d9551bd26684.7z

Perumal P S, perumal316@gmail.com

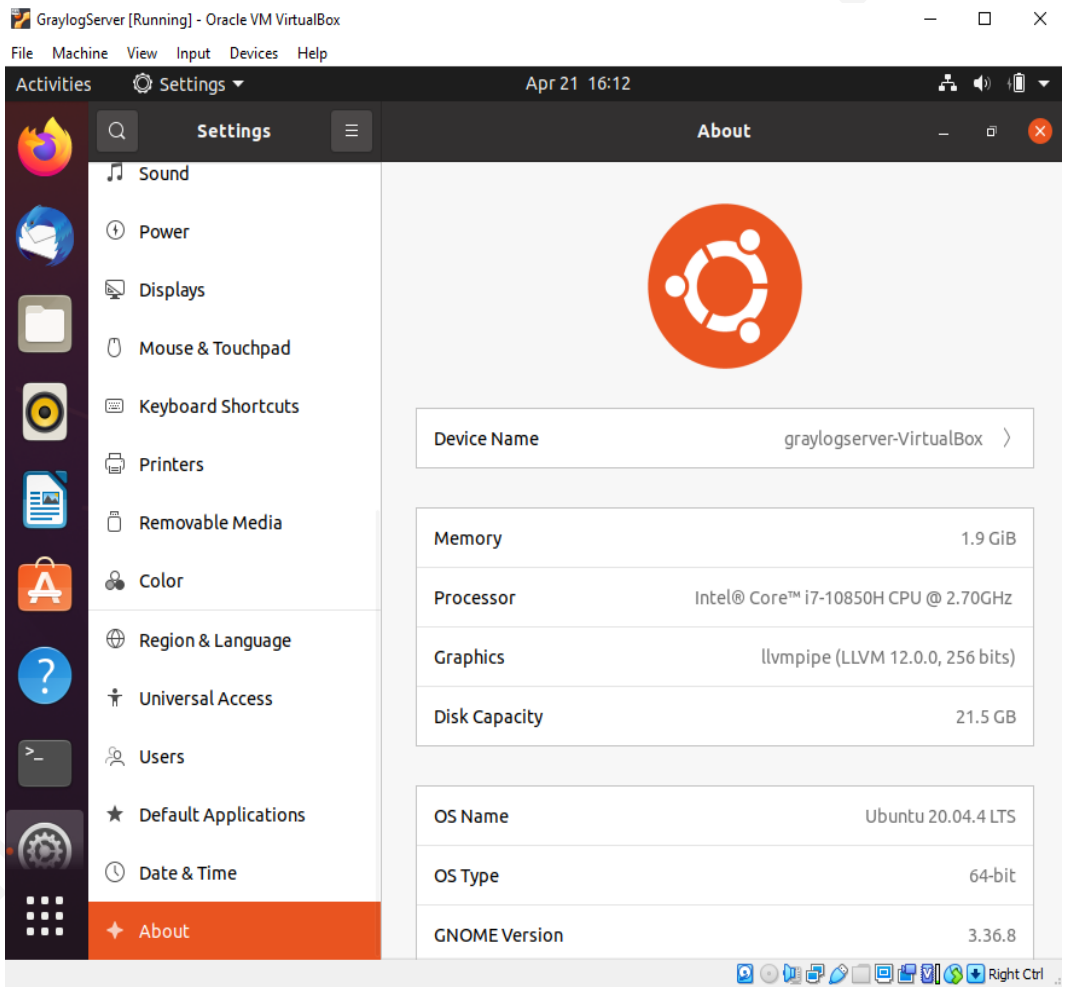
9	DeadBoltRansomware	https://samples.vx-underground.org/samples/Families/DeadBoltRansomware/Samples/444e537f86cbeeea5a4fcf94c485cc9d286de0ccd91718362cecf415bf362bcf.7z
10	DearCryRansomware	https://samples.vx-underground.org/samples/Families/DearCryRansomware/0e55ead3b8fd305d9a54f78c7b56741a.7z
11	DecafRansomware	https://samples.vx-underground.org/samples/Families/DecafRansomware/5da2a2ebe9959e6ac21683a8950055309eb34544962c02ed564e0deaf83c9477.7z
12	DiavolRansomware	https://samples.vx-underground.org/samples/Families/DiavolRansomware/Samples/ee13d59ae3601c948bd10560188447e6faaeef5336dcd605b52ee558ff2a8588.7z
13	EvilNominatusRansomware	https://samples.vx-underground.org/samples/Families/EvilNominatusRansomware/Samples/1ee21714bde9bf89cc6c55d7dac5686ad0e85f231c2ba7f91d575cb6a1f8092e.7z
14	HaronRansomware	https://samples.vx-underground.org/samples/Families/HaronRansomware/dedad693898bba0e4964e6c9a749d380.7z
15	HiveRansomware	https://samples.vx-underground.org/samples/Families/HiveRansomware/v5.1/win/aa78798172e873d88f42bf8bb5853aecfb74a3bf8980540f6be66f800bf1f153.7z
16	KoxicRansomware	https://samples.vx-underground.org/samples/Families/KoxicRansomware/Samples/699159e695e230a48d94b6103b48940ed596d0b48fb6d936c04d86eed539cecd.7z
17	KrusRansomware	https://samples.vx-underground.org/samples/Families/KrusRansomware/Samples/df109084e55980239d6d39a3a52afc372f5251653a3893497e3017e65c65e2a3.7z
18	LockBitRansomware	https://samples.vx-underground.org/samples/Families/LockBitRanso

