MALWARE ANALYSIS

AKIRA RANSOMWARE

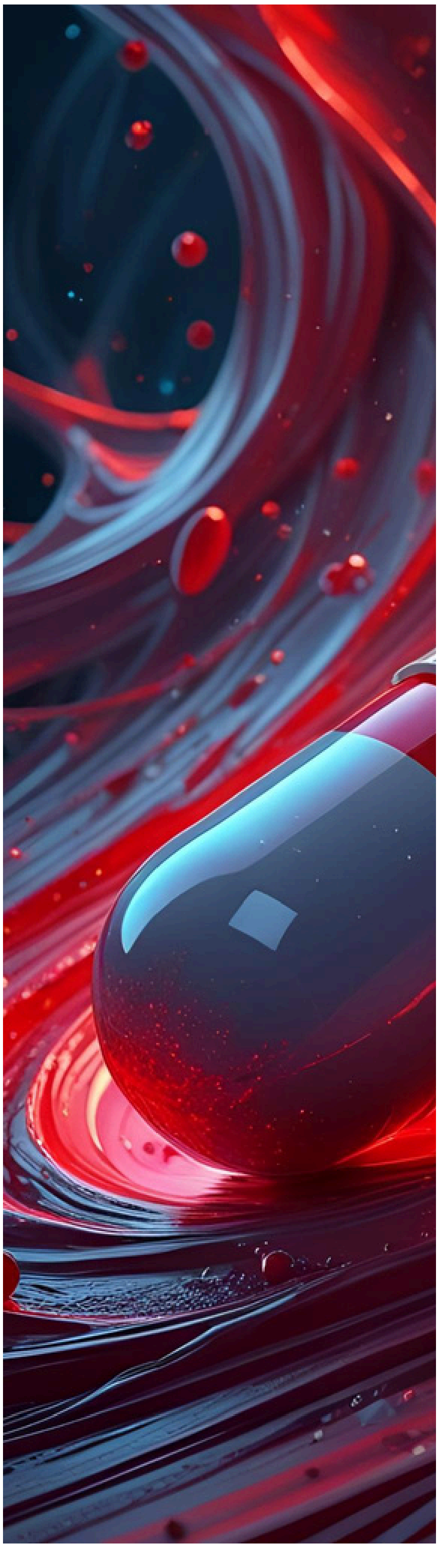
Tetsuo inside the wires

SORINT SEC

Table of Contents

Recently, a significant security incident impacted a critical infrastructure environment, the attack resulted in the encryption of substantial portions of the infrastructure, confirming Akira as the primary threat actor.

Forensic analysis revealed the presence of the Akira ransomware sample, in this blog post we provide a technical analysis of the Akira ransomware sample discovered during the incident, with a focus on its unique features and the ongoing evolution of the malware. Notably, we highlight how Akira has rapidly advanced since its initial appearance in early 2023, moving beyond its original, more traditional and more easly decryptable version.



1 Executive Summary

Recent analysis reveals that the latest iteration of Akira ransomware differs significantly from the initial 2023 version.
One of the most notable advancements is the inclusion of a log-erasure capability designed to delete all types of logs on the infected host. This feature helps attackers cover their tracks and complicates forensic investigation efforts.

Beyond this stealth enhancement, Akira's updated version demonstrates advanced string obfuscation techniques, which further impede reverse engineering and detection by security tools. The ransomware generates its encryption keys with high precision based on nanosecond timestamps, adding complexity to cryptographic operations and making key recovery more challenging.

These enhancements underscore the continual evolution of Akira ransomware, reflecting its operators' focus on both increasing efficiency and evading detection. Understanding these functionalities is critical for developing more effective defenses and incident response strategies against this emerging threat.

1.1 Key Findings

- This version of the ransomware is different from the first version appeared in 2023;
- The malware implement a feature aimed to delete all kind of logs of the target host in order to cover the tracks.

1.2 Key Functionality

- Advanced string obfuscation;
- Log-erase utility;
- Encryption key generate based on nanoseconds time precision;
- Exploit of Win Restart Manager API calls to increase the ransomware impact;
- Encryption percentage of files selectable;

2 Who is Akira

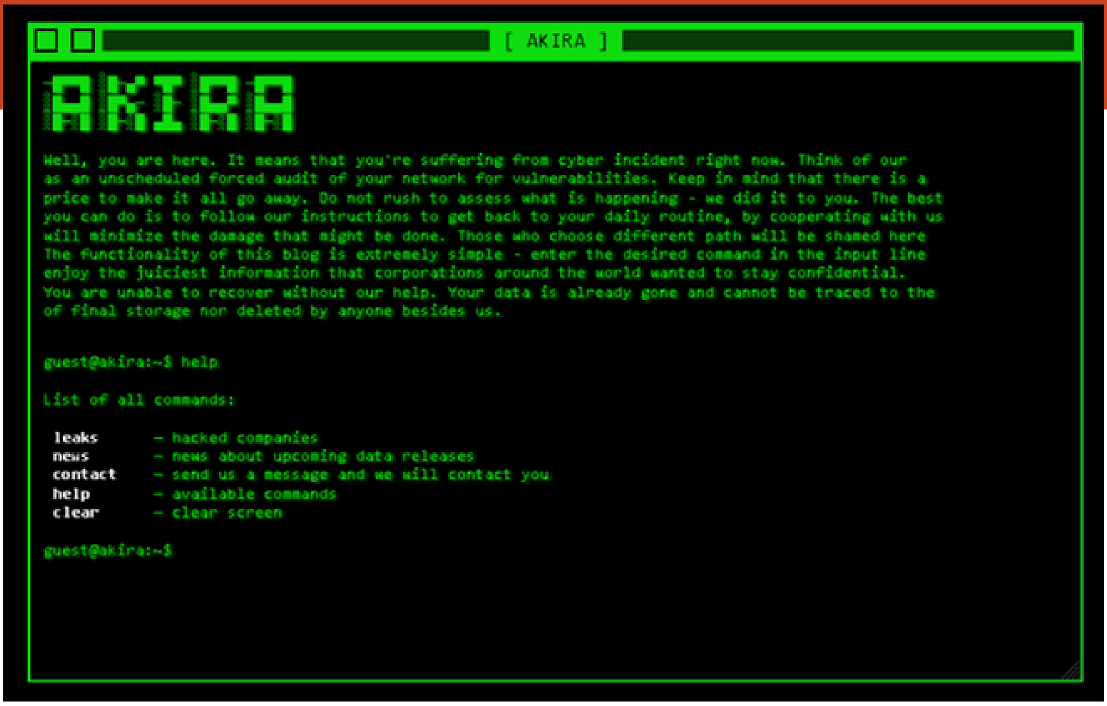
The Akira ransomware group, emerging in early 2023, is a cutting-edge cybercriminal operation blending brutal efficiency with technical skills. Operating under a Ransomware-as-a-Service (RaaS) model, Akira allows affiliates to deploy the ransomware in exchange for a percentage of the ransom payment. Akira recruits skilled affiliates to infiltrate targets, mostly small to medium businesses, via compromised VPN credentials and zero-day exploits, especially against Cisco VPNs. Once inside, they silently roam networks, stealing sensitive data before unleashing a hybrid encryption assault using ChaCha20 and RSA-4096, locking files and demanding a ransom.

There are suspected ties between Akira ransomware and the former CONTI ransomware group, as several CONTI affiliates migrated to independent campaigns like Royal, BlackBasta, and potentially Akira following CONTI's shutdown. Reports also indicate that Akira affiliates collaborate with other ransomware operations such as Snatch and BlackByte. This is supported by an exposed directory of tools linked to an Akira operator who had connections to Snatch ransomware.

What sets Akira apart is its bold double extortion strategy: victims face not only encrypted data but also the threat of public data dumps if ransoms aren't paid, with demands soaring up to $4 million. By early 2024, Akira had extorted an estimated $42 million from over 250 victims worldwide.

2.1 Akira Data Leak Site (DLS)

The Akira ransomware group's Data Leak Site is a unique, Tor-hosted platform featuring a command-line interface that lets users navigate stolen data and victim info interactively. It offers torrent links to leaked files, often password-protected, and allows victims to communicate directly with operators. Regularly updated with new victims and data, the leak site combines technical sophistication with thematic storytelling, making it a powerful tool for victim intimidation and public exposure.



```
Well, you are here. It means that you're suffering from cyber incident right now. Think of our
as an unscheduled forced audit of your network for vulnerabilities. Keep in mind that there is a
price to make it all go away. Do not rush to assess what is happening - we did it to you. The best
you can do is to follow our instructions to get back to your daily routine, by cooperating with us
will minimize the damage that might be done. Those who choose different path will be shamed here
The functionality of this blog is extremely simple - enter the desired command in the input line
enjoy the juiciest information that corporations around the world wanted to stay confidential.
You are unable to recover without our help. Your data is already gone and cannot be traced to the
of final storage nor deleted by anyone besides us.


guest@akira:~$ help

List of all commands:

 leaks       - hacked companies
 news        - news about upcoming data releases
 contact     - send us a message and we will contact you
 help        - available commands
 clear       - clear screen

guest@akira:~$
```

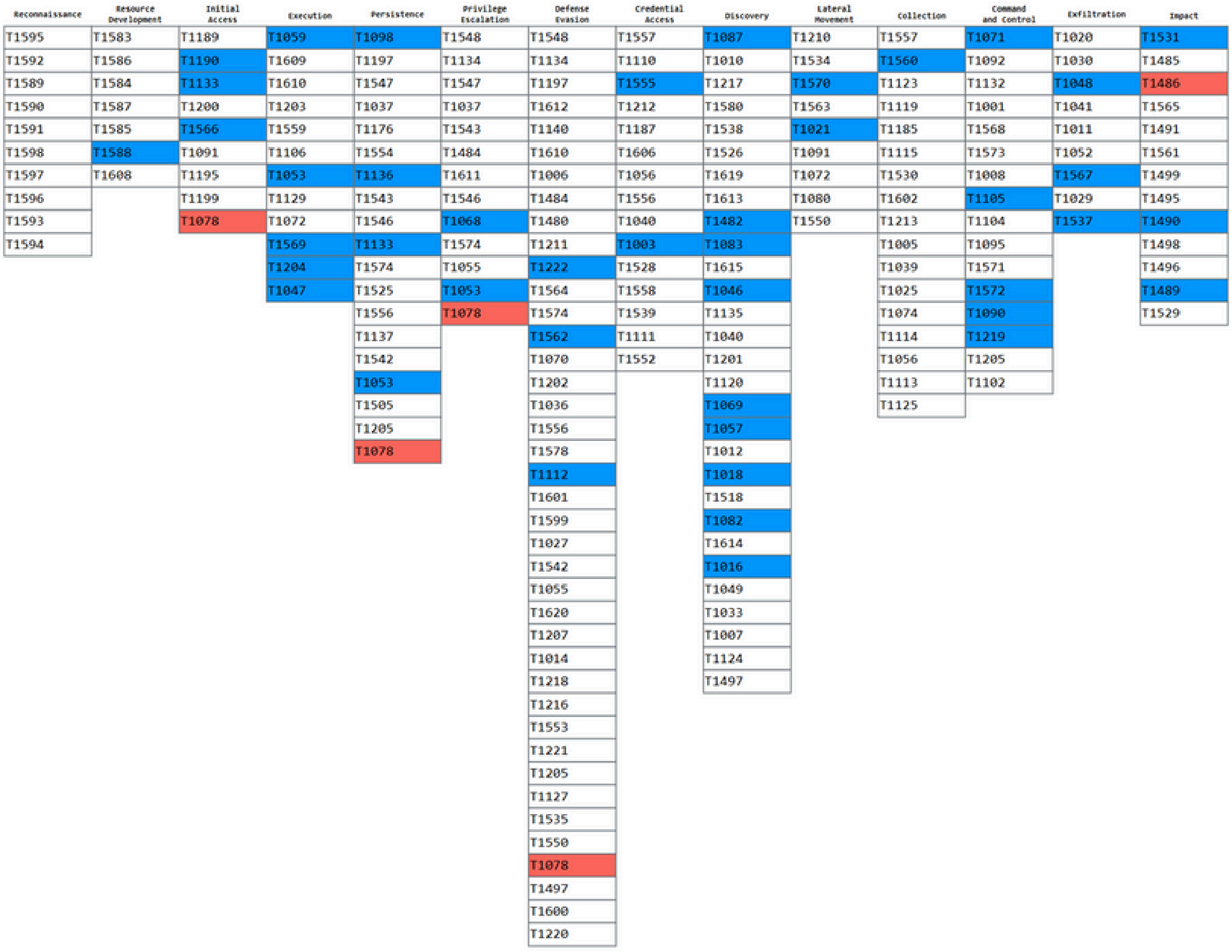
Akira DLS

DLS Onion Links:

```
hxxps://akiralkzxzq2dsrzsrvbr2xgbbu2wgsmxryd4csgfameg52n7efvr2id[.]onion
hxxps://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad[.]onion
```

Akira ransomware victims receive a unique .onion link and victim code in ransom notes to access a secure Tor-based chat platform. Through this private chat, victims negotiate directly with operators about ransom demands, stolen data, and decryption. Operators provide a list of encrypted and exfiltrated files and offer to decrypt select files as proof. Victims can also upload encrypted files for verification. This personalized communication allows tailored ransom negotiations, payment discussions, and data removal assurances. The chat system is a key part of Akira's extortion strategy, combining technical control with direct human interaction to pressure victims.

