Lab setup for investigating Storm-1567 threat actor malware

by Boluwarin Oladipo

I. LAB SETUP

This paper seeks to detail a lab setup to analyse malware and the malware analysis software tools installed to analyse malware utilized by the threat group Storm-1567. Existing publicly available analysis labs will be explored, the software tools as well as the best practices followed by these labs. Analysis of the behaviour of the Akira ransomware utilized by threat actor tracked as Storm-1567 was also conducted by consulting publications that have analysed them.

A malware sandbox is an isolated system that is used for dynamic analysis of malware samples. As the malware is executed within the sandbox, artefacts such as logs, process threads and network activity are monitored and collected to determine the functionality of the malware[1]. The Storm-1567 threat actor as tracked by Microsoft Threat Intelligence uses the Akira ransomware for their campaigns [2].

Ransomware is malware that encrypts a target individual or organization's systems with the aim of extortion for restoration of the data. Threat actors that use the Akira ransomware have been discovered to use a double extortion technique, extracting the data, deleting any backups from the infected machines and exfiltrating the data before encrypting it and demanding ransoms in exchange for decrypting the machines and not publishing the exfiltrated data on the web [3], [4].

The rest of the paper is organized as follows:

- Analysis of existing Sandboxes
- Lab setup
- Software tools installed
- Lab testing
- Identification of malware
- Analysis of malware
- Conclusions

A. *Analysis of existing sandboxes*

The sandboxes that will be analysed are listed below:

- **ANY.RUN Community Edition**: This is a free cloud- based malware sandbox. Malware samples may be uploaded via URL or file upload. The paid version of the ANY.RUN platform supports the Windows and Linux operating systems for running malware samples for a minimum of 60 seconds and a maximum of 11 minutes[5]. The tools available include process execution graphs showing the processes modified by the malware's execution, CPU, network and memory monitoring tools which can all be interacted with as the malware is executing. Reports using the MITRE ATT&CK framework are also generated after execution. Malware samples will also be run against public analysis of similar samples to provide more a more detailed report.
- **FlareVM**: This is a collection of free Powershell software installation scripts that enable management of a malware analysis environment on a Windows virtual machine. It is an open-source project maintained by security firm Mandiant. FlareVM leverages Chocolatey and Boxstarter to create repeatable scripted Windows environments for malware analysis by managing the software tools for analysis. [6]. Being a downloadable sandbox, an analyst may allocate system resources as required, making it more customizable than the online sandboxes. Software tools such as Yara, Wireshark, IDA Pro and x64dbg can be installed during initial setup. [7]
- **Joe Sandbox Cloud Basic**: This is a free cloud-based malware sandbox. Joe Sandbox offers the Windows, MacOS, Android and Linux operating systems for malware analysis.[8] Joe Sandbox is similar to ANY.RUN in its offered features except that Joe Sandbox allows the option of usage of physical machines as opposed to virtual machines to combat the behaviour of certain adaptive malware. [5]
- **RemNUX**: This is a downloadable open-source malware sandbox based on the Ubuntu distribution of the Linux operating system. RemNUX leverages SaltStack to automate the management and installation of the main components of the distribution [9]. RemNUX can be installed as a stand-alone Linux virtual appliance that can be run on a hypervisor, a command line interface or a Docker container. RemNUX may also be installed from scratch on an Ubuntu virtual machine to enable further customization[10]. Software tools available on RemNUX include cabextract [11], ProcDOT [12] , Ghidra [13] and exiftool [14].
- **Cuckoo**: This is a portable automated open-source malware analysis system. It is distributed as a set of Python libraries and can be installed with the Python Package Index (pip). [15], [16]. Software tools available on Cuckoo perform functions such as LibVirt for target virtual machine management, ProcMon for process monitoring, Volatility for memory dumping, and tcpdump for network monitoring. These tools collect various artefacts generated by execution of a malware sample within isolated operating systems managed by Cuckoo and generate comprehensive analyses of the artefacts. The libraries can be customized to run specific analysis on the artefacts. Cuckoo has been found

to be more modular and customizable in comparison to most other downloadable sandboxes due to its robust documentation and extensible libraries. [16]

B. *Virtual machine setup*

For the lab setup to analyse the Akira ransomware, a target machine running the malware and an analysis machine to observe the execution of the malware were set up on an isolated virtual network. A diagram of the lab setup is shown in Fig. 1. Details of the target and analysis machines are given Table 1 below:

