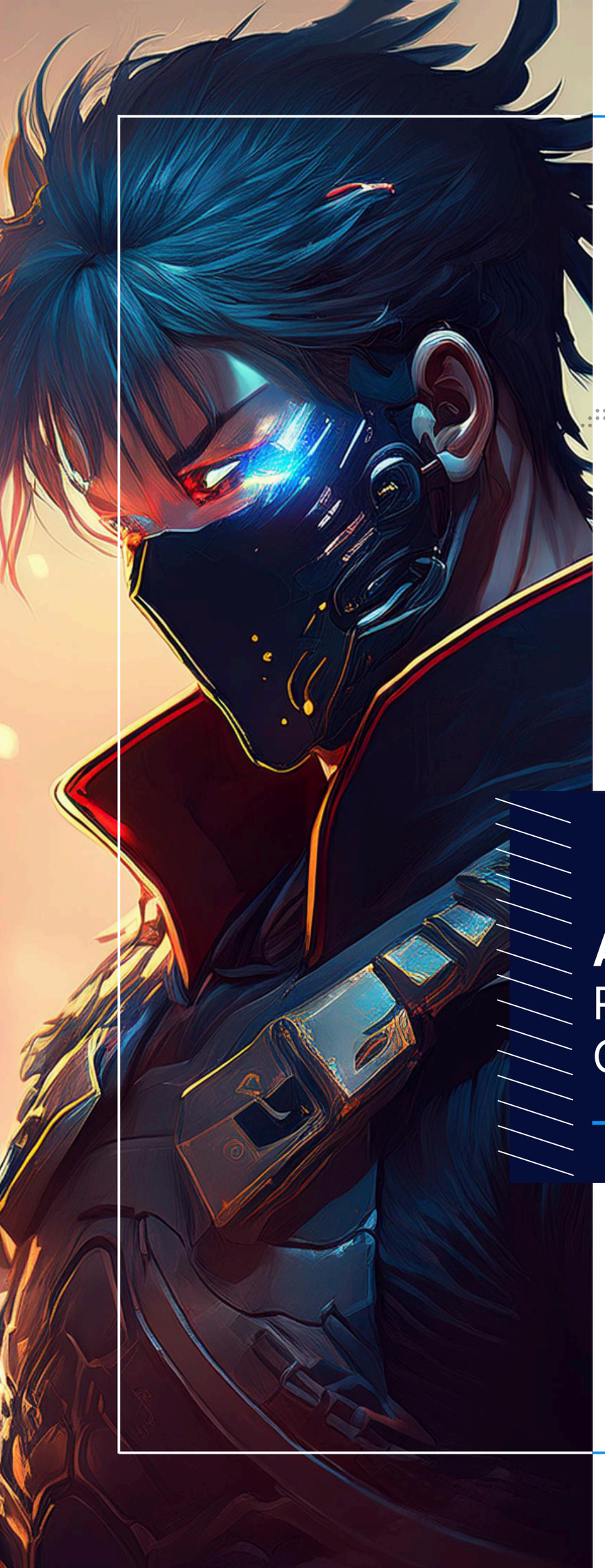


ThreatMon
Under Cyber Wings

AKIRA
RANSOMWARE GROUP REPORT

TABLE OF **CONTENTS**

Who?

The Akira ransomware group is a cybercrime organization that emerged in March 2023. It operates with a primary motive of financial gain. The group primarily targets organizations in the United States and Canada across sectors such as healthcare, finance, education, and manufacturing. The Akira ransomware group aims to gain a strategic advantage by specifically targeting financial institutions and government-related organizations. In Ecuador, targets include critical infrastructure and financial service providers.

What?

Akira employs a double-extortion ransomware model, encrypting victims' data and exfiltrating it. The group demands ransoms ranging from $200,000 to $4 million in exchange for decrypting files or refraining from publishing sensitive data. The first version of the Akira ransomware was written in C++ and appended files with the '.akira' extension, creating a ransom note named 'akira_readme.txt,' partially based on the Conti V2 source code.
On July 2, 2023, a version was released that fixed the decryption problem. Since then, the new version has been found to be written in Rust, this time named 'megazord.exe' and changing the extension for the encrypted files to '.powerranges'.

Where?

Initially targeting Windows systems, Akira expanded its operations in April 2023 to include VMware ESXi virtual machines. The group has impacted over 250 organizations worldwide, spanning industries such as services, manufacturing, education, construction, critical infrastructure, finance, healthcare, and legal sectors.
When?
Akira has been active since March 2023 and significantly intensified its attacks throughout 2024, impacting numerous sectors globally.

How?