		mware/Samples/fc720ba95ab46e6a5f9fd7f6b1f240cd9b29cd96f6cb075f0459fac230f7de94.7z
19	LockyRansomware	https://samples.vx-underground.org/samples/Families/LockyRansomware/E7AAD826559C8448CD8BA9F53F401182.7z
20	LokiLockerRansomware	https://samples.vx-underground.org/samples/Families/LokiLockerRansomware/Samples/4215b5ce91deb97011cba2dd94d5bac1a745d6d55f6938b86e209eaaf8e655df.7z
21	LorenzRansomware	https://samples.vx-underground.org/samples/Families/LorenzRansomware/Samples/Encryptor/edc2070fd8116f1df5c8d419189331ec606d10062818c5f3de865cd0f7d6db84.7z
22	MagniberRansomware	https://samples.vx-underground.org/samples/Families/MagniberRansomware/Samples/e2d3af7acd9bb440f9972b192cbfa83b07abdbb042f8bf1c2bb8f63944a4ae39.7z
23	MementoRansomware	https://samples.vx-underground.org/samples/Families/MementoRansomware/Samples/09a0caadc4df3d4278368f94f52007894c2b51d3785d985cb8e42646e8a33b68.7z
24	MidasRansomware	https://samples.vx-underground.org/samples/Families/MidasRansomware/Samples/4823f478e5fb68be06ba987539c3e1c52e2597b0b35edc5b66fcedcef66fb1f6.7z
25	NightSkyRansomware	https://samples.vx-underground.org/samples/Families/NightSkyRansomware/Samples/1fca1cd04992e0fcaa714d9dfa97323d81d7e3d43a024ec37d1c7a2767a17577.7z
26	NokoyawaRansomware	https://samples.vx-underground.org/samples/Families/NokoyawaRansomware/Samples/86953a6ce9fb7bf8b7791b9c6b751120c35ee1df5590ba4ff447e21c29259e51.7z
27	OnyxRansomware	https://samples.vx-underground.org/samples/Families/OnyxRansomw