TABLE I. TARGET MACHINE DETAILS

Category	Details	Justification
Hypervisor	Oracle VirtualBox 7.0.14 r161095 (Qt5.15.2)	VirtualBox is an easy-to-use hypervisor preferred over other hypervisors mainly because of its simplicity but also ability to create snapshots and an internal network configuration mode to aid a malware analyst.
Operating System	Windows 10 (Version: 22H2, Build number: 19045)	Windows 10 is a desktop operating system used by many enterprises globally. It was preferred to the newer Windows 11 due to its prevailing market share even though it is due to reach end-of-life in October 2025 [17], [18].
RAM	4 Gigabytes	This amount of allocated memory ensures smooth operation of the operating system, installed programs and running the malware.
CPU cores	1	Due to constraints of the host machine only possessing 2 CPU cores, 1 core had to be allocated to the target machine.
Disk space	50 Gigabytes	This amount of space ensures enough space to store the operating system files, installed programs, the malware sample and also prevent any potential detection from the malware code that it is being run in a virtualized environment
Network Settings	IP address – 192.168.56.50 Gateway/DNS – 192.168.56.1 Internal network	An internal network with a subnet mask of 255.255.255.0 was configured to ensure no traffic flows outside both virtual machines to prevent potential infection of the host or other machines on the network the host is on.
Isolation settings	Shared clipboard and folders disabled	The VirtualBox Guest Additions extension package was disabled.
Programs installed	Adobe Acrobat Reader Microsoft Office LTSC 2021 Google Chrome Mozilla Firefox	The installed programs will be typically found on an enterprise system and the effect of the malware will be analysed on these programs.
Snapshot configuration	Snapshot taken when OS and all programs were installed.	Snapshots of the system with all programs installed were taken to enable quick restoration after analysis.

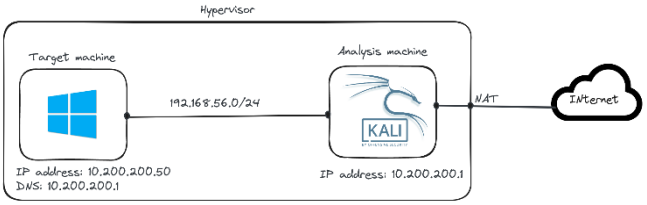

Fig. 1. Virtual machine setup

C. *Lab Testing*

To ensure the security of the lab environment, the below testing activities detailed below were carried out:

- **Network Isolation**: This activity ensures that the lab network is isolated from any external network where the malware under analysis might be able to infect other machines. To ensure this, a private IP subnet range **10.200.200.0/24** was used to connect the analysis and target machines. Attempts were made to ping the host machine from the target machine to ensure there was no communication possible. The IP address was also hard coded into the target machine's network interface settings with the gateway resolving to the analysis machine as an extra step. Fig. x below shows the ping attempts from the target to the analysis machine.