The Akira ransomware group employs a range of sophisticated techniques:

- Initial Access: Utilizing phishing emails, exploiting vulnerabilities, and using compromised credentials.
- Lateral Movement: Exploiting critical vulnerabilities such as CVE-2024-40766 (SonicWall SonicOS), CVE-2023-20269 (Cisco VPN), and CVE-2023-48788 (FortiClientEMS), CVE-2023-27532 (Veeam Backup & Replication), CVE-2024-40711 (Veam Backup & Replication (VBR) Servers).
- Data Exfiltration: Exfiltrating sensitive information before encryption.
- Robust Encryption: Deploying strong encryption algorithms to ensure the encrypted files are irrecoverable without a decryption key.

Many of Akira's initial access vectors use brute force attempts on Cisco VPN devices (which only use single-factor authentication).

Additionally, the exploitation of CVEs: CVE-2019-6693 and CVE-2022-40684 were detected for first access.

Group Site
akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion

Vulnerabilities Exploited by Akira

Vendor	Product	CVE	Source
Cisco	ASA & FTD	CVE-2023-20269	cisco.com
Cisco	ASA & FTD	CVE-2023-20263	blog.talosintelligence.com
Cisco	ASA & FTD	CVE-2020-3259	cisa.gov
Fortinet	FortiOS	CVE-2022-40684	stairwell.com
Fortinet	FortiOS	CVE-2019-6693	stairwell.com
Fortinet	FortiClient	CVE-2023-48788	blog.talosintelligence.com
SonicWall	SonicOS SSL-VPN	CVE-2024-40766	arcticwolf.com
Veeam	Backup & Replication	CVE-2024-40711	@SophosXOps
Veeam	Backup & Replication	CVE-2023-27532	sophos.com
VMware	ESXi	CVE-2024-37085 ("ESX Admins")	microsoft.com
VMware	vSphere Client	CVE-2021-21972	qualys.com

Tool Used By Akira Ransomware Group

Discovery	RMM Tools	Defense Evasion	Credential Theft
Advanced IP Scanner	AnyDesk	PowerTool	DonPAPI
Masscan	MobaXterm	Zemana Anti-Rootkit	LaZagne
ReconFTW	Radmin		Mimikatz
SharpHound	RustDesk		
SoftPerfect NetScan			

OffSec	Networking	Exfiltration
Impacket	Cloudflared	FileZilla
	OpenSSH	MEGA
	Ngrok	RClone
		Temp[.]sh
		WinSCP

1. **Cloudflare Tunnel:**
   - Used to gain initial access to Endpoint 2.
   - **Command:** C:\Users\[REDACTED]\Documents\Cloudflare.exe tunnel run --token [REDACTED]
2. **Advanced IP Scanner:**
   - Used to scan the network and identify targets.
   - **Command:** "C:\Users\[REDACTED]\AppData\Local\Temp\Advanced IP Scanner 2\advanced_ip_scanner.exe" /portable "C:/Users/[REDACTED]/Documents/" /lng en_us
3. **Win.exe:**
   - Deployed ransomware to identified targets.
   - **Command:** "C:\Users\[REDACTED]\Documents\win.exe" -s=C:\Users\[REDACTED]\Documents\path2.txt -n=20 -remote

Latest Attacks of the Akira Ransomware Group

Victim	Sector	Country
Archie Cochrane Ford	Consumer Services	United States
OL Products	Cosmetics	United States
A Geradora	Energy	Brazil
Toscano Law	Law	United States
Polskie Wydawnictwo Muzyczne	Music	Poland
Time Machine INC	Industry	United States
National Air Vibrator	Manufacturing	United States
Great Plains Bank	Financial Services	United States
Rob Levine & Associates	Law	United States
Diferencial Energia	Energy	Brazil
Luxor Capital Group	Financial Services	United States
Matagrano	Manufacturing	United States
Renée Blanche	Cosmetics	Italy
Nova Pole International	Manufacturing	United States
Matandy	Manufacturing	United States
Corporación BJR	Industry	Mexico
Proyectos y Seguros	Financial Services	Spain
Cipla	Healthcare	South Africa
Consumers Builders Supply	Construction	United States
ECBM	Financial Services	United Kingdom
Pelstar	Healthcare	United States
Pb Loader	Construction	United States
Jamaica Bearings Group	Logistics	United States