2.2 Akira Ransomware Group Cyber Kill Chain



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
T1595	T1583	T1189	T1059	T1098	T1548	T1548	T1557	T1087	T1210	T1557	T1071	T1020	T1531
T1592	T1586	T1190	T1609	T1197	T1134	T1134	T1110	T1010	T1534	T1560	T1092	T1030	T1485
T1589	T1584	T1133	T1610	T1547	T1547	T1197	T1555	T1217	T1570	T1123	T1132	T1048	T1486
T1590	T1587	T1200	T1203	T1037	T1037	T1612	T1212	T1580	T1563	T1119	T1001	T1041	T1565
T1591	T1585	T1566	T1559	T1176	T1543	T1140	T1187	T1538	T1021	T1185	T1568	T1011	T1491
T1598	T1588	T1091	T1106	T1554	T1484	T1610	T1606	T1526	T1091	T1115	T1573	T1052	T1561
T1597	T1608	T1195	T1053	T1136	T1611	T1006	T1056	T1619	T1072	T1530	T1008	T1567	T1499
T1596		T1199	T1129	T1543	T1546	T1484	T1556	T1613	T1080	T1602	T1105	T1029	T1495
T1593		T1078	T1072	T1546	T1068	T1480	T1040	T1482	T1550	T1213	T1104	T1537	T1490
T1594			T1569	T1133	T1574	T1211	T1003	T1083		T1005	T1095		T1498
			T1204	T1574	T1055	T1222	T1528	T1615		T1039	T1571		T1496
			T1047	T1525	T1053	T1564	T1558	T1046		T1025	T1572		T1489
				T1556	T1078	T1574	T1539	T1135		T1074	T1090		T1529
				T1137		T1562	T1111	T1040		T1114	T1219		
				T1542		T1070	T1552	T1201		T1056	T1205		
				T1053		T1202		T1120		T1113	T1102		
				T1505		T1036		T1069		T1125			
				T1205		T1556		T1057					
				T1078		T1578		T1012					
						T1112		T1018					
						T1601		T1518					
						T1599		T1082					
						T1027		T1614					
						T1542		T1016					
						T1055		T1049					
						T1620		T1033					
						T1207		T1007					
						T1014		T1124					
						T1218		T1497					
						T1216							
						T1553							
						T1221							
						T1205							
						T1127							
						T1535							
						T1550							
						T1078							
						T1497							
						T1600							
						T1220							

Figure 18 – Akira MITRE TTPs

The MITRE ATT&CK techniques used by Akira ransomware reflect its high level of operational sophistication through stealth, persistence, and effective extortion strategies. Akira's exploitation of multi-factor authentication (MFA) bypasses (e.g., CVE-2023-20269) for initial access demonstrates advanced targeting of security controls, enabling stealthy entry into networks. Their use of credential dumping tools like LSASS memory dumps and lateral movement via RDP or tools like Mimikatz shows deep knowledge of Windows internals to escalate privileges and spread undetected. Furthermore, Akira's data exfiltration via legitimate tools such as Rclone and WinSCP highlights their operational security focus, blending malicious activity with normal network traffic to avoid detection. These TTPs, combined with double extortion and tailored ransom negotiations, illustrate Akira's sophisticated, multi-layered approach that maximizes impact while minimizing early discovery.

Initial Access

Akira's operators commonly gain initial access to victim environments by exploiting vulnerabilities in virtual private network (VPN) services, especially those without multi-factor authentication (MFA). Notable exploited flaws include Cisco VPN vulnerabilities such as CVE-2020-3259 and the 2023 zero-day CVE-2023-20269. In addition, Akira actors use stolen or compromised credentials to log into external-facing services like VPN portals or Remote Desktop Protocol (RDP) endpoints. Spear phishing campaigns and abuse of valid credentials (e.g., purchased or stolen) also enable initial footholds, providing attackers direct entry into targeted networks.

Persistence

After initial compromise, Akira operators move quickly to establish persistence. This often involves creating new domain user accounts with administrative privileges to maintain long-term access, sometimes using stealth techniques to hide these accounts from visible login screens. Remote access tools such as AnyDesk, RustDesk, or Radmin are frequently deployed, allowing attackers covert remote management even if initial vulnerabilities are patched or detected.

Defense Evasion

Akira's defense evasion toolbox includes multiple powerful techniques. Operators commonly deploy utilities like PowerTool, KillAV, and Terminator, which terminate security and antivirus processes to disable endpoint protection. PowerShell commands are also used extensively to disable Microsoft Defender real-time protection and delete Windows volume shadow copies, preventing easy recovery of encrypted data. Registry modifications further disable or reconfigure security tools and can obscure attacker-created accounts by hiding them from standard listings.

Discovery

Mapping the victim environment is critical to Akira's lateral movement and impact strategies. The group uses popular network scanning tools such as Advanced IP Scanner and MASSCAN to identify active systems, open ports, and accessible network shares. Tools like AdFind, net commands, and nltest help in enumerating Active Directory domain information, trusts, and permissions. Akira operators also employ BloodHound to visualize attack paths for efficient privilege escalation. These discovery activities provide detailed intel on domain controllers, backup servers, and security appliances, informing follow-on attacks.

Credential Access

Akira operators make extensive use of credential dumping techniques, often leveraging tools such as Mimikatz and LaZagne alongside scripted attacks like Kerberoasting to extract credentials from memory and local caches. Credentials harvested from LSASS, Windows Credential Manager, and cached domain stores are used for lateral impersonation and privilege escalation, enabling the attackers to spread their access seamlessly across the network.

Lateral Movement

With valid credentials in hand, the attackers utilize multiple protocols for lateral movement, primarily RDP and SMB. “Pass-the-hash” and “pass-the-ticket” techniques enable them to authenticate to remote systems without needing plaintext passwords. Akira operators often transfer additional tools and payloads across systems using PSExec, file shares, or RDP file transfers, preparing endpoints for encryption. Network shares discovered during the reconnaissance phase become prime targets for spreading the ransomware.

Command and Control

Remote management tools, often legitimate applications like AnyDesk or PuTTy, serve as the primary channels for command and control (C2). These tools help attackers maintain persistent communication and control while blending in with normal administrative activity, making detection challenging. In some cases, Akira operators deploy proxy or tunneling services such as Ngrok or Cloudflare Tunnel to provide access to systems behind firewalls or NAT environments.

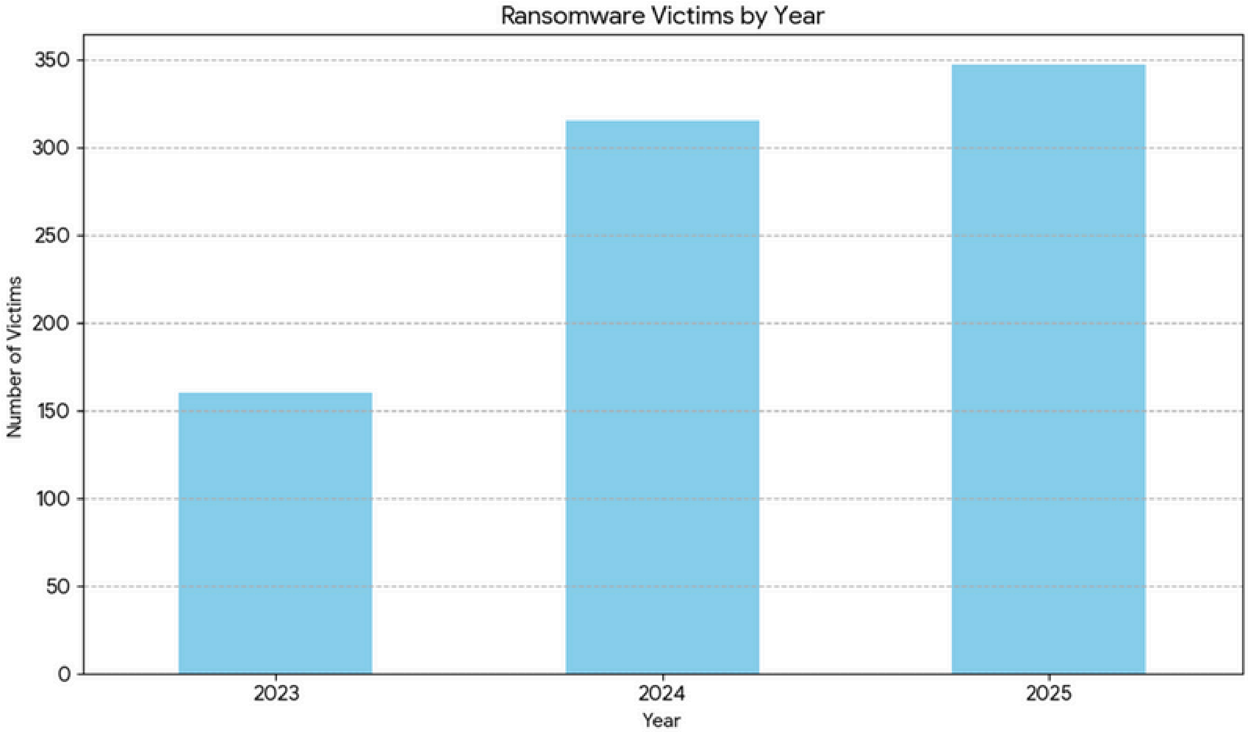
Data Exfiltration

Distinctively, Akira employs a double-extortion strategy. Before locking victims’ data with encryption, operators exfiltrate sensitive corporate information. They compress data archives using utilities like WinRAR and transfer them using protocols such as FTP, SFTP, or cloud services (e.g., via Rclone). Exfiltration channels mimic legitimate network traffic to evade detection and increase pressure on victims by threatening to publicly release stolen data if ransoms aren’t paid.

Impact

The final—and most devastating stage—is the encryption of critical files and disruption of system recovery capabilities. Akira uses a hybrid encryption scheme combining the ChaCha20 stream cipher and RSA public-key cryptography to quickly and securely encrypt data. Encrypted files typically carry extensions like .akira . The ransomware deletes volume shadow copies using PowerShell commands (Get-WmiObject Win32_Shadowcopy | Remove-WmiObject), disables backups, and terminates backup and security processes to prevent recovery without the decryption keys. Victims receive ransom notes with instructions, often delivered via anonymous Tor-based websites, demanding payment generally in Bitcoin. Operators frequently threaten to leak exfiltrated data publicly as leverage to coerce payments.

2.3 Attacks over the years

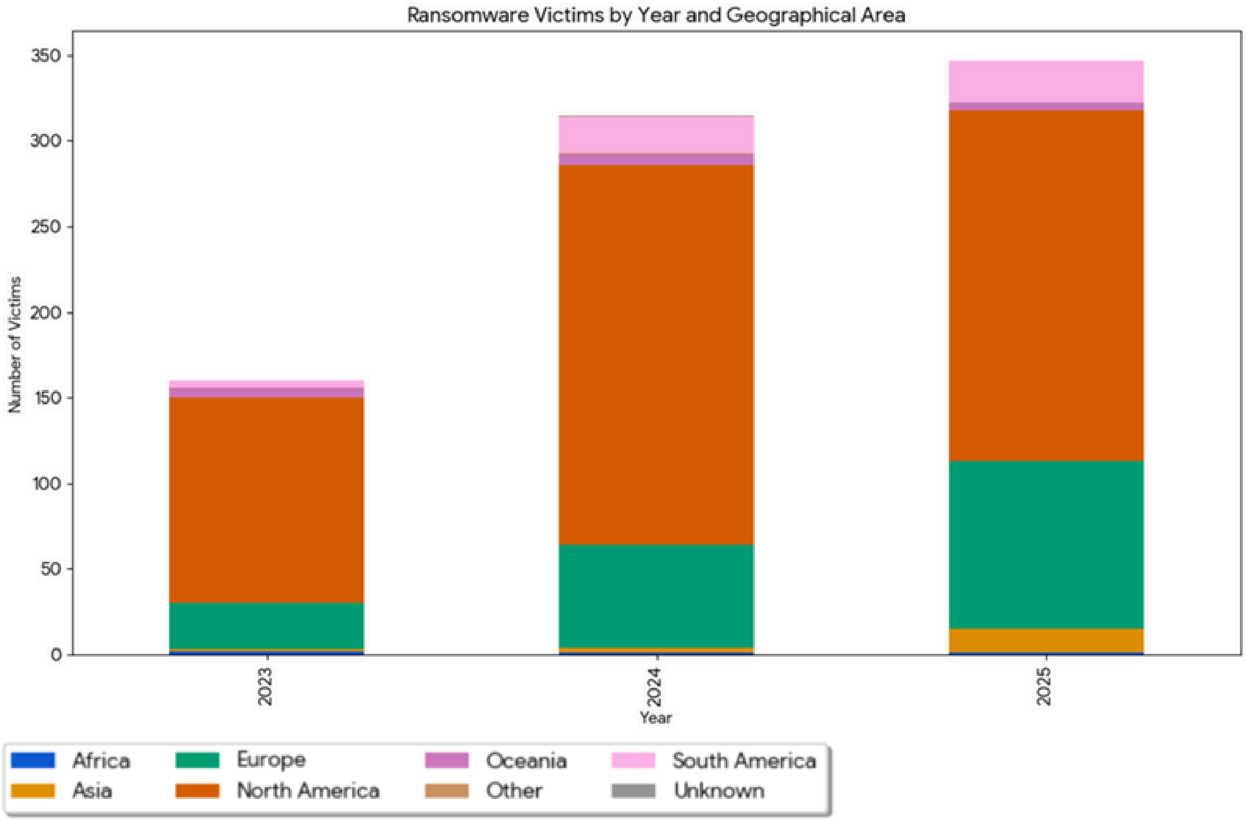


Akira victims by year – ransomfeed data

Since its emergence in March 2023, Akira ransomware has seen a rapid and significant increase in victims and impact. By early 2024, it had already targeted over 250 organizations globally, including notable entities like Nissan Australia and Stanford University, generating approximately $42 million in ransom payments. The group's activity steadily intensified throughout 2024, with monthly victim counts rising from single digits to a peak of 73 victims in November 2024. Akira became one of the most detected ransomware variants in the US by Q3 2024, responsible for around 21% of ransomware attacks in early 2024. Its expansion continued into 2025, with reports of a 60% surge in activity in January alone, targeting sectors such as manufacturing, finance, and IT across North America and Europe. This growth reflects Akira's evolving tactics, including targeting vulnerable VPNs and deploying both Windows and Linux variants, cementing its position as a major ransomware threat.