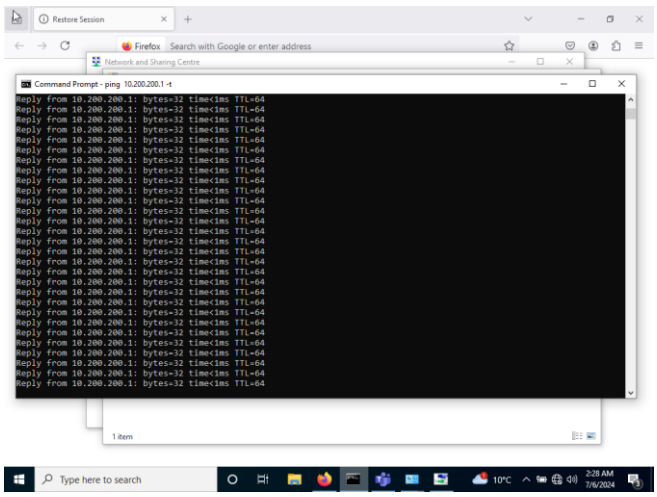

Fig. 2. Successful ping attempt from the target machine to the analysis machine

TABLE II. SOFTWARE TOOLS

Tool	Category	Description	Alternative Tool	Justification
IDA Free	Static analysis	This is a reverse engineering used translate binary code into assembly language, helping malware analysts analyse suspicious executables. [19]	Ghidra	IDA is an industry standard tool as well as a debugger in addition to a robust feature set that allows for customization. IDA requires a fairly expensive license to unlock a large part of the feature set. [20]
Strings	Static analysis	This is a Linux system utility used for extracting readable text within given non-text files. [21]	Hexdump	Strings is available on the Linux command line and can extract ASCII strings from
Yara	Static analysis	This is a pattern-matching tool used for identifying and classifying malware using text or binary identifiers written into shareable rules.[22]	Sigma	Yara focuses mainly on file-based threats as opposed to Sigma which focus on log events or databases utilising written yara rules for detection of malware.
RootKitBuster	Dynamic analysis	This is a rootkit detector that scans for hidden system files, registry entries, driver and processes on a target suspected to be compromised with a rootkit.	RootKitRevealer	RootKitBuster is developed by security company Trend Micro and is more recently updated than the alternative tool RootKitRevealer in the sysinternals suite.
Process Monitor	Dynamic analysis	This is a monitoring tool as part of the Sysinternals suite for Windows that shows real time file system, Registry and process activity, logging the output to a file.[23]	Process Explorer, Process Hacker	Process Monitor is the most lightweight tool enabling quick dynamic analysis and detailed event logging without a great impact on system resources in relation to the alternatives.
Wireshark	Network analysis	This is a network packet analysis tool used to analyse data contained in a network packet such as protocols used for determining the network activity of suspected malicious programs	Fakenet-NG	Wireshark operates transparently on network interfaces, allowing uninterrupted network traffic capture without altering the environment unlike Fakenet-NG.
PEstudio	Dynamic analysis	This is a Windows-based tool used for detecting and analysing the signatures and characteristics of executable files to identify packers, encryptors, and compilers.	PE Bear	In addition to packer detection, PE studio tries to identify an executable as malicious or not based on the indicators found during analysis.
Volatility	Dynamic analysis	Volatility is an open-source memory forensics framework used to analyse volatile memory dumps [24].	FTK Imager	Volatility is free and open source and is cheaper to use than the alternatives. One significant drawback of Volatility is that it only analyses and cannot capture memory dumps.

- **Virtual machine network settings**: This activity ensures the correct settings are applied to lab machines to ensure no unintentional interaction with the host network or the internet. To ensure this, the network interface of the target machine is set to **Internal network** mode.
- **Backup and recovery**: This activity ensures the entire lab environment is easily recoverable in case of a catastrophic failure. The virtual hard disk files of the target and analysis machines were backed up to an external drive to complete this activity.
- **Snapshots**: This activity ensures the target machine is easily restored easily and quickly when compromised by malware. To achieve this, snapshots are taken before the malware is run.
- **Patch Management:** This activity ensures the operating system; software tools and user programs remain up to date to properly analyse the effect of the malware. This is done by running update operations on valid snapshots of the virtual machines before running the malware.

D. Software Tools

The software tools utilised within the lab environment are listed, categorised and their selection justified in Table II below:

II. MALWARE ANALYSIS

Storm-1567 is a code name used by Microsoft to track a threat actor utilizing the Akira ransomware [2]. Security vendor Sophos published an article [25] describing the capabilities and behaviour of the malware when responding to reports from their North American customers in April 2023. Avast Threat Labs released a decryptor for systems affected by the malware shortly after it was first discovered. [26]

A. Identification

- File Type: The akira ransomware is a 32-bit Windows portable executable file.
- File Name: akira.exe; win_locker.exe [27], [28]
- File Size: 606 Kilobytes
- Hashes: f526a8ea744a8c5051deefbf2c6010af (MD5); 8bfa4c2c1065b105ec80a86f460e0e0221b39610109cc6cd4b441dd86e6b4aef (SHA-256); d4f6241abe5f46e6b18f10da95d004924eac4ed3 (SHA-1) [28].
- Malware Names: The ransomware is detected by major anti-virus engines under the following names: Win.Ransomware.Akira (Avast and AVG); Troj/Akira-A (Sophos); Ransom:Win32/Akira.A!ibt (Microsoft) [28].
- Anti-Virus Detection Capabilities: It is currently detected by 58 of 74 anti-virus engines on VirusTotal [28],
- First created: 29th July 2023 [28].