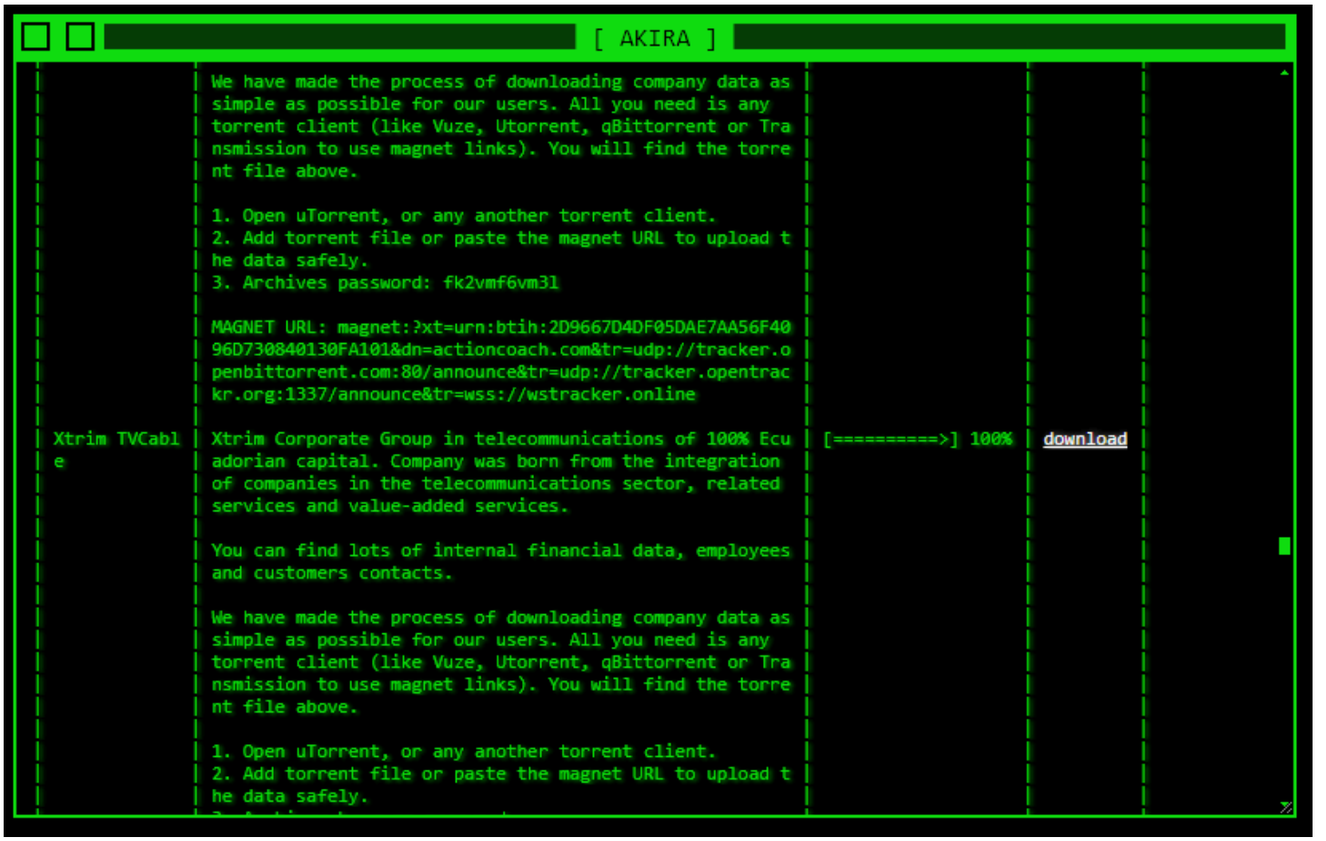
The attacks in December were discussed.

Latest Ransomware Attacks in Ecuador

Victim	Sector	Group	Date
Biodimed	Healthcare	Stormous	2024-12-10
Frigopesca	Agriculture and Food Production	Ransomhub	2024-12-04
Xtrim TVCable	Telecommunication	Akira	2024-11-14
todoagro	Agriculture and Food Production	Spacebears	2024-04-28
Grupocreativo Herrera	Telecommunication	Qilin	2024-04-02
isspol.gov	Public Sector	Lockbit3	2024-02-12

The attacks in 2024 were discussed.