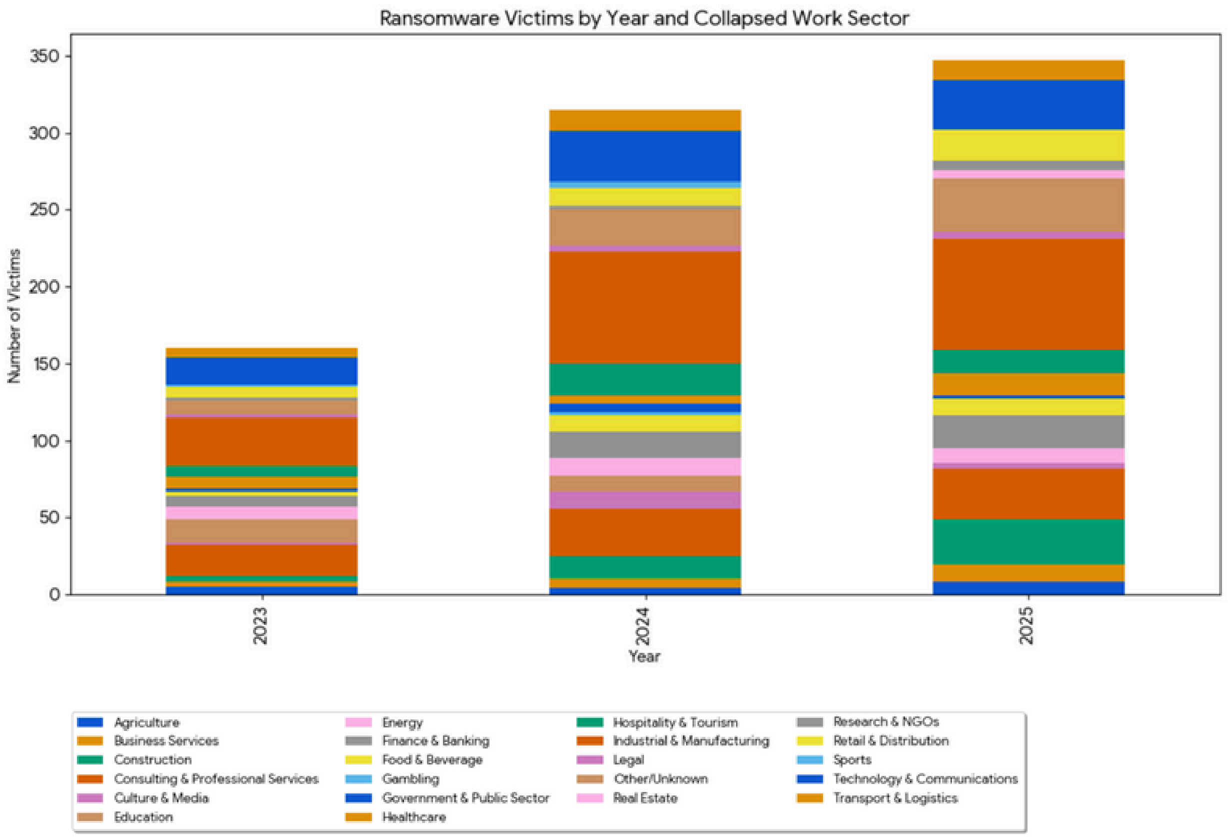
2.4 Akira targtes

Akira ransomware has demonstrated a broad and global targeting pattern since its emergence in 2023. North America, especially the United States, is heavily targeted, making Akira one of the top ransomware threats there by 2024. Other frequently attacked countries include the United Kingdom, Australia, Germany, Sweden, and Japan.



Akira victims by geographical area – ransomfeed data

Akira's indiscriminate approach focuses on exploiting vulnerable systems worldwide, with no clear industry or regional limitation, except for avoiding countries using Russian keyboard layouts likely reflecting the group's Russian origin and an unspoken rule to avoid domestic law enforcement pressure. This global reach, combined with a high volume of attacks (up to 70+ victims monthly at peak), underscores Akira's rapid expansion and significant impact across diverse countries and industries.



Akira victims by sector – ransomfeed data

Akira ransomware targets a broad range of sectors, with a particular focus on small to medium-sized enterprises. The most affected industries include education, manufacturing, finance, healthcare, legal, retail, and critical infrastructure. Its indiscriminate targeting spans North America, Europe, Australia, and beyond, affecting organizations from universities and hospitals to manufacturing plants and law firms.

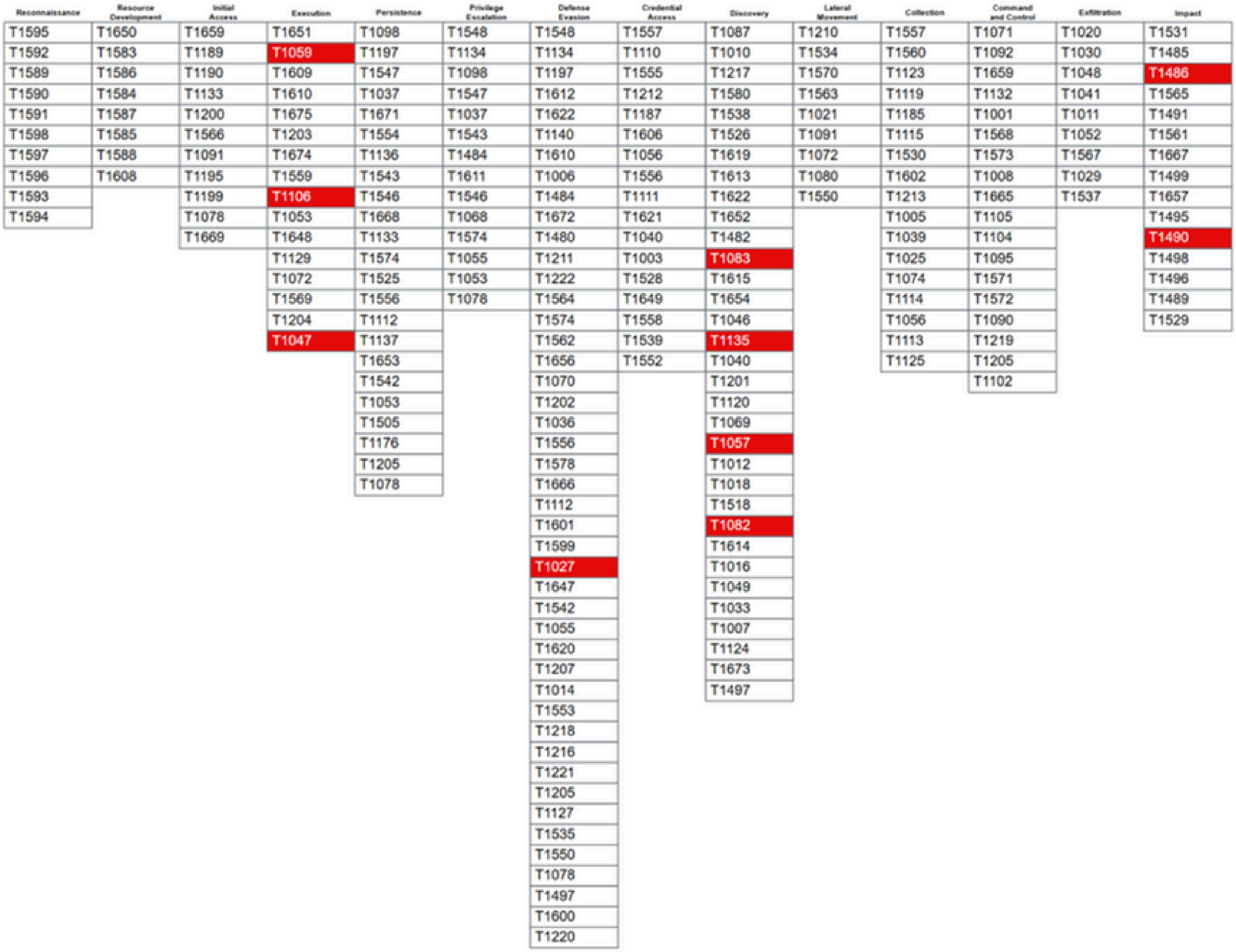
3 Summary of the Malware

The initial version of Akira ransomware was written in C++ and appended encrypted files with the extension ".akira," while dropping a ransom note named "akira_readme.txt." This version's code was partially based on Conti V2. Notably, on June 29, 2023, security vendor Avast released a decryptor for this variant due to a flaw in its encryption mechanism.

However, on July 2, 2023, Akira operators released updated versions that fixed the decryption vulnerability. This sample integrates advanced evasion techniques and configurable features for execution.

4 Malware Technical Details

4.1 MITRE ATT&CK TTPs and Malware Behavior Catalog (MBC) observation



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
T1595	T1650	T1659	T1651	T1098	T1548	T1548	T1557	T1087	T1210	T1557	T1071	T1020	T1531
T1592	T1583	T1189	**T1059**	T1197	T1134	T1134	T1110	T1010	T1534	T1560	T1092	T1030	T1485
T1589	T1586	T1190	T1609	T1547	T1098	T1197	T1555	T1217	T1570	T1123	T1659	T1048	**T1486**
T1590	T1584	T1133	T1610	T1037	T1547	T1612	T1212	T1580	T1563	T1119	T1132	T1041	T1565
T1591	T1587	T1200	T1675	T1671	T1037	T1622	T1187	T1538	T1021	T1185	T1001	T1011	T1491
T1598	T1585	T1566	T1203	T1554	T1543	T1140	T1606	T1526	T1091	T1115	T1568	T1052	T1561
T1597	T1588	T1091	T1674	T1136	T1484	T1610	T1056	T1619	T1072	T1530	T1573	T1567	T1667
T1596	T1608	T1195	T1559	T1543	T1611	T1006	T1556	T1613	T1080	T1602	T1008	T1029	T1499
T1593		T1199	**T1106**	T1546	T1546	T1484	T1111	T1622	T1550	T1213	T1665	T1537	T1657
T1594		T1078	T1053	T1668	T1068	T1672	T1621	T1652		T1005	T1105		T1495
		T1669	T1648	T1133	T1574	T1480	T1040	T1482		T1039	T1104		**T1490**
			T1129	T1574	T1055	T1211	T1003	**T1083**		T1025	T1095		T1498
			T1072	T1525	T1053	T1222	T1528	T1615		T1074	T1571		T1496
			T1569	T1556	T1078	T1564	T1649	T1654		T1114	T1572		T1489
			T1204	T1112		T1574	T1558	T1046		T1056	T1090		T1529
			T1047	T1137		T1562	T1539	**T1135**		T1113	T1219		
				T1653		T1656	T1552	T1040		T1125	T1205		
				T1542		T1070		T1201			T1102		
				T1053		T1202		T1120					
				T1505		T1036		T1069					
				T1176		T1556		**T1057**					
				T1205		T1578		T1012					
				T1078		T1666		T1018					
						T1112		T1518					
						T1601		**T1082**					
						T1599		T1614					
						T1027		T1016					
						T1647		T1049					
						T1542		T1033					
						T1055		T1007					
						T1620		T1124					
						T1207		T1673					
						T1014		T1497					
						T1553							
						T1218							
						T1216							
						T1221							
						T1205							
						T1127							
						T1535							
						T1550							
						T1078							
						T1497							
						T1600							
						T1220							

MITRE TTPs

Akira ransomware, like many modern ransomware families, blends high-level tactics designed to compromise and disrupt victim environments with low-level malware behaviors that ensure its encryption routines execute effectively. While MITRE ATT&CK helps us understand the tactics and techniques of Akira at the campaign level, the Malware Behavior Catalog (MBC) adds granularity by detailing its inner workings—cryptographic routines, obfuscation methods, file system manipulations, and process interactions. Together, these frameworks allow us to paint a complete picture of Akira's behavior.