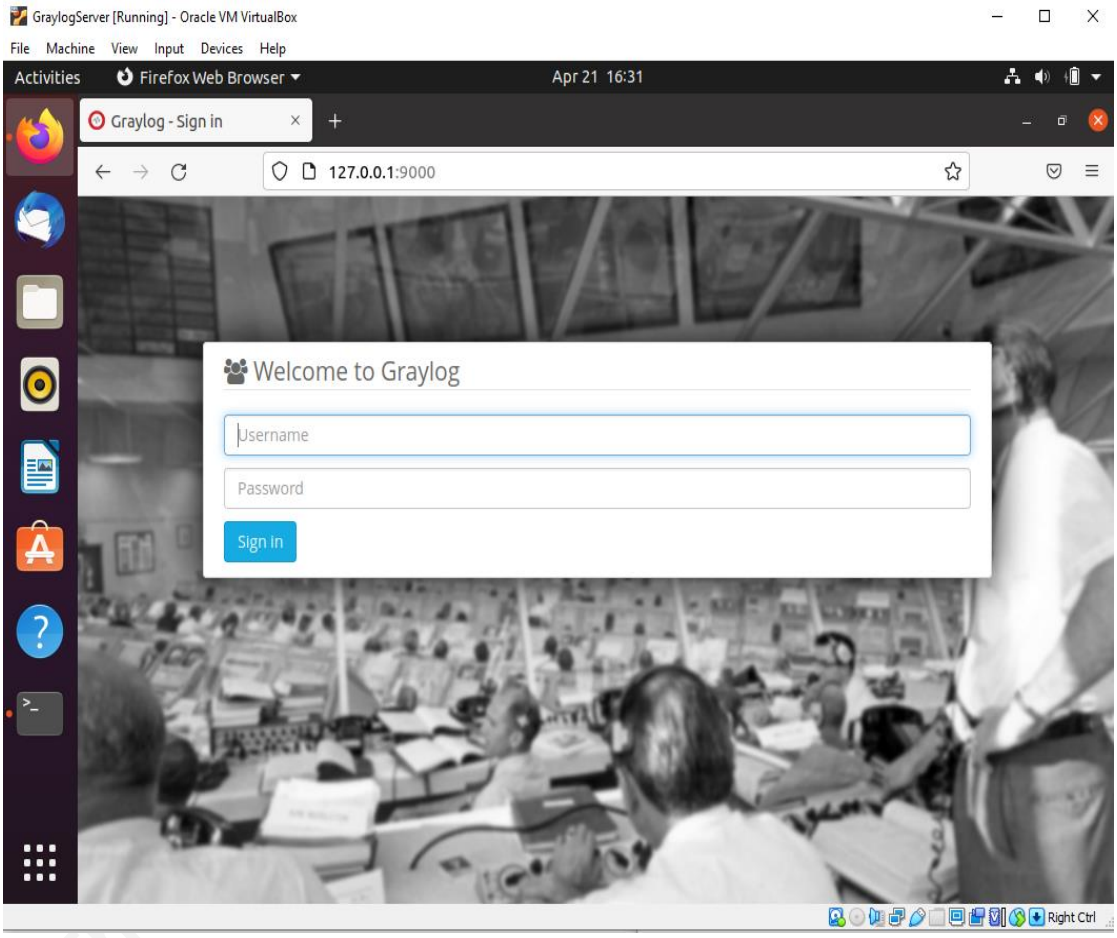
		are/Samples/a7f09cfde433f3d47fc96502bf2b623ae5e7626da85d0a0130dcd19d1679af9b.7z
28	PandoraRansomware	https://samples.vx-underground.org/samples/Families/PandoraRansomware/Samples/5b56c5d86347e164c6e571c86dbf5b1535eae6b979fede6ed66b01e79ea33b7b.7z
29	PhobosRansomware	https://samples.vx-underground.org/samples/Families/PhobosRansomware/a91491f45b851a07f91ba5a200967921bf796d38677786de51a4a8fe5ddeafd2.7z
30	RansomExx	https://samples.vx-underground.org/samples/Families/RansomExx/fe564fb38a99dbb94cc8a66d8955b0b7f8e67bf0a5eb820c4a5d0c3efb96c1e5.7z
31	RookRansomware	https://samples.vx-underground.org/samples/Families/RookRansomware/Samples/96f7df1c984c1753289600f7f373f3a98a4f09f82acc1be8ecfd5790763a355b.7z
32	SFileRansomware	https://samples.vx-underground.org/samples/Families/SFileRansomware/win/feddee093d72838ac1f13ea9bbfc0473e2f3df1495432d6f95d6fe8ddf7ff09b.7z
33	SamsamRansomware	https://samples.vx-underground.org/samples/Families/SamsamRansomware/FFA28DB79DACA3B93A283CE2A6FF24791956A768CB5FC791C075B638416B51F4.7z
34	SugarRansomware	https://samples.vx-underground.org/samples/Families/SugarRansomware/Samples/0f05b893b67c4fc8680f2040b4069eba81e144253a7f6e20507eaa4d2576461d.7z
35	SynAckRansomware	https://samples.vx-underground.org/samples/Families/SynAckRansomware/5b9dee21841e1b6fd1477008b73729a0.7z
36	WhiteRabbitRansomware	https://samples.vx-underground.org/samples/Families/WhiteRabbitRansomware/Samples/03e8b29ad5055f1dda1b0e9353dc2c1421974eb3d0a115d0bb35c7d76f50de20.7z