Xtrim TVCable Attack in Ecuador by Akira

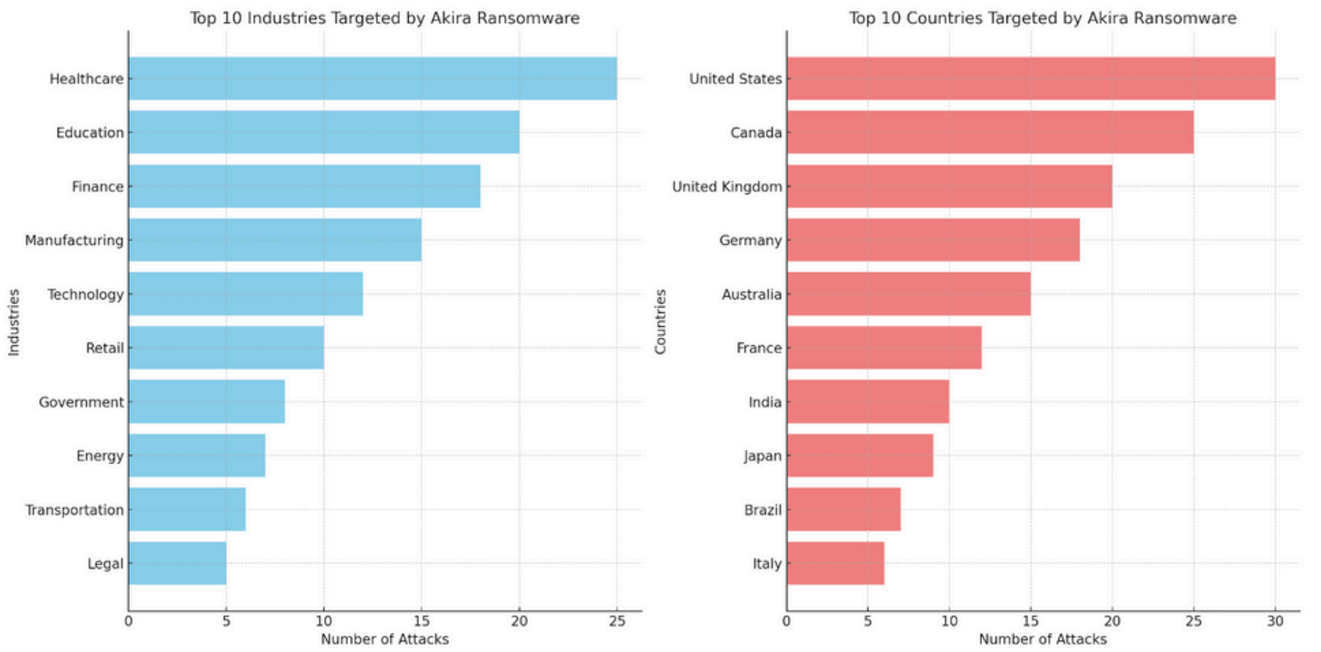


Akira Ransomware Group announced that it attacked Xtrim TVCable on 2024-11-14. The Akira group, which then expected a ransom, published all the data publicly after failing to receive the ransom expectation.

The relevant data included financial data, employees and customers contacts.

Targeted Industries and Countries

Akira's attacks have targeted industries like information technology, finance, education, healthcare. **The group typically infiltrates systems using weak VPN credentials or compromised remote desktop protocols (RDP).**



Graph of the Sectors and Countries targeted by Akira Ransomware the Most

The above graph shows the top 10 industries and top 10 countries targeted by the Akira Ransomware group. The industry most targeted by the Akira Ransomware group is healthcare, and the country most targeted by the group is the United States.

Ransomware Analysis

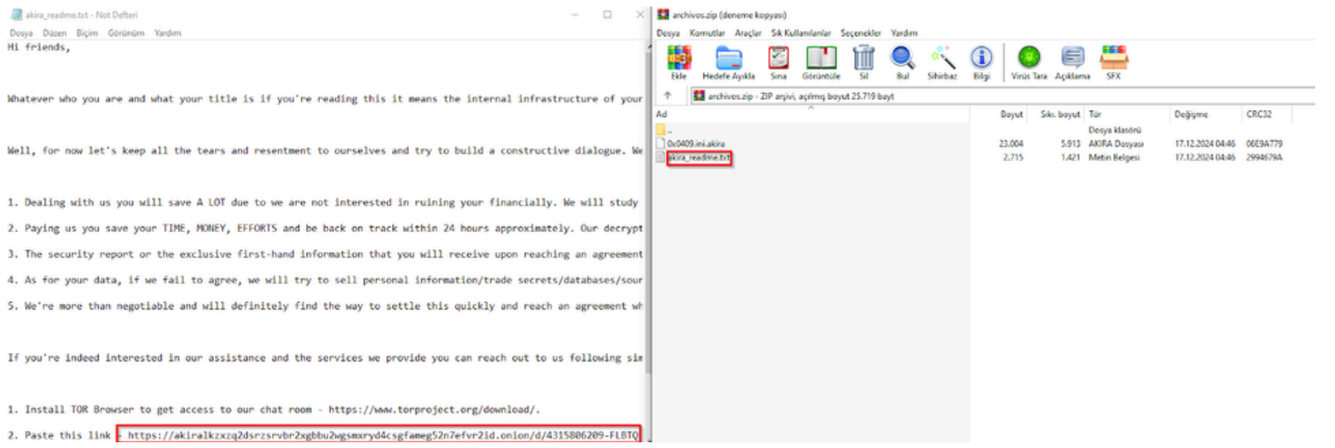


Image of Akira Ransomware Group

Within the compromised system, the extension, the readme file and the content of the file indicate that the group that carried out the attack is the Akira Ransomware group.