4.2 Dissecting Akira Ransomware Using ATT&CK and MBC

Execution (ATT&CK: TA0002)

When Akira begins execution, it leverages native Windows utilities such as PowerShell and cmd.exe to run its malicious code. Tactics like WMI-based command execution and API calls allow it to automate tasks, spread laterally, and disable services.

On the MBC side, we observe multiple low-level execution markers. For example, Akira makes frequent use of process creation (C0017) and thread management behaviors (C0038, C0039, C0041)—creating threads to parallelize encryption, terminating processes that may lock files, and using thread-local storage to manage encryption keys per thread. These behaviors underpin its ability to simultaneously encrypt large volumes of files across a system.

Defense Evasion (ATT&CK: TA0005)

Akira goes to great lengths to avoid detection, primarily through obfuscation. Files and payloads are frequently obfuscated or encoded to hinder analysis, and encoded payload segments may only be decrypted at runtime.

MBC provides more technical insight here: Akira applies Obfuscated Files or Information::Encoding-Standard Algorithm (E1027.m02) to disguise payload data, and in some variants employs Disassembler Evasion::Argument Obfuscation (B0012.001)—a technique where API call arguments are intentionally obscured to disrupt static analysis in reverse engineering tools. This ensures that analysts and security products have a harder time detecting or accurately modeling its behavior before execution.

Discovery (ATT&CK: TA0007)

Before encrypting, Akira performs environment reconnaissance. It enumerates drives, files, and processes to ensure maximum reach and efficiency. Network share discovery and system information collection are standard components of this phase.

MBC adds precision by detailing how Akira conducts Code Discovery through PE Enumeration (B0046.001). By examining Portable Executable (PE) sections, the malware can identify which code libraries and modules are of interest. This behavior also supports anti-analysis mechanisms and may aid in privilege escalation or process targeting.

Impact (ATT&CK: TA0040)

The hallmark of Akira is its impact stage, where it encrypts files en masse and inhibits system recovery by deleting shadow copies and disabling recovery tools. Victims are left without access to critical data and pressured to pay ransom demands.

Here, MBC mapping reveals the cryptographic underpinnings of Akira's file encryption. Instead of relying solely on standard algorithms, Akira incorporates a mix of crypto routines and encoding behaviors:

It has been observed using RC4 (C0027.009) for encryption and the RC4 PRGA (C0021.004) to generate pseudo-random keystreams.

Hashing functions play a role as well, including MD5 (C0029.001) for data integrity checks and FNV (C0030.005) as a lightweight non-cryptographic hash.

Data encoding is also central, with Base64 (C0026.001) and XOR (C0026.002) operations being used to conceal payloads, obfuscate stored keys, or wrap strings.

Additional resilience is provided by string verification routines (Check String: C0019) and checksum techniques like the Luhn algorithm (C0032.002) to validate targeted data elements before encryption.

At the filesystem level, Akira demonstrates clear file manipulation behaviors captured by MBC: it creates directories (C0046), queries attributes (C0049), reads (C0051), and overwrites files (C0052) as part of its encryption cycle and ransom note deployment.

Operating System Interaction: Another dimension of Akira's activity is its direct OS-level manipulation. It sets environment variables (C0034.001) to manage execution paths and runtime parameters. Combined with its API-based process/thread control, this allows Akira to operate flexibly in varied environments while maintaining stealth.

MBC Objective	MBC Behavior
ANTI-STATIC ANALYSIS	Disassembler Evasion::Argument Obfuscation [B0012.001]
CRYPTOGRAPHY	Cryptographic Hash::MD5 [C0029.001] Encrypt Data::RC4 [C0027.009] Generate Pseudo-random Sequence::RC4 PRGA [C0021.004]
DATA	Check String:: [C0019] Checksum::Luhn [C0032.002] Encode Data::Base64 [C0026.001] Encode Data::XOR [C0026.002] Non-Cryptographic Hash::FNV [C0030.005]
DEFENSE EVASION	Obfuscated Files or Information::Encoding-Standard Algorithm [E1027.m02]
DISCOVERY	Code Discovery::Enumerate PE Sections [B0046.001]
FILE SYSTEM	Create Directory:: [C0046] Get File Attributes:: [C0049] Read File:: [C0051] Writes File:: [C0052]
OPERATING SYSTEM	Environment Variable::Set Variable [C0034.001]
PROCESS	Allocate Thread Local Storage:: [C0040] Create Process:: [C0017] Create Thread:: [C0038] Set Thread Local Storage Value:: [C0041] Terminate Thread:: [C0039]

Objectives and behaviors detected in the sample under analysis categorized according to the Malware Behavior Catalog (MBC).

Conclusion

By layering MITRE ATT&CK and the Malware Behavior Catalog, we gain a dual perspective on Akira ransomware. ATT&CK frames Akira's high-level objectives—executing malicious code, evading defenses, exploring the system, and ultimately encrypting data for impact—while MBC uncovers the deeper technical detail: cryptographic primitives, encoding schemes, disassembly evasion methods, and process/thread behaviors.

5 Static Analysis

This chapter provides an in-depth overview of the static analysis performed on the examined malware sample. The findings from this phase lay the groundwork for subsequent dynamic analysis and behavioral correlation described in the next chapters.

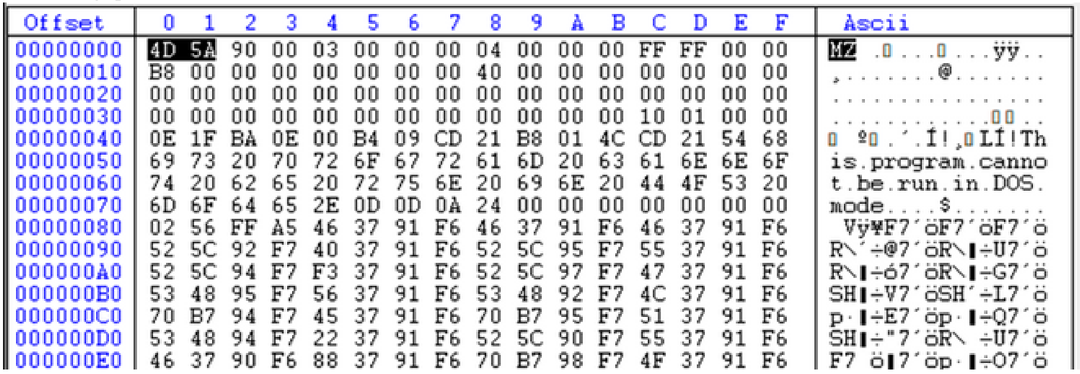
File Name: a.exe

File Hash:

MD5: 5337D181CE59D7DDA9CC955B2DDE48A7
SHA1: 232AC61A697D776BEBB1541634E80B9A219ECFCD
SHA256: 9E0D9E831E14EFA69941A2CA5DD3131B466DBF737A8936C34411D0EA6330D9BD

File Size: 1081856 (bytes)

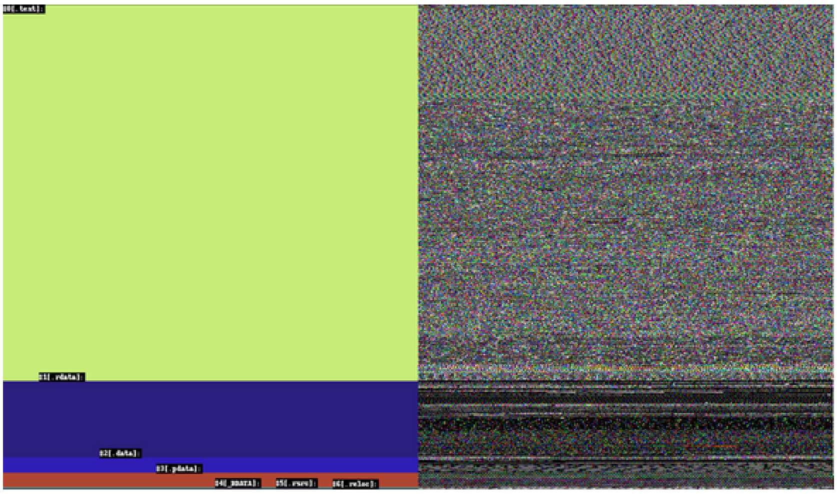
File Type: executable



```
Offset    0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   Ascii
00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ .▯...▯...ÿÿ..
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ,.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00  ............▯▯..
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ▯ º▯.´.Í!,▯LÍ!Th
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is.program.canno
00000060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t.be.run.in.DOS.
00000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
00000080  02 56 FF A5 46 37 91 F6 46 37 91 F6 46 37 91 F6   Vÿ¥F7´öF7´öF7´ö
00000090  52 5C 92 F7 40 37 91 F6 52 5C 95 F7 55 37 91 F6  R\´÷@7´öR\▌÷U7´ö
000000A0  52 5C 94 F7 F3 37 91 F6 52 5C 97 F7 47 37 91 F6  R\▌÷ó7´öR\▌÷G7´ö
000000B0  53 48 95 F7 56 37 91 F6 53 48 92 F7 4C 37 91 F6  SH▌÷V7´öSH´÷L7´ö
000000C0  70 B7 94 F7 45 37 91 F6 70 B7 95 F7 51 37 91 F6  p·▌÷E7´öp·▌÷Q7´ö
000000D0  53 48 94 F7 22 37 91 F6 52 5C 90 F7 55 37 91 F6  SH▌÷"7´öR\ ÷U7´ö
000000E0  46 37 90 F6 88 37 91 F6 70 B7 98 F7 4F 37 91 F6  F7 ö▌7´öp·▌÷O7´ö
```

MZ header

PE Section Graphic Overview:



Bin sections

MALWARE ANALYSIS REPORT

Compiler Info: Microsoft Visual C/C++

Compile Timestamp: Wed Mar 19 13:53:17 2025

Notable strings: Different notable and/or human readable strings are present in the sample, highlighted below the most significant:

`Create auto save file failed! (`

The string is indicative of an internal process designed to automatically save data to a file. The error message is generated when this process fails, suggesting the malware attempts to create or update an auto save file

```
powershell.exe -Command "Get-WmiObject Win32_Shadowcopy | Remove-WmiObject"
```

Finding this string signifies an attempt to destroy local backup snapshots, making recovery and investigation significantly more difficult. This is a hallmark of destructive or extortion-focused malware, such as ransomware.

`Log-%d-%m-%Y-%H-%M-%S`

The string indicates that the malware creates log files named with precise timestamps, enabling detailed and organized logging of its activities.

`Command line to argvW failed!`

The string suggests that the malware attempts to parse command-line arguments into a Unicode argument array but encountered an error during this process, revealing that command-line input handling is a component of its operation.

`--encryption_percent`

This string indicates that the malware includes a configurable parameter to specify the percentage of each target file that will be encrypted during its execution. This indicates a sophisticated encryption strategy where the malware encrypts only a configurable portion of each target file. This approach balances encryption speed, stealth, and effectiveness, allowing attackers to optimize their ransomware operations while complicating detection and recovery efforts.

akira_readme.txt

The string confirm that the sample is associated with Akira ransomware and that it drops this specific ransom note file to communicate ransom demands and instructions to victims after encrypting their files.

Imported/exported functions:

Highlighted below are some functions that help to understand better the capabilities of the sample.

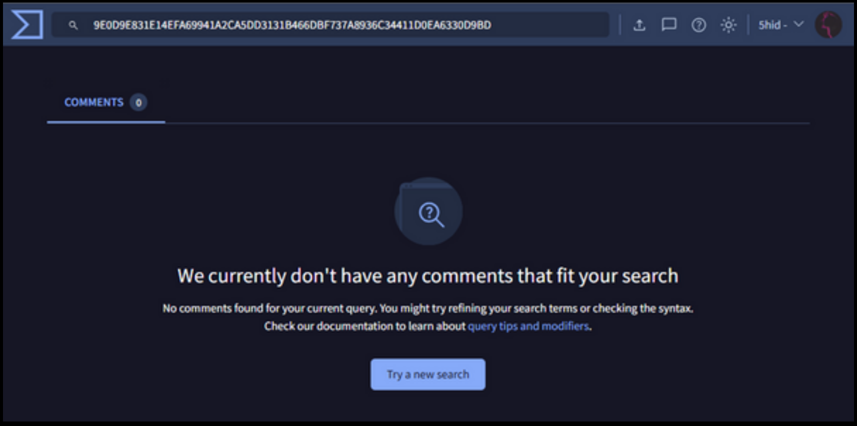
RmShutdown
RmStartSession
RmEndSession
RmRegisterResources
RmGetList

These Restart Manager APIs can unlock or close files/processes that are being used by other apps, often used by ransomware to terminate processes/services preventing file encryption. Call this function, as you will also see in the code view section, are used by Akira ransomware to maximize damage by ensuring files are accessible for encryption or wiping.