37	YanluowangRansomware	https://samples.vx-underground.org/samples/Families/YanluowangRansomware/d11793433065633b84567de403c1989640a07c9a399dd2753aaf118891ce791c.7z

Appendix C

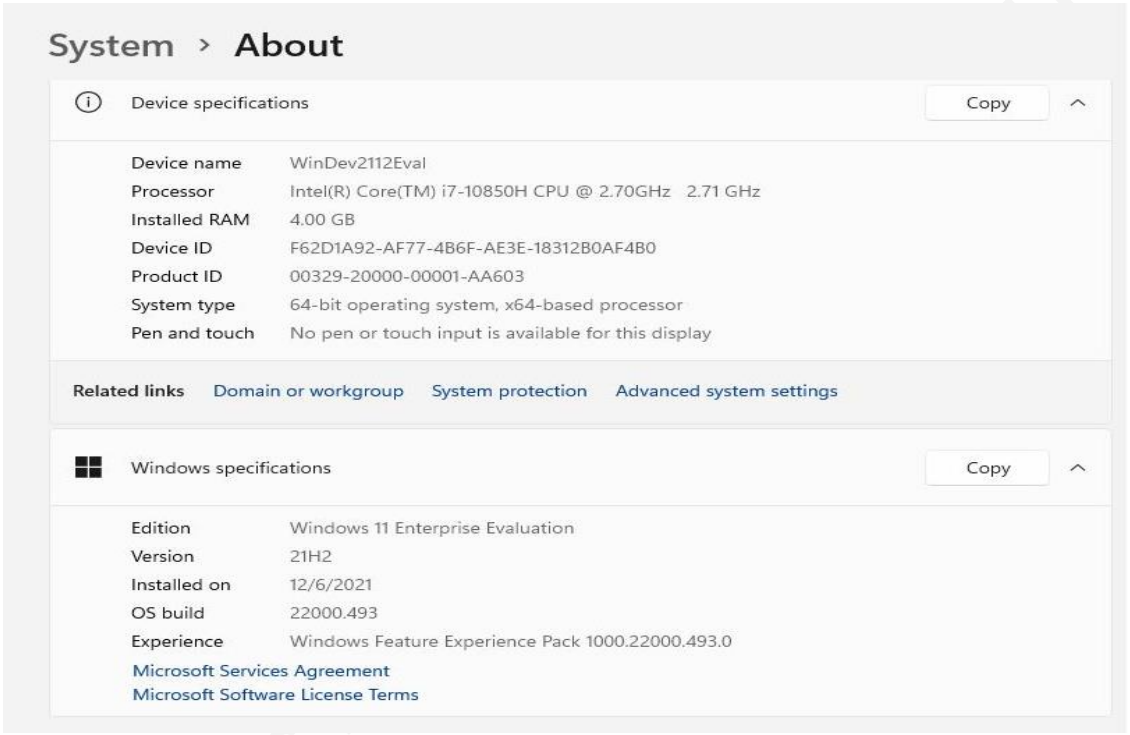


GrayLog Server Setup



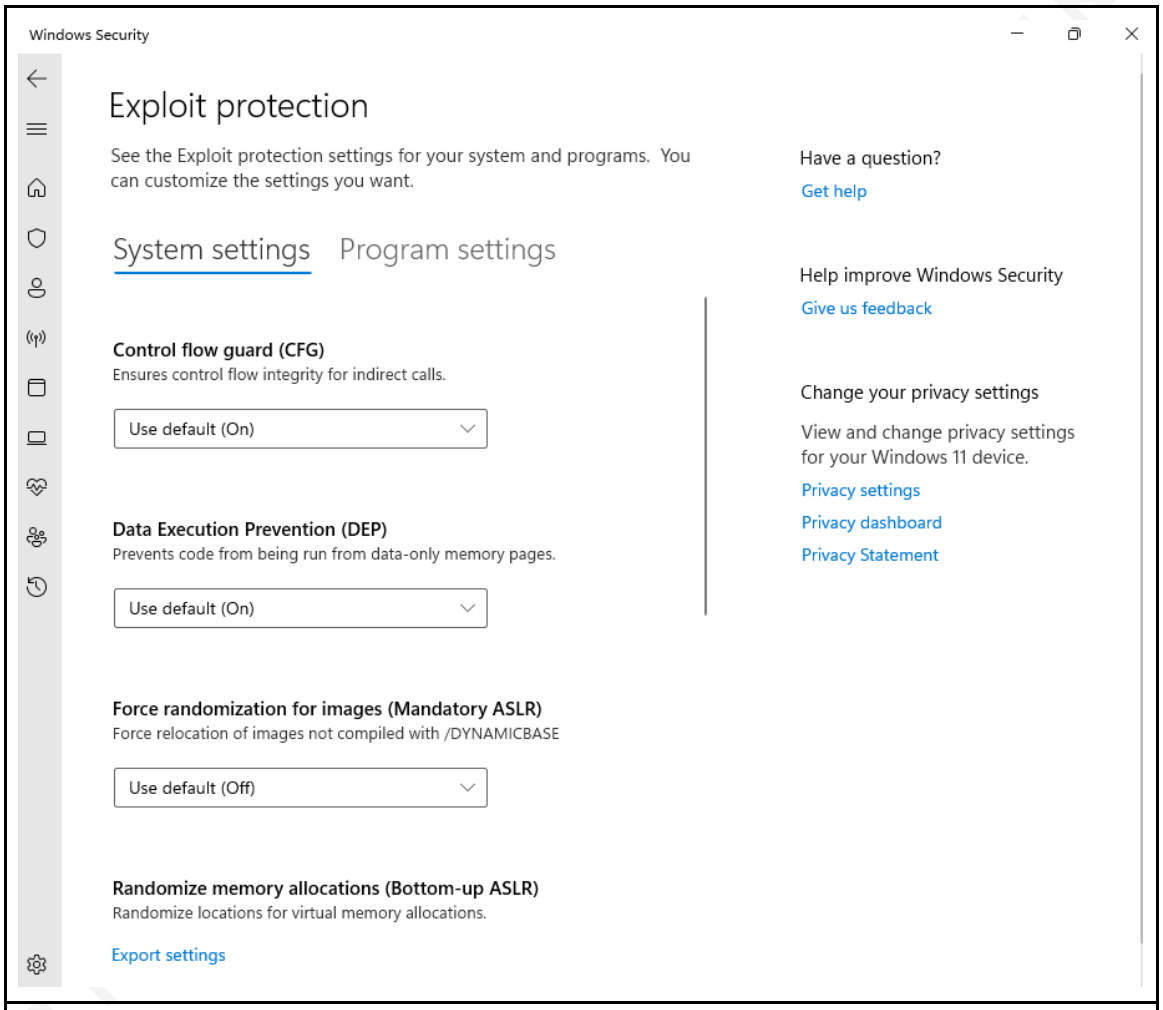
GrayLog Server Web Interface

Perumal P S, perumal316@gmail.com