Content of the Readme File

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.
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 your 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 a 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 accidently 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 a great value, since NO full audit of your network will show you the vulnerabilities that we've managed to detect and used in order to get into, identify backup solutions and upload 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 ones. Then all of this will be published in our blog - https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion.

5. We're more than negotiable and will definitely find the way to settle this quickly and reach an agreement which will satisfy both of us.

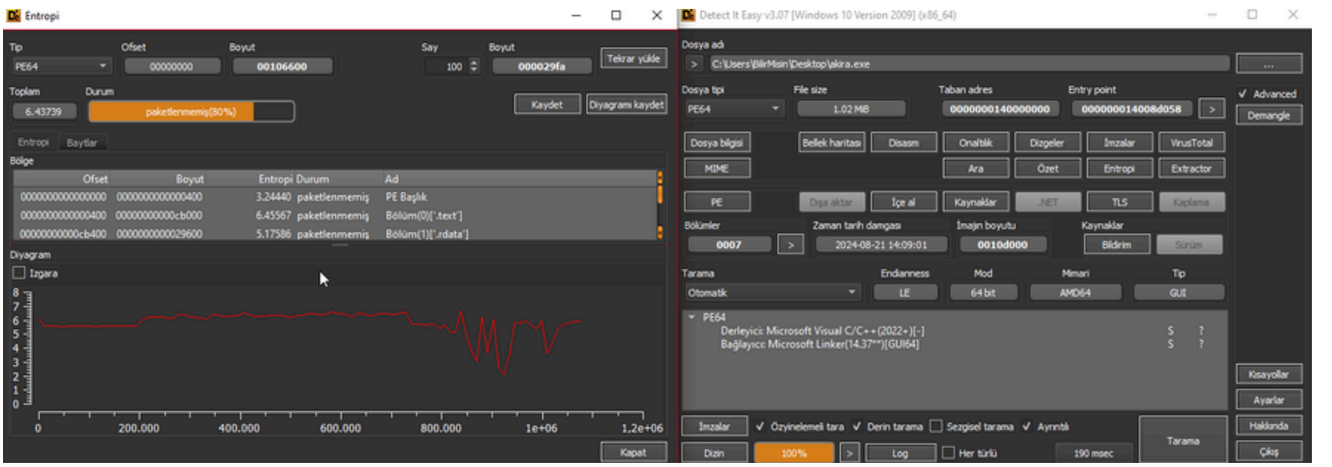
If you're indeed interested in our assistance and the services we provide you can reach out to us following simple instructions:

1. Install TOR Browser to get access to our chat room - https://www.torproject.org/download/.

2. Paste this link - https://akiralkzxzq2dsrzsrvbr2xgbbu2wgsmxryd4csgfameg52n7efvr2id.onion/d/4315806209-FLBTQ

3. Use this code - 1312-FJ-WDQH-PHOW - to log into our chat.

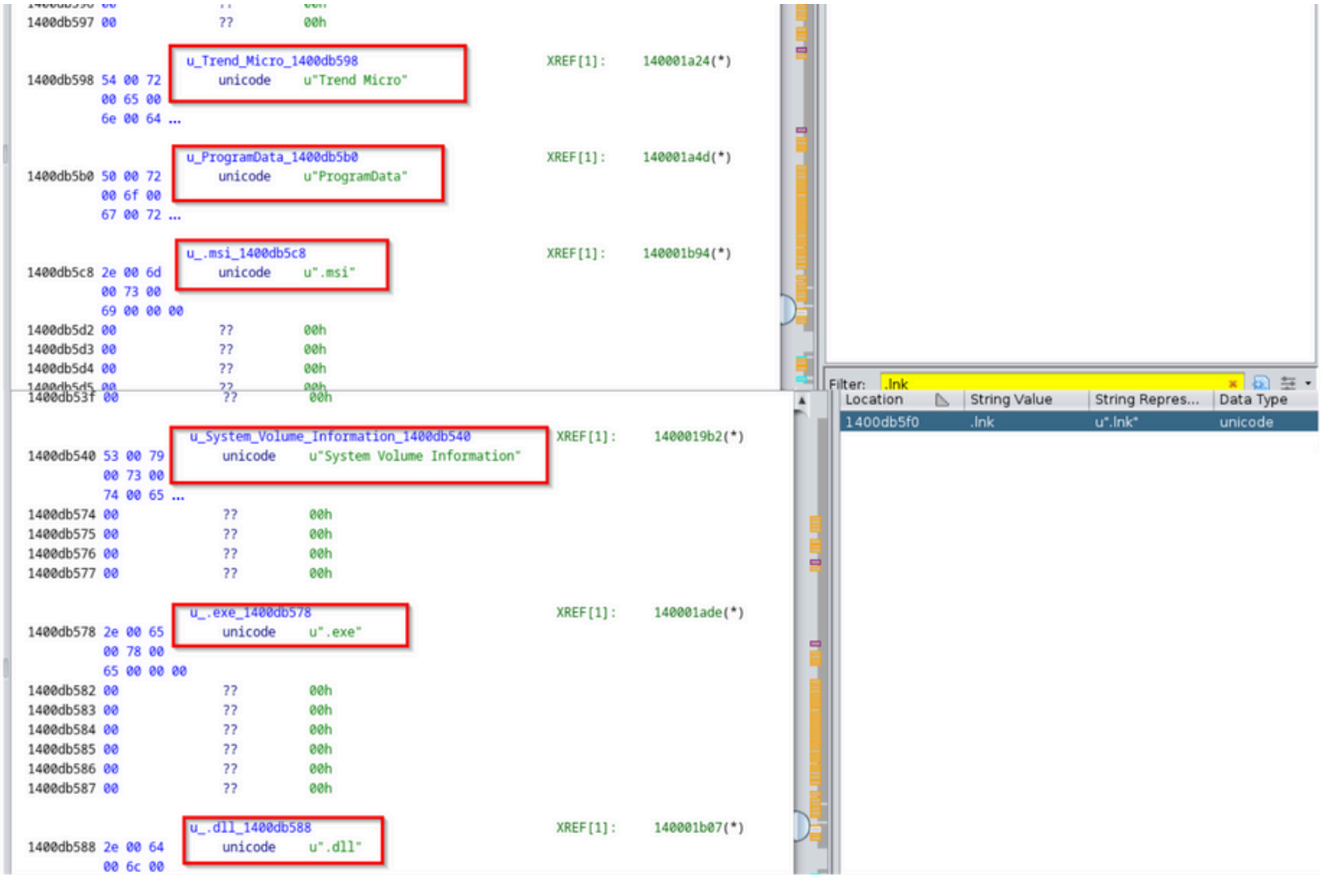
Keep in mind that the faster you will get in touch, the less damage we cause.



Basic Characteristics of Akira Ransomware

Akira ransomware is compiled in C++ language, has a disk space of 1.02MB and the sample is not packed.

File Type	PE64 Windows Executable
Detected Language	C++
File Size	1.02MB
PE Size	1.02MB
Packer	Not Packed
SHA256	74fbb7885ee486028fe2723f95911474b771f361b2b40ddb77c46f252059c696
MD5	ab6a985dbef013596ac79ca5117ef77c
ImpHASH	9b9e1545a27f74c7e825990e6d713212



Analysis I

During the static analysis process, it was found that akira ransomware contains an exclusion list for some files and folders. The files and directories that Akira Ransomware does not encrypt are as follows:

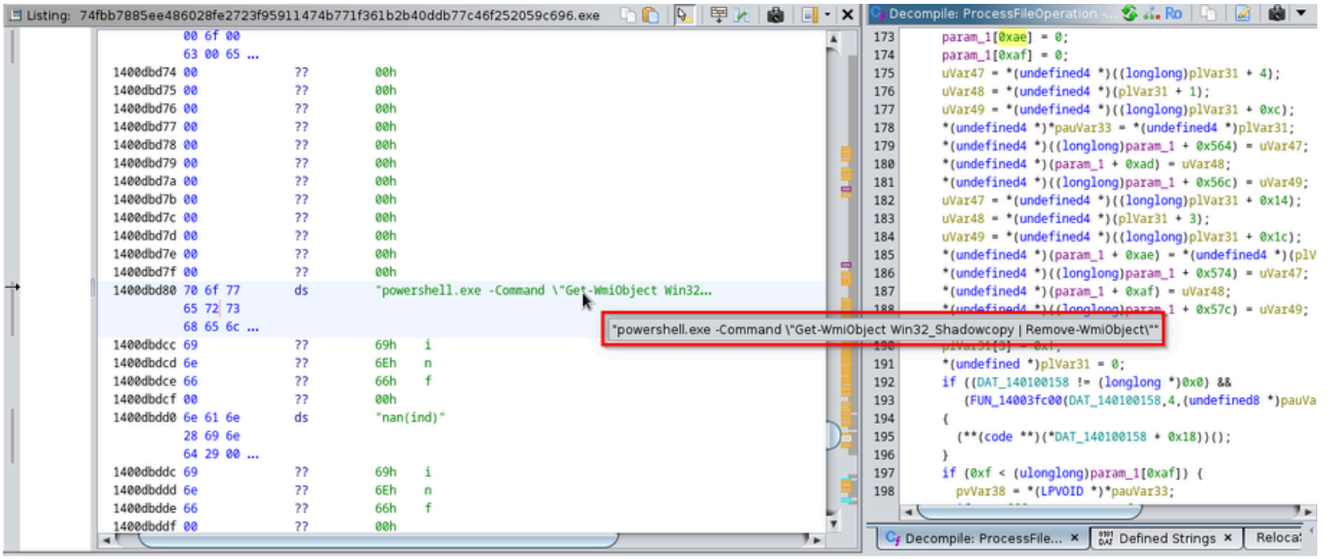
Folders Excluded by Akira Ransomware:

```
System Volume Information, Boot, $Recycle.Bin, Winnt, $RECYCLE.BIN,
Windows, Trend Micro, Temp, Thumb
```