QueryPerformanceFrequency
QueryPerformanceCounter

Commonly used by malware for host timing checks for debugger detection or sandbox evasion, these functions are used by Akira to generate a not-so-bruteforceble encryption seed.

No evidences related to VirusTotal detections or public references about the sample while report writing.



9E0D9E831E14EFA69941A2CA5DD3131B466DBF737A8936C34411D0EA6330D9BD

We currently don't have any comments that fit your search

No comments found for your current query. You might try refining your search terms or checking the syntax. Check our documentation to learn about query tips and modifiers.

Virus Total

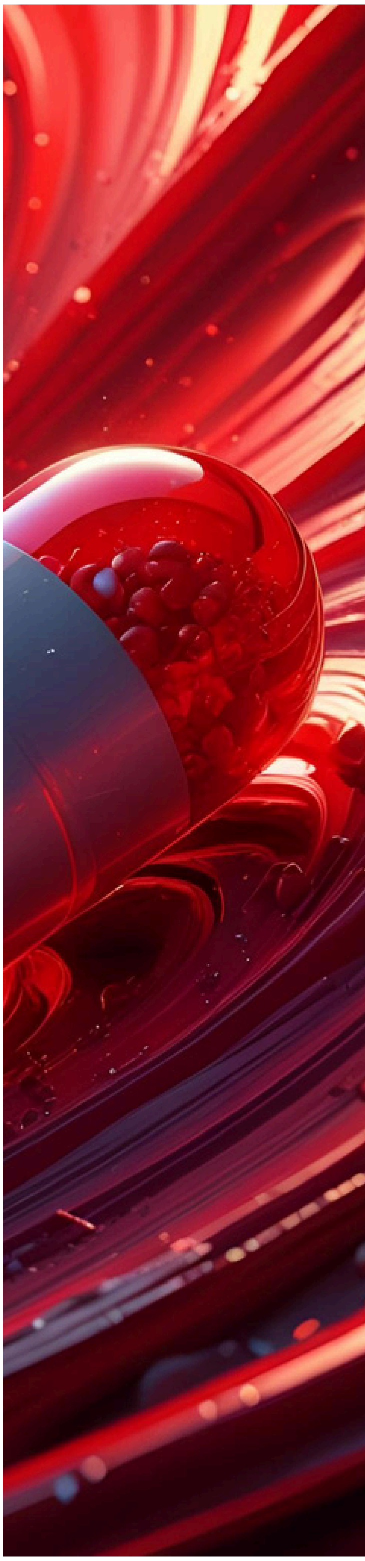
6 Dynamic Analysis

6.1 Execution in a containment environment

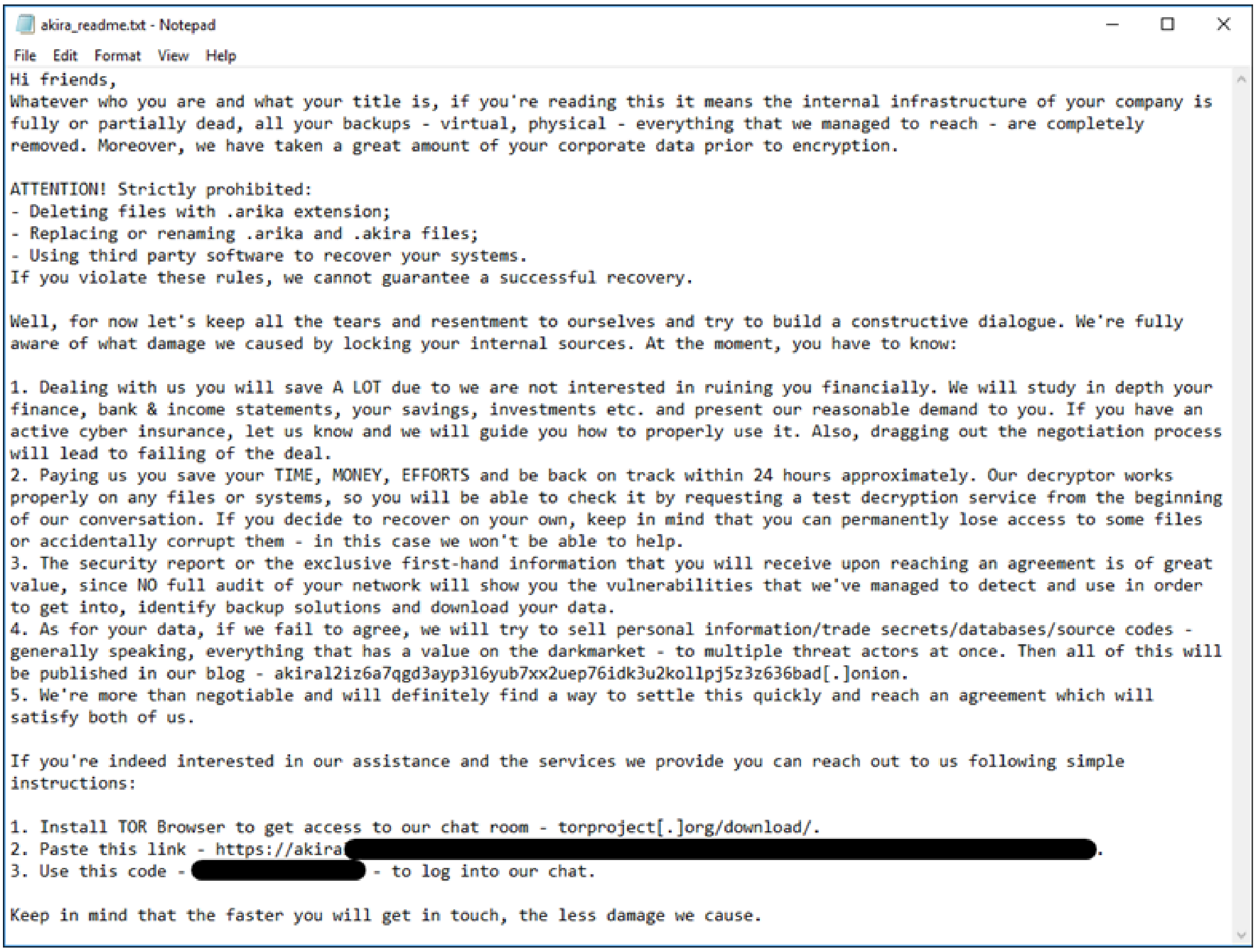
To emulate the ransomware's operational behavior, a temporary directory was provisioned with diverse file types. Subsequently, the malware sample was executed with this directory explicitly set as the target for encryption.

Below specified the instruction flags that the sample takes as input:

Command-line instruction	Description
-p -encryption_path	Indicates the directory in which files will be encrypted, including all subfolders.
-s -share_file	A file that lists the directories and devices designated for encryption.
-e -exclude	Used to exclude specific paths.
-n -encryption_percent	Encrypts only a portion of the file, specifying the percentage to be encrypted.
-localonly	Targets encryption solely on the victim's own device, excluding remote systems.
-dellog	Wipe event logs from the system.



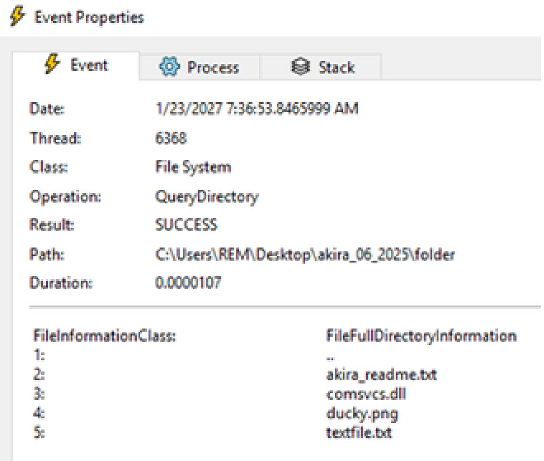
Upon execution a log file named [Log-%d-%m-%Y-%H-%M-%S].log is generated to record execution details, alongside a text file titled akira_readme.txt containing ransom payment instructions for the victim.



```
Hi friends,
Whatever who you are and what your title is, if you're reading this it means the internal infrastructure of your company is
fully or partially dead, all your backups - virtual, physical - everything that we managed to reach - are completely
removed. Moreover, we have taken a great amount of your corporate data prior to encryption.

ATTENTION! Strictly prohibited:
- Deleting files with .arika extension;
- Replacing or renaming .arika and .akira files;
- Using third party software to recover your systems.
If you violate these rules, we cannot guarantee a successful recovery.

Well, for now let's keep all the tears and resentment to ourselves and try to build a constructive dialogue. We're fully
aware of what damage we caused by locking your internal sources. At the moment, you have to know:

1. Dealing with us you will save A LOT due to we are not interested in ruining you financially. We will study in depth your
finance, bank & income statements, your savings, investments etc. and present our reasonable demand to you. If you have an
active cyber insurance, let us know and we will guide you how to properly use it. Also, dragging out the negotiation process
will lead to failing of the deal.
2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24 hours approximately. Our decryptor works
properly on any files or systems, so you will be able to check it by requesting a test decryption service from the beginning
of our conversation. If you decide to recover on your own, keep in mind that you can permanently lose access to some files
or accidentally corrupt them - in this case we won't be able to help.
3. The security report or the exclusive first-hand information that you will receive upon reaching an agreement is of great
value, since NO full audit of your network will show you the vulnerabilities that we've managed to detect and use in order
to get into, identify backup solutions and download your data.
4. As for your data, if we fail to agree, we will try to sell personal information/trade secrets/databases/source codes -
generally speaking, everything that has a value on the darkmarket - to multiple threat actors at once. Then all of this will
be published in our blog - akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad[.]onion.
5. We're more than negotiable and will definitely find a way to settle this quickly and reach an agreement which will
satisfy both of us.

If you're indeed interested in our assistance and the services we provide you can reach out to us following simple
instructions:

1. Install TOR Browser to get access to our chat room - torproject[.]org/download/.
2. Paste this link - https://akira[redacted].
3. Use this code - [redacted] - to log into our chat.

Keep in mind that the faster you will get in touch, the less damage we cause.
```

Ransom note

Upon execution, the sample enumerates the contents of the specified target directory, identifying files such as .txt, .dll, and .png, and compares their extensions against the sample's predefined blacklist and whitelist.



```
Date:        1/23/2027 7:36:53.8465999 AM
Thread:      6368
Class:       File System
Operation:   QueryDirectory
Result:      SUCCESS
Path:        C:\Users\REM\Desktop\akira_06_2025\folder
Duration:    0.0000107

FileInformationClass:        FileFullDirectoryInformation
1:                           ..
2:                           akira_readme.txt
3:                           comsvcs.dll
4:                           ducky.png
5:                           textfile.txt
```

Query directory event

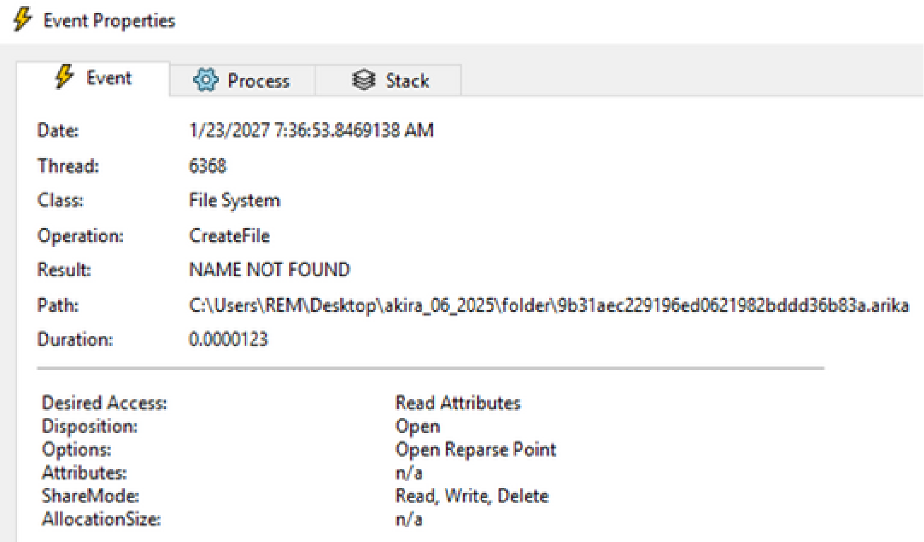
Below is the whitelist employed by the ransomware to exclude specified files and processes from modification, thereby preventing system instability and ensuring successful encryption. Notably, the DLL file in the test folder remains unaffected by the malware.

Processes	Folders	Extensions
- spoolsv.exe - explorer.exe - sihost.exe - fontdrvhost.exe - cmd.exe - dwm.exe - LogonUI.exe - SearchUI.exe - lsass.exe - csrss.exe - smss.exe - winlogon.exe - services.exe - conhost.exe - System - System - Idle - Process - Secure - System - Registry - Memory - Compression - wininit.exe	- $Recycle.Bin - $RECYCLE.BIN - Boot - ProgramData - System Volume Information - temp - thumb - tmp - Trend Micro - Windows - winnt	- .dll - .exe - .lnk - .msi - .sys - .arika

Below is the blacklist of file extensions that the ransomware targets for complete encryption.