B. Analysis

The Akira threat actors such as Storm-1567 have been noted to employ double extortion techniques by exfiltrating the data found on the target system before deployment of the ransomware [29]. The capabilities, behaviour and recommendations for mitigation of the malware will be detailed below:

- **Initial Access**: At these stages of the kill chain, detection is extremely hard due to the lack of distinction between legitimate and malicious traffic and is usually detected after the fact. Demboski [30] and Bello Vieda [31] reported the most common mode of access was compromise of CVE 2023-20269 [32], a vulnerability in Cisco virtual private network software without multi factor authentication enabled, used by the target organizations. It is likely the threat actors will survey target organizations that use this. Organizations should enforce multi-factor authentication for all users on their network to mitigate the risk at these stages.
- **Exploitation**: At this stage of the kill chain, the threat actors will attempt to use the vulnerabilities found in the initial stages to gain access to the target system. Demboski [30] reports that the threat actors utilize credential theft techniques to obtain credentials and move laterally within a corporate network. Credentials are obtained using data dumps from the Local Security Authority Subsystem Service (LSASS) running in memory [29], [30]. The actors then leveraged this access to move laterally through the network stealing cached browser credentials and using remote desktop software such as AnyDesk to gain access to other systems. Organizations may install host-based intrusion detection systems on every endpoint within the network and disable remote desktop access to endpoints that do not require it.
- **Installation:** The malware runs by encrypting all files on a target except system files and the ransom note that is dropped. It then deletes all the shadow copies created on the disk to ensure that immediate recovery using the Windows recovery tool is not possible. If a file is bigger than 2 megabytes, it is split into blocks which are partially encrypted to render the file unusable while encrypting more files per time. If the indicators of compromise are detected on any endpoint, the endpoint should be immediately isolated to prevent further spread. See the appendix for a table of the indicators of compromise.
- **Command and Control:** The actors utilize the access gained at this stage to continue spread the malware using remote desktop software such as AnyDesk. The actors attempt to steal more relevant credentials with each endpoint they access. Vulnerability management should be regularly done within an organization's systems to prevent unrestricted lateral movement [33].
- **Actions on Objectives**: The actors may carry out their objectives at this stage by exfiltrating stolen data in archives using file transfer tools. Anomalous network activity far over baseline values should be flagged and analysed to minimize the damage done.

C. Conclusion and Recommendations

This paper details a lab setup for analyzing malware, specifically focusing on tools and best practices used by the threat group Storm-1567, which employs Akira ransomware. The setup involves malware sandboxes like ANY.RUN, FlareVM, Joe Sandbox, RemNUX, and Cuckoo, each offering various features for dynamic malware analysis. The lab setup includes a target machine with specific configurations to run the malware and an analysis machine to monitor its behavior, ensuring network isolation and backup procedures for security. Software tools like IDA Free, Strings, Yara, and Wireshark are utilized for static and dynamic analysis. Akira ransomware, a 32-bit Windows executable, employs double extortion by encrypting files and exfiltrating data, targeting systems via vulnerabilities and credential theft. The paper concludes with recommendations for mitigating these attacks through network security measures and endpoint protection.

It is recommended that organizations implement multi-factor authentication as well as a comprehensive patch management program to mitigate the risks posed by the ransomware. It is also recommended for organizations to utilise off-site cold backups to ensure that restoration is possible in the worst case scenario.

If the malware were to be analysed:

- The malware sample will be downloaded in a password-protected archive file directly on to the target machine.
- All other target machine network interfaces except the internal network interface will be turned off completely.
- The anti-virus software on the target machine will be disabled.
- A snapshot of the machine will be taken prior to executing the malware for analysis.
- The malware will be statically analysed with strings and IDA to view the readable strings and executable code.
- Updates will be disabled completely for the duration of the analysis.

APPENDIX

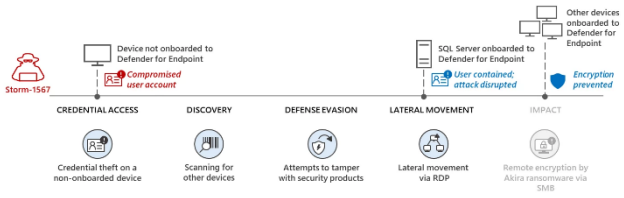

Fig. 3. Storm-1567 process [2]