Files Excluded by Akira Ransomware:

```
.msi, .sys, .dll, .lnk, akira_readme.txt, .exe
```

Akira Ransomware is observed to encrypt all other data on the system.

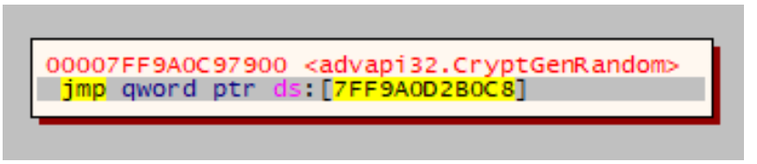


Analysis II

In the analyzed ransomware sample, it was determined that system backups were deleted at the rst stage with the **Get-WmiObject Win32_Shadowcopy | Remove-WmiObject** command via PowerShell

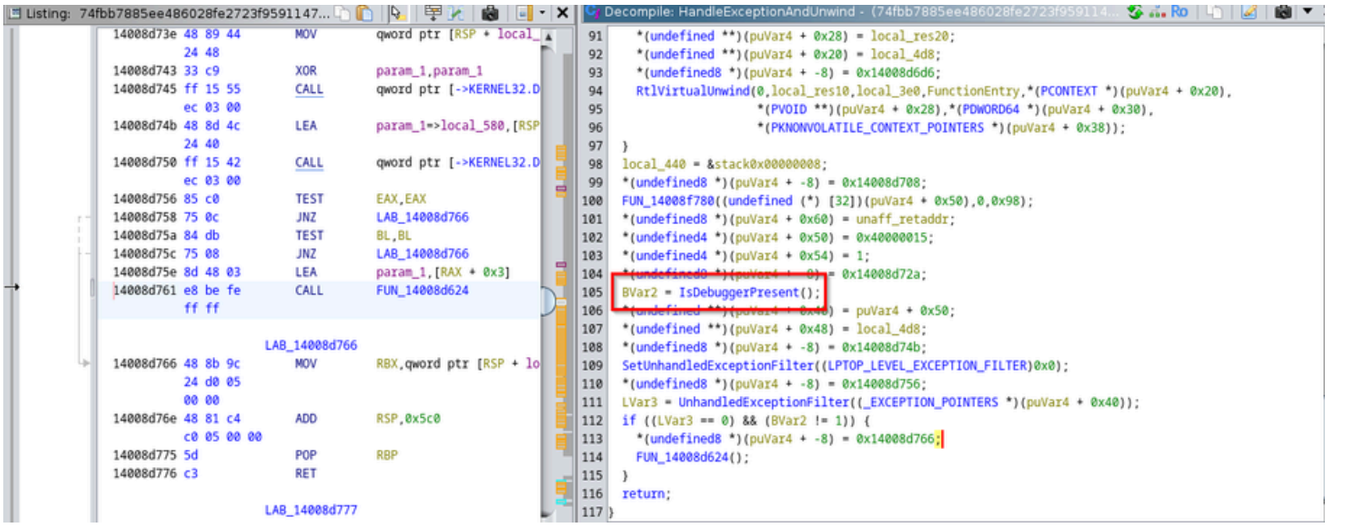
Detected Powershell Command:

```
Get-WmiObject Win32_Shadowcopy | Remove-WmiObject
```