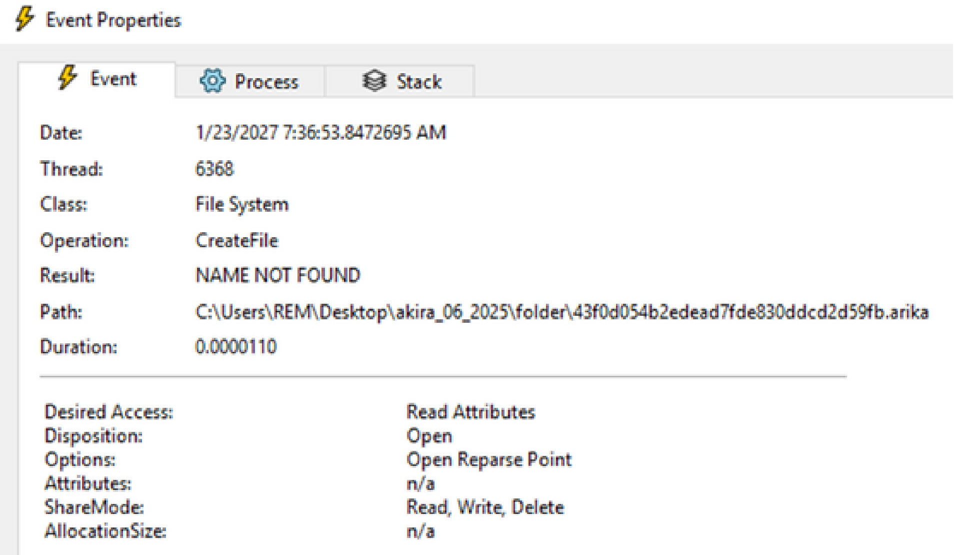
- .4dd
- .4dl
- .abcddb
- .abs
- .abx
- .accdb
- .accdc
- .accde
- .accdr
- .accdt
- .accdw
- .accft
- .adb
- .ade
- .adf
- .adn
- .adp
- .alf
- .arc
- .ask
- .avdx
- .avhd
- .bdf
- .bin
- .btr
- .cat
- .cdb
- .ckp
- .cma
- .cpd
- .dacpac
- .dad
- .dadiagrams
- .daschema
- .db
- .db-shm
- .db-wal
- .db2
- .db3
- .dbc
- .dbf
- .dbs
- .dbt
- .dbv
- .dbx
- .dcb
- .dct
- .dcx
- .ddl
- .dlis
- .dp1
- .dqy
- .dsk
- .dsn
- .dtsx
- .dxl
- .eco
- .ecx
- .edb
- .epim
- .exb
- .fcd
- .fic
- .fm5
- .fmp
- .fmp12
- .fmpsl
- .fol
- .fp3
- .fp4
- .fp5
- .fp7
- .fpt
- .frm
- .gdb
- .grdb
- .gwi
- .hdb
- .his
- .hjt
- .ib
- .icg
- .icr
- .idb
- .ihx
- .ini
- .iso
- .itdb
- .itw
- .jet
- .jtx
- .kdb
- .kdb
- .kexi
- .kexic
- .kexis
- .lgc
- .lut
- .lwx
- .maf
- .maq
- .mar
- .mas
- .mav
- .maw
- .mdb
- .mdf
- .mdn
- .mdt
- .mpd
- .mrg
- .mud
- .mwb
- .myd
- .ndf
- .nnt
- .nrmlib
- .ns2
- .ns3
- .ns4
- .nsf
- .nv
- .nv2
- .nvram
- .nwdb
- .nyf
- .odb
- .oqy
- .ora
- .orx
- .owc
- .p96
- .p97
- .pan
- .pdb
- .pdm
- .pnz
- .pvm
- .qcow2
- .qry
- .qvd
- .raw
- .rbf
- .rctd
- .rod
- .rodx
- .rpd
- .rsd
- .sas7bdat
- .sbf
- .scx
- .sdb
- .sdc
- .sdf
- .sis
- .spq
- .sql
- .sqlite
- .sqlite3
- .sqlitedb
- .subvol
- .te.tps
- .temx
- .tmd
- .trc
- .trm
- .udb
- .udl
- .usr
- .v12
- .vdi
- .vhd
- .vhdx
- .vis
- .vmcx
- .vmdk
- .vmem
- .vmrs
- .vmsd
- .vmsn
- .vmx
- .vpd
- .vsv
- .vvv
- .wdb
- .wmdb
- .wrk
- .xdb
- .xld
- .xmlff

Based on the examination of target file extensions during test execution in the custom-created folder, we found evidence of a file with the extension .arika, named after a hash corresponding to the modified file.



```
Date:        1/23/2027 7:36:53.8469138 AM
Thread:      6368
Class:       File System
Operation:   CreateFile
Result:      NAME NOT FOUND
Path:        C:\Users\REM\Desktop\akira_06_2025\folder\9b31aec229196ed0621982bddd36b83a.arika
Duration:    0.0000123

Desired Access:          Read Attributes
Disposition:             Open
Options:                 Open Reparse Point
Attributes:              n/a
ShareMode:               Read, Write, Delete
AllocationSize:          n/a
```

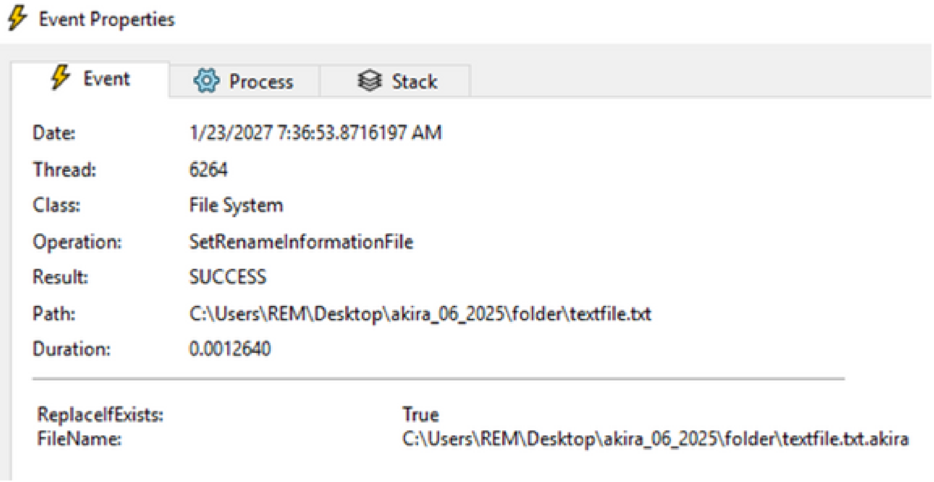
txt file .airka temp file creation



```
Date:        1/23/2027 7:36:53.8472695 AM
Thread:      6368
Class:       File System
Operation:   CreateFile
Result:      NAME NOT FOUND
Path:        C:\Users\REM\Desktop\akira_06_2025\folder\43f0d054b2edead7fde830ddcd2d59fb.arika
Duration:    0.0000110

Desired Access:          Read Attributes
Disposition:             Open
Options:                 Open Reparse Point
Attributes:              n/a
ShareMode:               Read, Write, Delete
AllocationSize:          n/a
```

png file .airka temp file creation

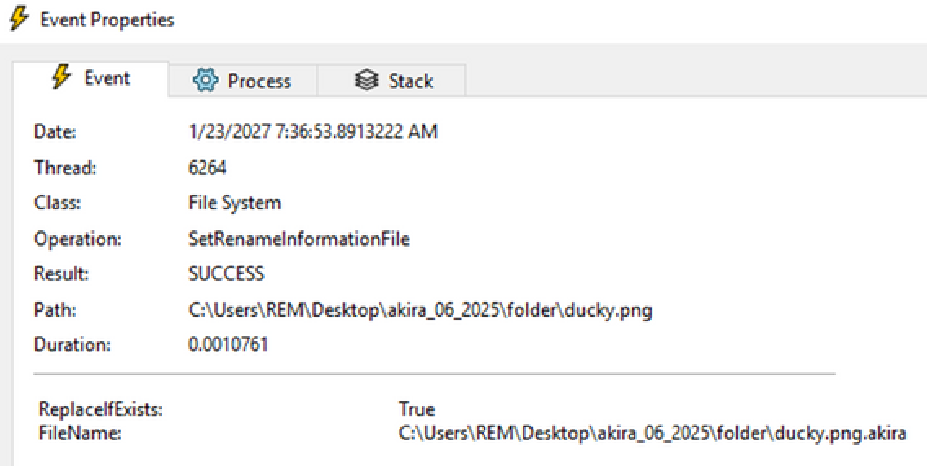
Subsequently, the malware renames the previously generated file, originally appended with the .arika extension, to the correctly encrypted file with the .akira extension.



Date: 1/23/2027 7:36:53.8716197 AM
Thread: 6264
Class: File System
Operation: SetRenameInformationFile
Result: SUCCESS
Path: C:\Users\REM\Desktop\akira_06_2025\folder\textfile.txt
Duration: 0.0012640

ReplaceIfExists: True
FileName: C:\Users\REM\Desktop\akira_06_2025\folder\textfile.txt.akira

txt .akira file renaming



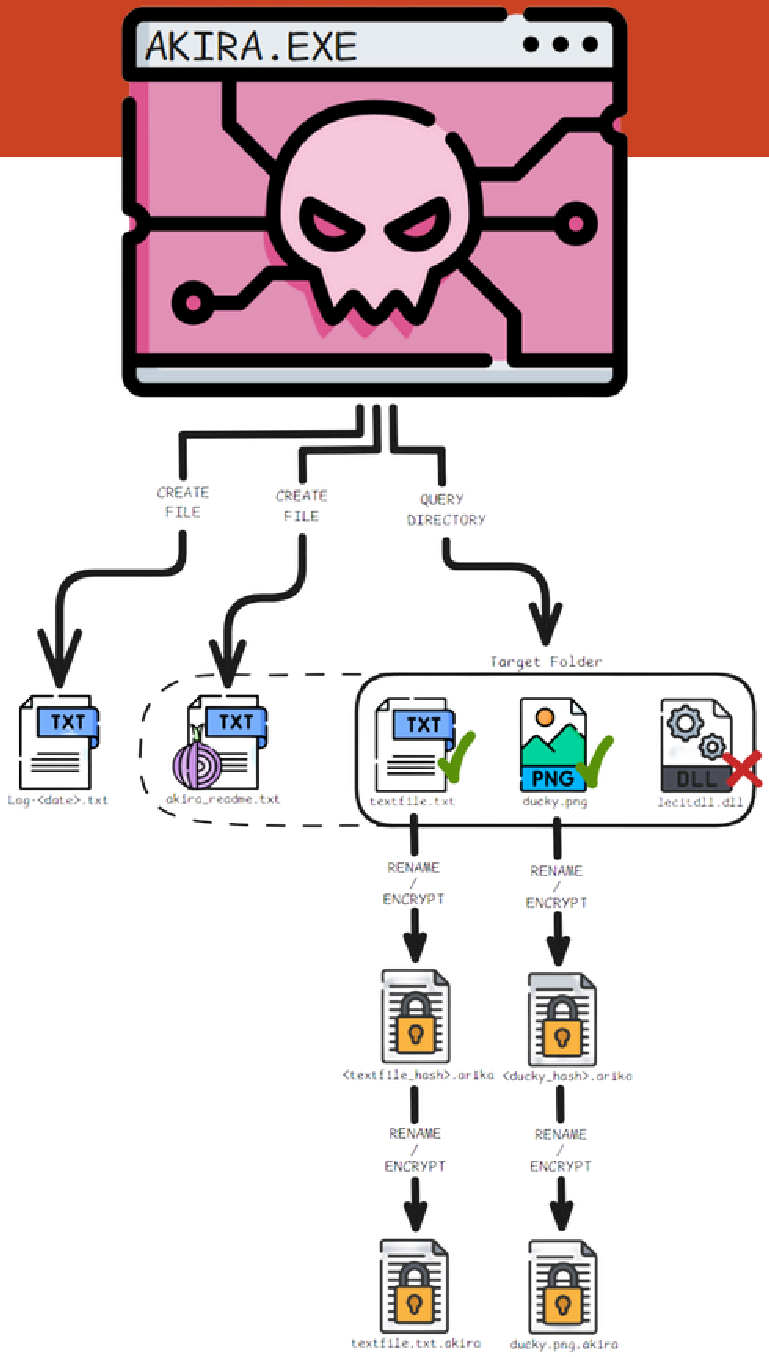
Date: 1/23/2027 7:36:53.8913222 AM
Thread: 6264
Class: File System
Operation: SetRenameInformationFile
Result: SUCCESS
Path: C:\Users\REM\Desktop\akira_06_2025\folder\ducky.png
Duration: 0.0010761

ReplaceIfExists: True
FileName: C:\Users\REM\Desktop\akira_06_2025\folder\ducky.png.akira

png .akira file renaming

6.2 Graphic Execution Overview

Below is a graphical overview of the ransomware's execution within the containment environment.