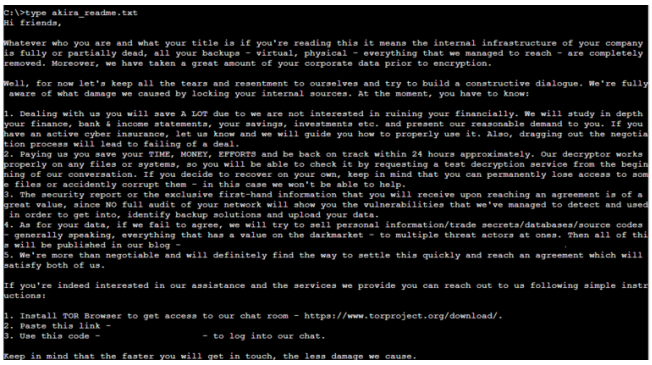

Fig. 4. Sample ransom note after the akira ransomware has been run [31]

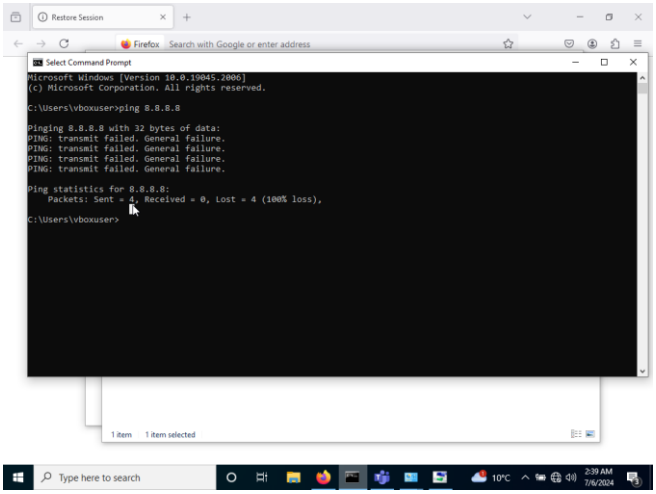

Fig. 5. Attempt to ping Google DNS server 8.8.8.8 from target machine when internal network mode is enabled

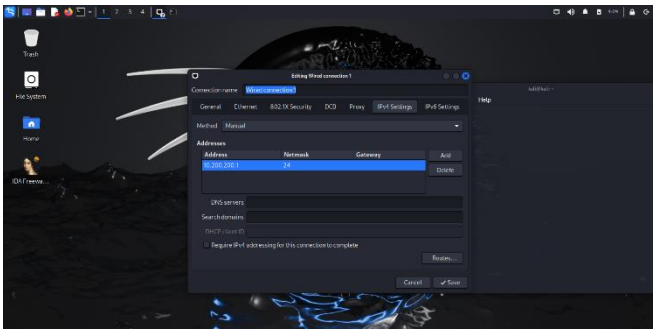

Fig. 6. IPv4 configuration details on analysis machine

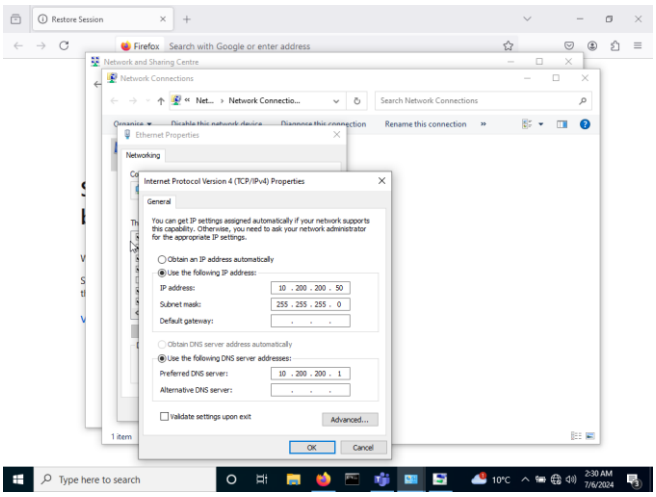

Fig. 7. IPv4 configuration details on target machine

TABLE III. INDICATORS OF COMPROMISE

Indicator	Indicator Type	Context
*.akira	File Name	Appendage to filenames left after encryption is complete
akira_readme.txt	File Name	Name of text file left after encryption
Log-<Day>-<Month>-<Year>-<Hour>-	File Name	Name of log file left after encryption

<Minute>-<Second>.txt		
powershell.exe -Command "Get-WmiObject Win32_Shadowcopy | Remove-WmiObject"	Process Name	Powershell command for removing shadow copy objects, used to remove potential backup files

Fig. 8. Indicators of compromise[31]