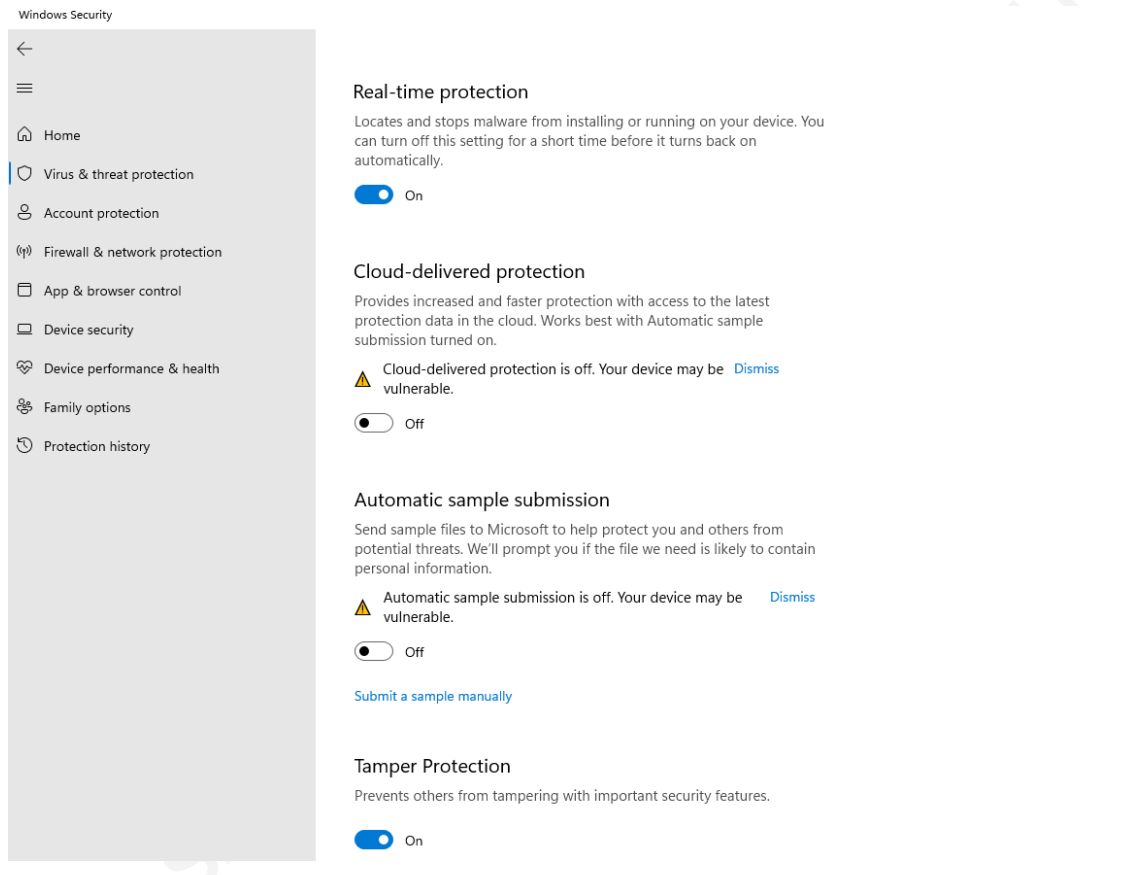


Windows 11 Version

Microsoft Defender Version



Windows Exploit Protection Settings



Microsoft Defender Settings