Execution Overview

6.3 Commands Executed

During the execution of the ransomware, the command aimed at deleting shadow copies is executed.

```
powershell.exe -Command "Get-WmiObject Win32_Shadowcopy |
Remove-WmiObject"
```

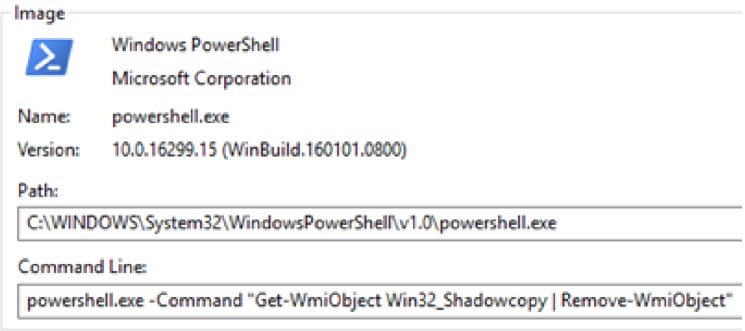


Image
Windows PowerShell
Microsoft Corporation
Name: powershell.exe
Version: 10.0.16299.15 (WinBuild.160101.0800)
Path:
C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe
Command Line:
powershell.exe -Command "Get-WmiObject Win32_Shadowcopy | Remove-WmiObject"

Shadowcopy erasing powershell command

This command removes system restore points and backup snapshots, making it impossible to restore files to a previous state using these mechanism. This technique is often used by ransomware and other malicious actors to inhibit system recovery and prevent victims from restoring their data after an attack.

A second command is also executed while the ransomware execution if it’s executed with the flag -dellog :

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ep bypass -
Command "Get-WinEvent -ListLog * | where { $_.RecordCount } | ForEach-Object
-Process{ [System.Diagnostics.Eventing.Reader.EventLogSession]:
:GlobalSession.ClearLog($_.LogName) }"
```

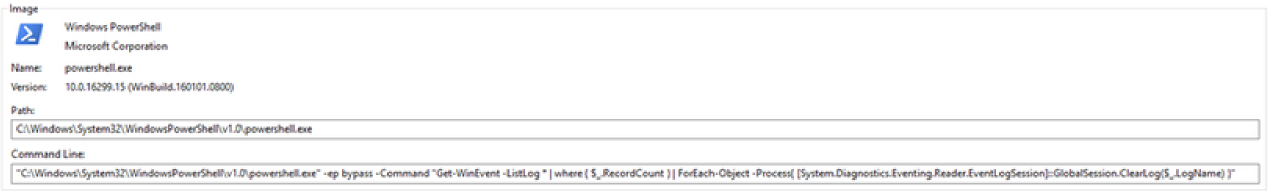


Image
Windows PowerShell
Microsoft Corporation
Name: powershell.exe
Version: 10.0.16299.15 (WinBuild.160101.0800)
Path:
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Command Line:
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ep bypass -Command "Get-WinEvent -ListLog * | where { $_.RecordCount } | ForEach-Object -Process{ [System.Diagnostics.Eventing.Reader.EventLogSession]::GlobalSession.ClearLog($_.LogName) }"

eventlogs erasing powershell command

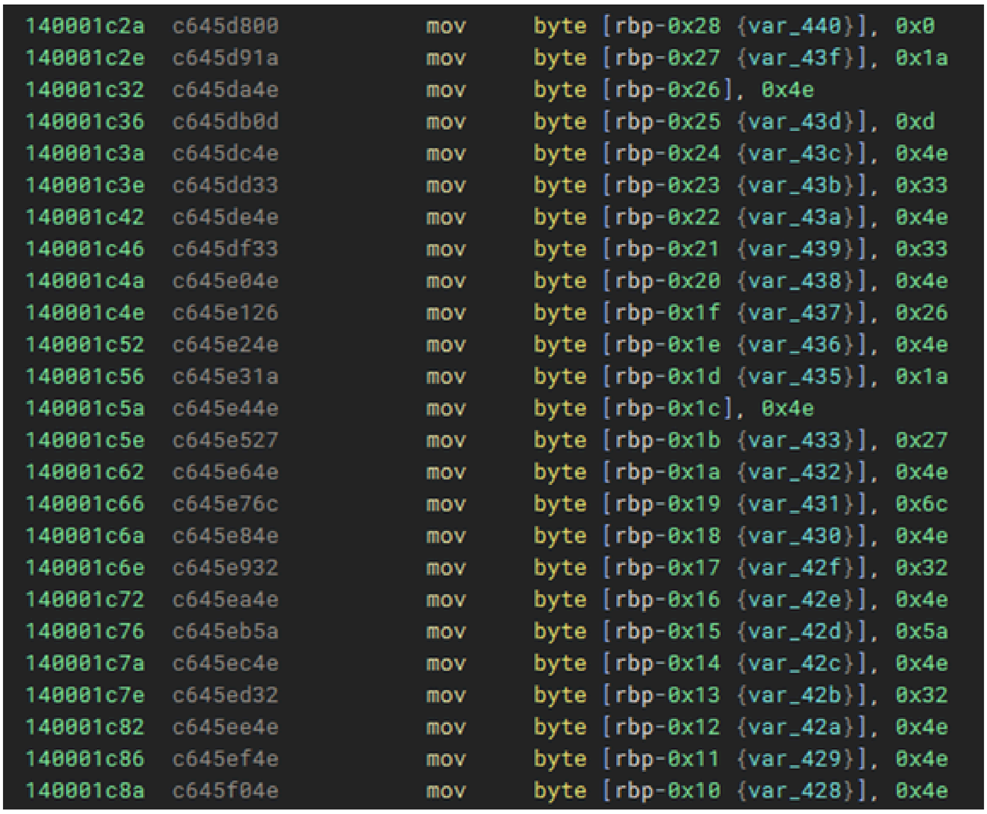
This command deletes all entries from every event log on the system that contains records. It is a commonly employed technique to obscure traces following unauthorized or malicious activities, since event logs are essential for forensic investigation and incident response.

7 Code Analysis

The following outlines the most distinctive techniques employed by ransomware. As previously discussed, this version differs notably from those observed in prior years during the group's initial emergence. It features enhanced stealth and more robust encryption. While the original version allowed for a predictable encryption process, making the development of a decryptor feasible, recent versions have reduce drastically this predictability, rendering earlier decryptors ineffective against new iterations of the malware.

7.1 Advanced String Obfuscation

Instead of embedding readable strings directly into the binary's data section, where they can be quickly spotted by security tools or analysts, the malware constructs these strings dynamically on the stack at runtime, protecting its internal logic.



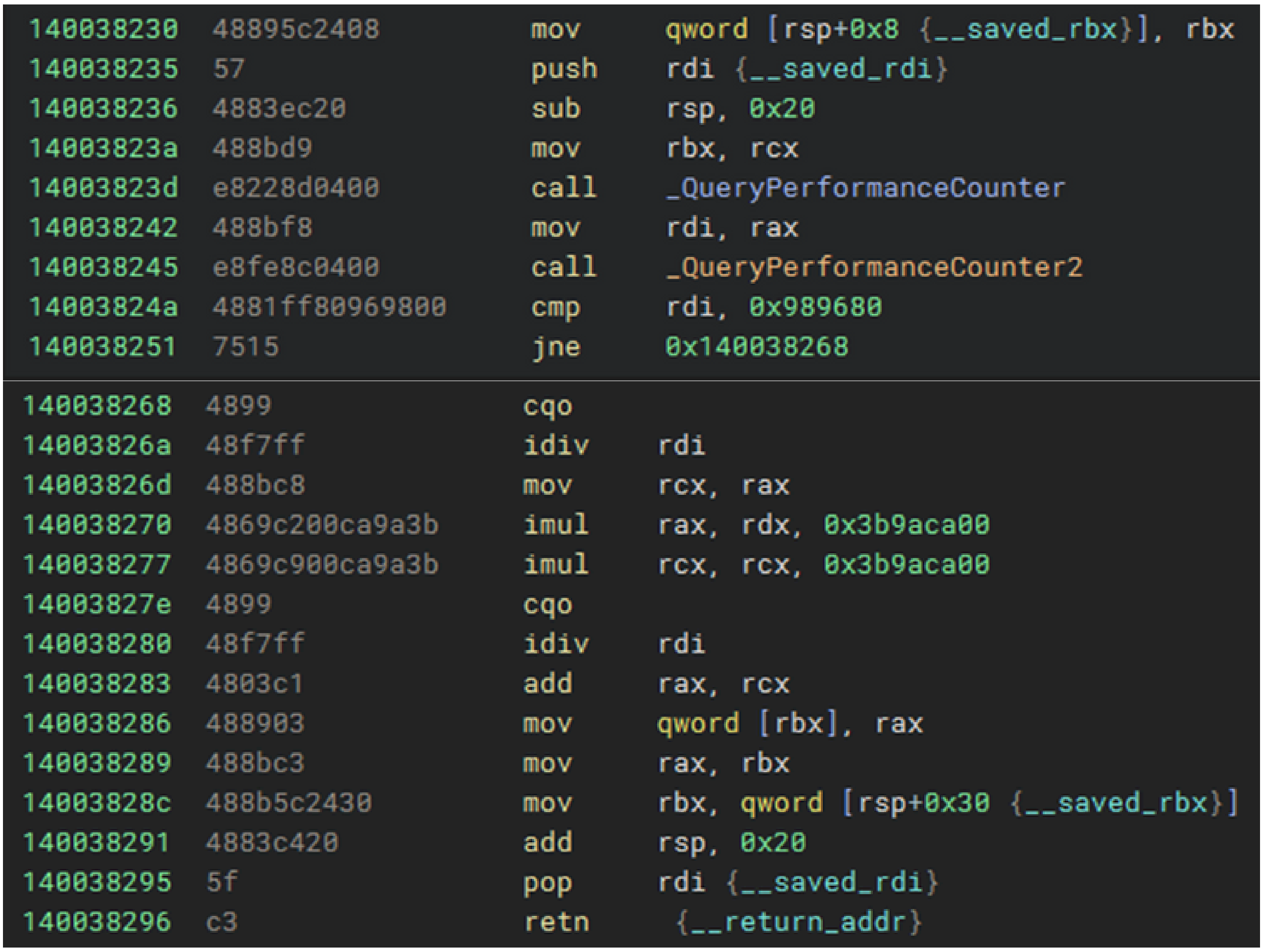
```
140001c2a  c645d800          mov     byte [rbp-0x28 {var_440}], 0x0
140001c2e  c645d91a          mov     byte [rbp-0x27 {var_43f}], 0x1a
140001c32  c645da4e          mov     byte [rbp-0x26], 0x4e
140001c36  c645db0d          mov     byte [rbp-0x25 {var_43d}], 0xd
140001c3a  c645dc4e          mov     byte [rbp-0x24 {var_43c}], 0x4e
140001c3e  c645dd33          mov     byte [rbp-0x23 {var_43b}], 0x33
140001c42  c645de4e          mov     byte [rbp-0x22 {var_43a}], 0x4e
140001c46  c645df33          mov     byte [rbp-0x21 {var_439}], 0x33
140001c4a  c645e04e          mov     byte [rbp-0x20 {var_438}], 0x4e
140001c4e  c645e126          mov     byte [rbp-0x1f {var_437}], 0x26
140001c52  c645e24e          mov     byte [rbp-0x1e {var_436}], 0x4e
140001c56  c645e31a          mov     byte [rbp-0x1d {var_435}], 0x1a
140001c5a  c645e44e          mov     byte [rbp-0x1c], 0x4e
140001c5e  c645e527          mov     byte [rbp-0x1b {var_433}], 0x27
140001c62  c645e64e          mov     byte [rbp-0x1a {var_432}], 0x4e
140001c66  c645e76c          mov     byte [rbp-0x19 {var_431}], 0x6c
140001c6a  c645e84e          mov     byte [rbp-0x18 {var_430}], 0x4e
140001c6e  c645e932          mov     byte [rbp-0x17 {var_42f}], 0x32
140001c72  c645ea4e          mov     byte [rbp-0x16 {var_42e}], 0x4e
140001c76  c645eb5a          mov     byte [rbp-0x15 {var_42d}], 0x5a
140001c7a  c645ec4e          mov     byte [rbp-0x14 {var_42c}], 0x4e
140001c7e  c645ed32          mov     byte [rbp-0x13 {var_42b}], 0x32
140001c82  c645ee4e          mov     byte [rbp-0x12 {var_42a}], 0x4e
140001c86  c645ef4e          mov     byte [rbp-0x11 {var_429}], 0x4e
140001c8a  c645f04e          mov     byte [rbp-0x10 {var_428}], 0x4e
```

stack strings code snippet

Malware authors use this technique primarily to evade static string detection and signature-based scanning, this dynamic assembly of strings forces analysts to engage in more time-consuming methods like debugging or emulation to uncover the true content, thereby slowing down or complicating the analysis by security researchers. This sample pushed into the stack an array with obfuscated bytes and then decode it in runtime, adding an additional layer of obfuscation.
Many other ransomware families have also used similar string obfuscation methods, including Conti, Ryuk, and REvil.

7.2 High-resolution timer conversion routine for cryptographic seed

Last versions of Akira ransomware are known to use QueryPerformanceCounter and QueryPerformanceFrequency for timing-related operations for cryptographic seed generation.



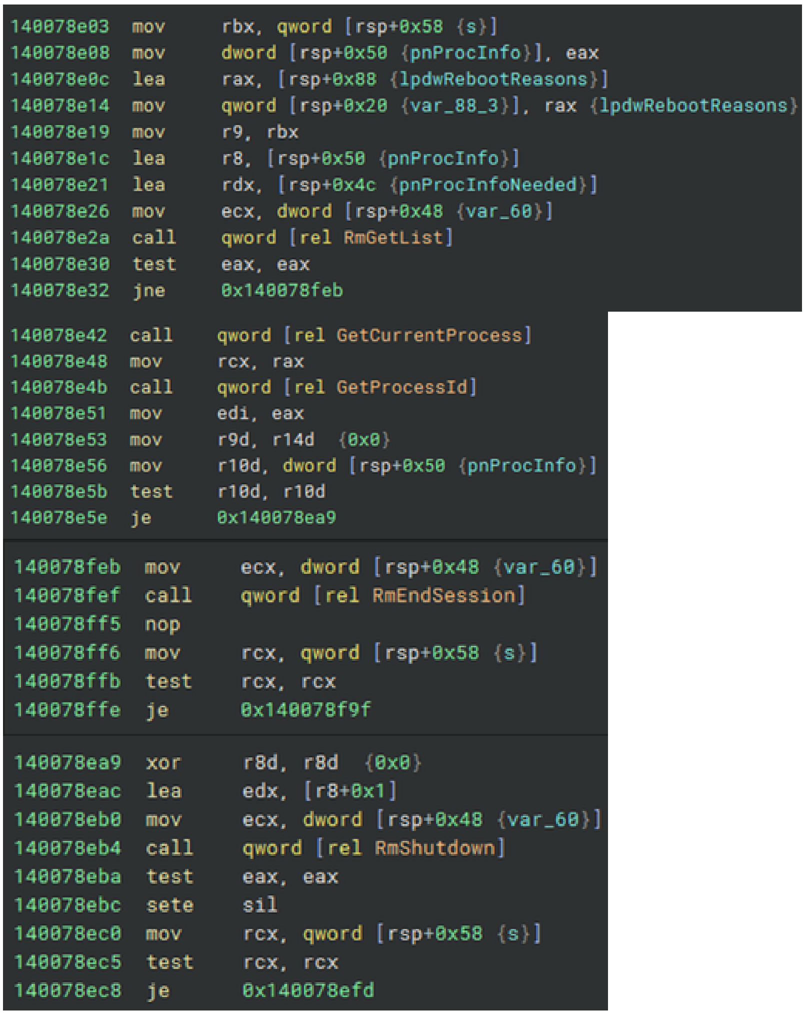
```
140038230  48895c2408       mov   qword [rsp+0x8 {__saved_rbx}], rbx
140038235  57               push  rdi {__saved_rdi}
140038236  4883ec20         sub   rsp, 0x20
14003823a  488bd9           mov   rbx, rcx
14003823d  e8228d0400       call  _QueryPerformanceCounter
140038242  488bf8           mov   rdi, rax
140038245  e8fe8c0400       call  _QueryPerformanceCounter2
14003824a  4881ff80969800   cmp   rdi, 0x989680
140038251  7515             jne   0x140038268