REFERENCES

[1] Kaspersky, "Sandbox | Kaspersky." Accessed: Jun. 24, 2024. [Online]. Available: https://www.kaspersky.com/enterprise-security/wiki-section/products/sandbox

[2] Microsoft Threat Intelligence, "Automatic disruption of human-operated attacks through containment of compromised user accounts | Microsoft Security Blog." Accessed: Jun. 11, 2024. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2023/10/11/automatic-disruption-of-human-operated-attacks-through-containment-of-compromised-user-accounts/

[3] Cybersecurity and Infrastructure Security Agency, "#StopRansomware: Akira Ransomware | CISA." Accessed: Jun. 14, 2024. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a

[4] HelpRansomware, "Akira Ransomware: How To Recover Files Safely." Accessed: Jun. 18, 2024. [Online]. Available: https://helpransomware.com/akira-ransomware/

[5] C. Pernet, "ANY.RUN vs Joe Sandbox | Malware Analysis Tool Comparison | TechRepublic," ANY.RUN vs Joe Sandbox | Malware Analysis Tool Comparison | TechRepublic. Accessed: Jun. 25, 2024. [Online]. Available: https://www.techrepublic.com/article/anyrun-vs-joe-sandbox/

[6] M. Wrock and Boxstarter, "Boxstarter | Why Boxstarter?," Boxstarter | Why Boxstarter? Accessed: Jun. 26, 2024. [Online]. Available: https://boxstarter.org/whyboxstarter

[7] Mandiant, "VM-Packages/packages at main · mandiant/VM-Packages · GitHub," VM-Packages/packages at main · mandiant/VM-Packages · GitHub. Accessed: Jun. 26, 2024. [Online]. Available: https://github.com/mandiant/VM-Packages/tree/main/packages

[8] Joe Sandbox, "https://www.joesandbox.com/#windows," Automated Malware Analysis - Joe Sandbox Cloud Basic. Accessed: Jun. 26, 2024. [Online]. Available: https://www.joesandbox.com/#windows

[9] RemNUX, "Technologies | REMnux Documentation," Technologies | REMnux Documentation. Accessed: Jun. 27, 2024. [Online]. Available: https://docs.remnux.org/behind-the-scenes/technologies

[10] RemNUX, "REMnux: A Linux Toolkit for Malware Analysis | REMnux Documentation," REMnux: A Linux Toolkit for Malware Analysis | REMnux Documentation. Accessed: Jun. 27, 2024. [Online]. Available: https://docs.remnux.org/

[11] S. Caie, M. Russotto, and D. Tritscher, "cabextract," cabextract. Accessed: Jun. 27, 2024. [Online]. Available: https://www.cabextract.org.uk/

[12] C. Wojner, "ProcDOT's Home," ProcDOT's Home. Accessed: Jun. 27, 2024. [Online]. Available: https://www.procdot.com/

[13] National Security Agency, "Ghidra," Ghidra. Accessed: Jun. 27, 2024. [Online]. Available: https://ghidra-sre.org/

[14] P. Harvey, "ExifTool by Phil Harvey," ExifTool by Phil Harvey. Accessed: Jun. 27, 2024. [Online]. Available: https://exiftool.org/

[15] Cuckoo Foundation, "Installing Cuckoo — Cuckoo Sandbox v2.0.7 Book." Accessed: Jul. 01, 2024. [Online]. Available: https://cuckoo.readthedocs.io/en/latest/installation/host/installation/

[16] Cuckoo Foundation, "What is Cuckoo? — Cuckoo Sandbox v2.0.7 Book." Accessed: Jun. 26, 2024. [Online]. Available: https://cuckoo.readthedocs.io/en/latest/introduction/what/

[17] S. Endicott, "Windows 10 still has more than double the market share of Windows 11, and that doesn't look like it will change any time soon | Windows Central." Accessed: Jun. 14, 2024. [Online]. Available: https://www.windowscentral.com/software-apps/windows-11/windows-10-still-has-more-than-double-the-market-share-of-windows-11-and-that-doesnt-look-like-it-will-change-any-time-soon

[18] Microsoft, "Windows 10 Home and Pro - Microsoft Lifecycle | Microsoft Learn." Accessed: Jul. 05, 2024. [Online]. Available: https://learn.microsoft.com/en-us/lifecycle/products/windows-10-home-and-pro

[19] Hex Rays, "IDA Free." Accessed: Jul. 05, 2024. [Online]. Available: https://hex-rays.com/ida-free/

[20] Omkar Bhat, Z. Yeprem, and V. Lingesh, "Comparison of 3 Reverse Engineering Tools," 2019, doi: 10.13140/RG.2.2.35123.07203.

[21] Free Software Foundation, "strings(1) - Linux man page." Accessed: Jul. 06, 2024. [Online]. Available: https://linux.die.net/man/1/strings

[22] V. M. Alvarez, "YARA - The pattern matching swiss knife for malware researchers." Accessed: Jul. 06, 2024. [Online]. Available: https://virustotal.github.io/yara/

[23] M. Russinovich, "Process Monitor - Sysinternals | Microsoft Learn." Accessed: Jul. 06, 2024. [Online]. Available: https://learn.microsoft.com/en-us/sysinternals/downloads/procmon

[24] Volatility Foundation, "GitHub - volatilityfoundation/volatility: An advanced memory forensics framework." Accessed: Jul. 06, 2024. [Online]. Available: https://github.com/volatilityfoundation/volatility

[25] P. Jaramilo, "Akira Ransomware is "bringin' 1988 back" – Sophos News." Accessed: Jun. 14, 2024. [Online]. Available: https://news.sophos.com/en-us/2023/05/09/akira-ransomware-is-bringin-88-back/

[26] Avast Threat Labs, "Decrypted: Akira Ransomware - Avast Threat Labs," Decrypted: Akira Ransomware - Avast Threat Labs. Accessed: Jun. 14, 2024. [Online]. Available: https://decoded.avast.io/threatresearch/decrypted-akira-ransomware/

[27] "VirusTotal report for win_locker.exe." Accessed: Jul. 03, 2024. [Online]. Available: https://vtbehaviour.commondatastorage.googleapis.com/8bfa4c2c1065b105ec80a86f460e0e0221b39610109cc6cd4b441dd86e6b4aef_Zenbox.html?GoogleAccessId=758681729565-rc7fgq07icj8c9dm2gi34a4cckv235v1@developer.gserviceaccount.com&Expires=1720013106&Signature=AeGgZqsDWZd15pI7jj5NO1KIOo4LWncp%2Fu7sFiDH9a%2FR0Dh2Gk63S55v3MXLpPA4zEpEI9BHMRNauaY10jQ1mbWl1MzKrFBppZQ7qaAc10SLLclTujRXxNWfeI1D7mIrd7xdh8Lm%2FTol8bdMINJbR12xypjVxLk5Qt1HdnCFEcrkhAIlNFAJiroKeAGQtNq%2BSpprwdPb09hfk4gCayyt02RHAyukQSMXBkwc5VpCXANMgw4Gtxami%2F8tEBUyYeAP3LiW2%2FziqNaCsC%2B6Bg5S%2ForZZTlo7Nbj8FB3ogPm75N8n2A419%2B5Qs2MZSEjBXXXGINBZ8%2BFLhHfJlGnmvyUcw%3D%3D&response-content-type=text%2Fhtml;

[28] "VirusTotal - File - 8bfa4c2c1065b105ec80a86f460e0e0221b39610109cc6cd4b441dd86e6b4aef." Accessed: Jul. 03, 2024. [Online]. Available: https://www.virustotal.com/gui/file/8bfa4c2c1065b105ec80a86f460e0e0221b39610109cc6cd4b441dd86e6b4aef/behavior

[29] M. Kersten and A. Mundo, "Akira Ransomware." Accessed: Jun. 12, 2024. [Online]. Available: https://www.trellix.com/blogs/research/akira-ransomware/

[30] M. Demboski, "Akira, again: The ransomware that keeps on taking – Sophos News." Accessed: Jun. 14, 2024. [Online]. Available: https://news.sophos.com/en-us/2023/12/21/akira-again-the-ransomware-that-keeps-on-taking/

[31] Jaime Andres Bello Vieda, "A spotlight on Akira ransomware from X-Force Incident Response and Threat Intelligence." Accessed: Jun. 11, 2024. [Online]. Available: https://securityintelligence.com/x-force/spotlight-akira-ransomware-x-force/

[32] "NVD - CVE-2023-20269." Accessed: Jul. 07, 2024. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2023-20269

[33] M. Souppaya and K. Scarfone, "Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology," National Institute of Standards and Technology, Nov. 2021. doi: 10.6028/NIST.SP.800-40r4-draft.