140038268  4899             cqo
14003826a  48f7ff           idiv  rdi
14003826d  488bc8           mov   rcx, rax
140038270  4869c200ca9a3b   imul  rax, rdx, 0x3b9aca00
140038277  4869c900ca9a3b   imul  rcx, rcx, 0x3b9aca00
14003827e  4899             cqo
140038280  48f7ff           idiv  rdi
140038283  4803c1           add   rax, rcx
140038286  488903           mov   qword [rbx], rax
140038289  488bc3           mov   rax, rbx
14003828c  488b5c2430       mov   rbx, qword [rsp+0x30 {__saved_rbx}]
140038291  4883c420         add   rsp, 0x20
140038295  5f               pop   rdi {__saved_rdi}
140038296  c3               retn   {__return_addr}
```

Time-related seed generation code snippet

It generates multiple timestamp seeds with nanosecond precision to strengthen key generation. If the seed is predictable or can be approximated, researchers can recreate the keys and decrypt the files, because the seed is based on the current time, it creates a huge space of possible values (over a billion per second), making brute force difficult and computationally expensive and complex.
A researcher recently succeeded in recovering the encryption key using GPU-accelerated brute-force techniques (https://github.com/yohanes/akira-bruteforce). However, threat actors have promptly updated the malware by integrating stronger encryption methods, thereby rendering the researcher’s decryptor ineffective against the latest versions of the ransomware.

7.3 Use of Windows Restart Manager API

Akira ransomware leverages the Restart Manager to gracefully terminate processes that might lock files targeted for encryption. This technique helps Akira ensure that files are not locked and can be encrypted without interference.



```
140078e03  mov     rbx, qword [rsp+0x58 {s}]
140078e08  mov     dword [rsp+0x50 {pnProcInfo}], eax
140078e0c  lea     rax, [rsp+0x88 {lpdwRebootReasons}]
140078e14  mov     qword [rsp+0x20 {var_88_3}], rax {lpdwRebootReasons}
140078e19  mov     r9, rbx
140078e1c  lea     r8, [rsp+0x50 {pnProcInfo}]
140078e21  lea     rdx, [rsp+0x4c {pnProcInfoNeeded}]
140078e26  mov     ecx, dword [rsp+0x48 {var_60}]
140078e2a  call    qword [rel RmGetList]
140078e30  test    eax, eax
140078e32  jne     0x140078feb

140078e42  call    qword [rel GetCurrentProcess]
140078e48  mov     rcx, rax
140078e4b  call    qword [rel GetProcessId]
140078e51  mov     edi, eax
140078e53  mov     r9d, r14d  {0x0}
140078e56  mov     r10d, dword [rsp+0x50 {pnProcInfo}]
140078e5b  test    r10d, r10d
140078e5e  je      0x140078ea9

140078feb  mov     ecx, dword [rsp+0x48 {var_60}]
140078fef  call    qword [rel RmEndSession]
140078ff5  nop
140078ff6  mov     rcx, qword [rsp+0x58 {s}]
140078ffb  test    rcx, rcx
140078ffe  je      0x140078f9f

140078ea9  xor     r8d, r8d  {0x0}
140078eac  lea     edx, [r8+0x1]
140078eb0  mov     ecx, dword [rsp+0x48 {var_60}]
140078eb4  call    qword [rel RmShutdown]
140078eba  test    eax, eax
140078ebc  sete    sil
140078ec0  mov     rcx, qword [rsp+0x58 {s}]
140078ec5  test    rcx, rcx
140078ec8  je      0x140078efd
```

Restart Manager usage code snippet

This snippet code of the function aimed to exploit Restart Manager API, first calls RmGetList to retrieve the list of processes currently using resources registered in a Restart Manager session, obtains the current process ID to potentially exclude itself from shutdown, checks if any processes are locking the resources, and if so, calls RmShutdown to forcibly shut down those processes to release the resources.

This approach is more reliable than classic brute-force termination because it targets only the specific processes locking a file, reducing system instability and increasing encryption success.

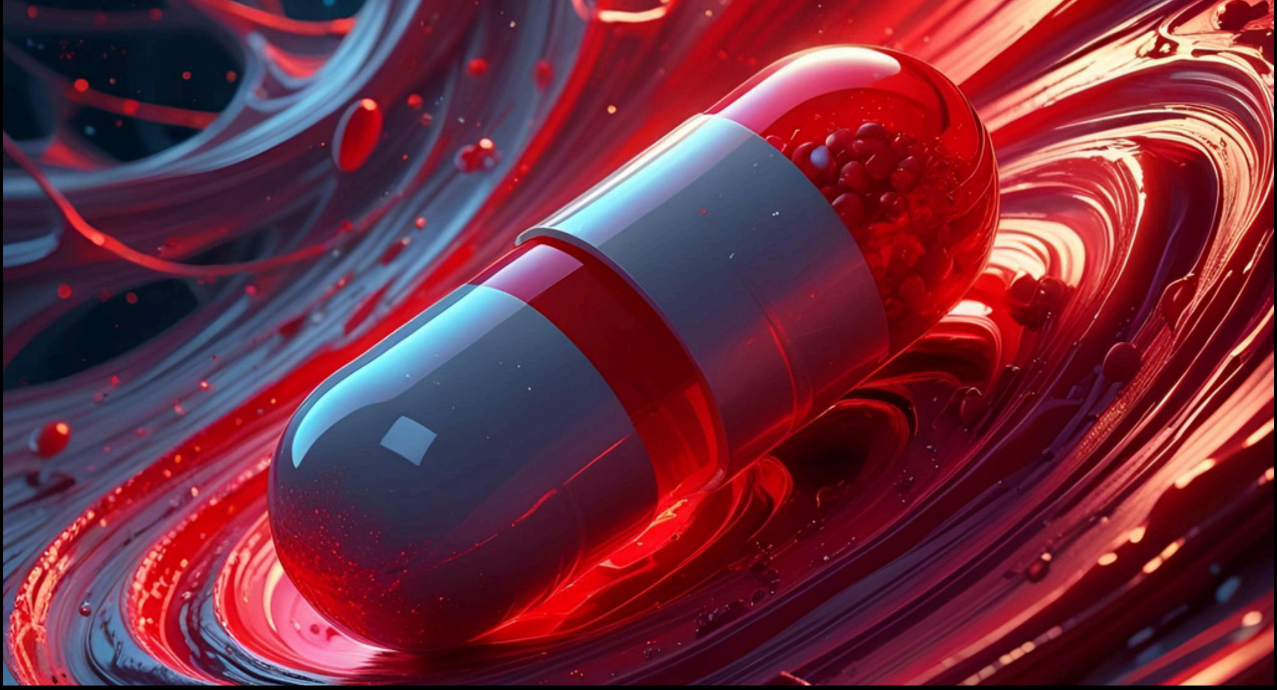
This kind of technique was used by another threat group, Conti ransomware's leaked source code revealed a function that dynamically loads the Restart Manager library in order to proceed to find and terminates those processes to release file locks. While Akira has evolved and introduced new features, its *roots* appear to be based on or heavily influenced by leaked Conti source code, making it effectively a descendant or spin-off of Conti ransomware.

8 IOCs

Type	Name	IOC
File	a.exe	MD5: 5337D181CE59D7DDA9CC955B2DDE48A7 SHA1: 232AC61A697D776BEBB1541634E80B9A219ECFCD SHA256: 9E0D9E831E14EFA69941A2CA5DD3131B466DBF737A8936C34411D0EA6330D9BD
Domain	DLS	akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad[.]onion
Domain	Chat platform	akiralkzxzq2dsrzsrvbr2xgbbu2wgsmxryd4csgfameg52n7efvr2id[.]onion

9 Yara Rule

```
rule Akira
{
 meta:
    author = "5hid"
    comment = "Detects Akira Ransomware"
    description = "Akira Payload"
    sample_date = "Wed Mar 19 13:53:17 2025”
    copyright = "Sorint.Sec"

 strings:
 $x1 = "https://akira" ascii
 $x2 = ".arika" ascii
 $x3 = ".akira" ascii
 $x4 = "akira_readme.txt" ascii nocase
 $s1 = "Get-WmiObject Win32_Shadowcopy | Remove-WmiObject" ascii
 $s2 = "Win32_ProcessStartup" fullword wide
 $s3 = "Command line to argvW failed!" ascii wide
 $s4 = "--encryption_percent" ascii
 $s5 = "--dellog" ascii
 $s6 = { 43 6F 6D 70 61 72 65 53 74 72 69 6E 67 45 78 }
 $s7 = { 47 65 74 2D 57 6D 69 4F 62 6A 65 63 74 20 57 69 6E 33 32 5F 53 68 61 64 6F 77
63 6F 70 79 20 7C 20 52 65 6D 6F 76 65 2D 57 6D 69 4F 62 6A 65 63 74 }
 $s8 = { 48 69 20 66 72 69 65 6E 64 73 }
 $s9 = ".onion" ascii
 $s10 = "No path to encrypt" ascii

 condition:
    uint16 ( 0 ) == 0x5a4d and ( 3 of ( $x* ) or ( 1 of ( $x* ) and 4 of ( $s* ) ) or 6 of ( $s* ) )
}
```



Author

Francesco Facoetti - TID&R Manager

Document Information

Sorint.SEC S.R.L. si adopera per garantire che le informazioni contenute in questo documento siano corrette e, sebbene ogni sforzo sia fatto per garantire l'esattezza di tali informazioni non si assume alcuna responsabilità per eventuali errori od omissioni nella stessa. Tutti i marchi e nomi di prodotti utilizzati nel presente documento sono pertanto riconosciuti.

Sorint.SEC srl endeavors to ensure that the information contained in this document is correct, and whilst every effort is made to ensure the accuracy of such information it accepts no liability for any error or omission in the same. All trademarks and product names used within this document are hereby acknowledged.

SORINT SEC