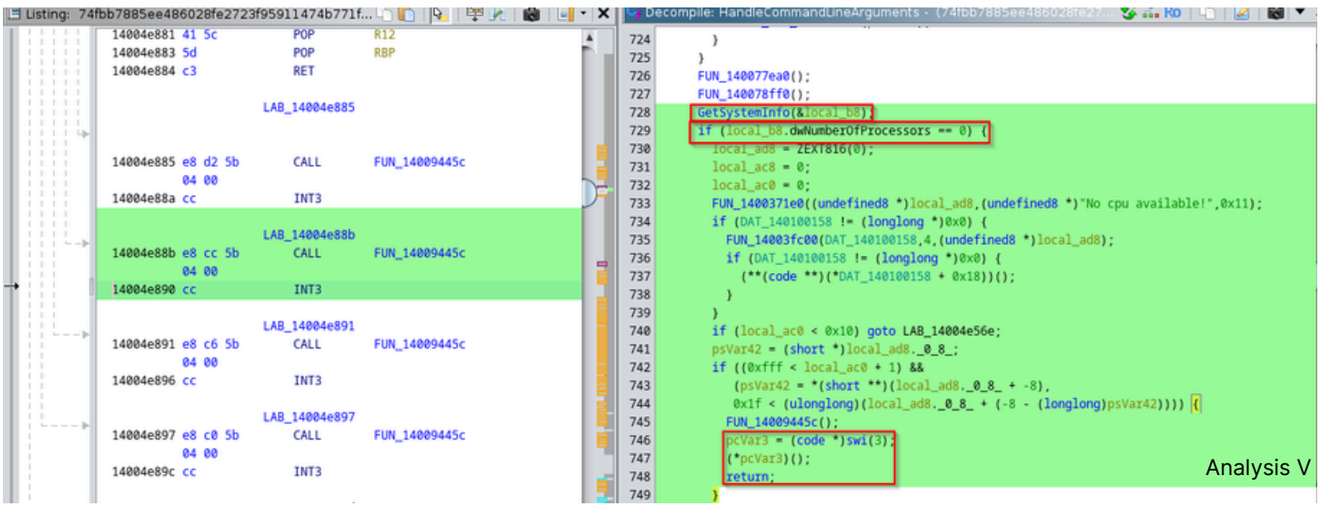
Analysis III

Akira Ransomware has been found to use the CryptGenRandom() function in its execution process. This function is used to generate random number data and is used by Akira Ransomware for key generation.



Analysis IV

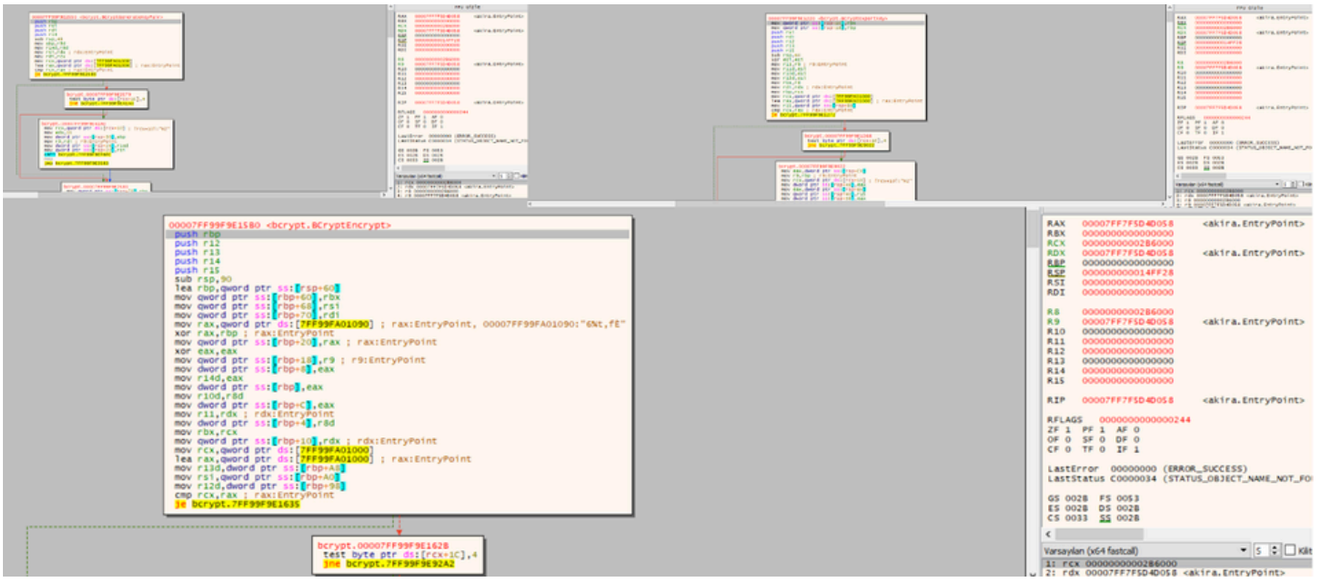
The IsDebuggerPresent() API has been detected in the code structure of Akira Ransomware. This indicates that the ransomware checks the debugger on the system it is running on.

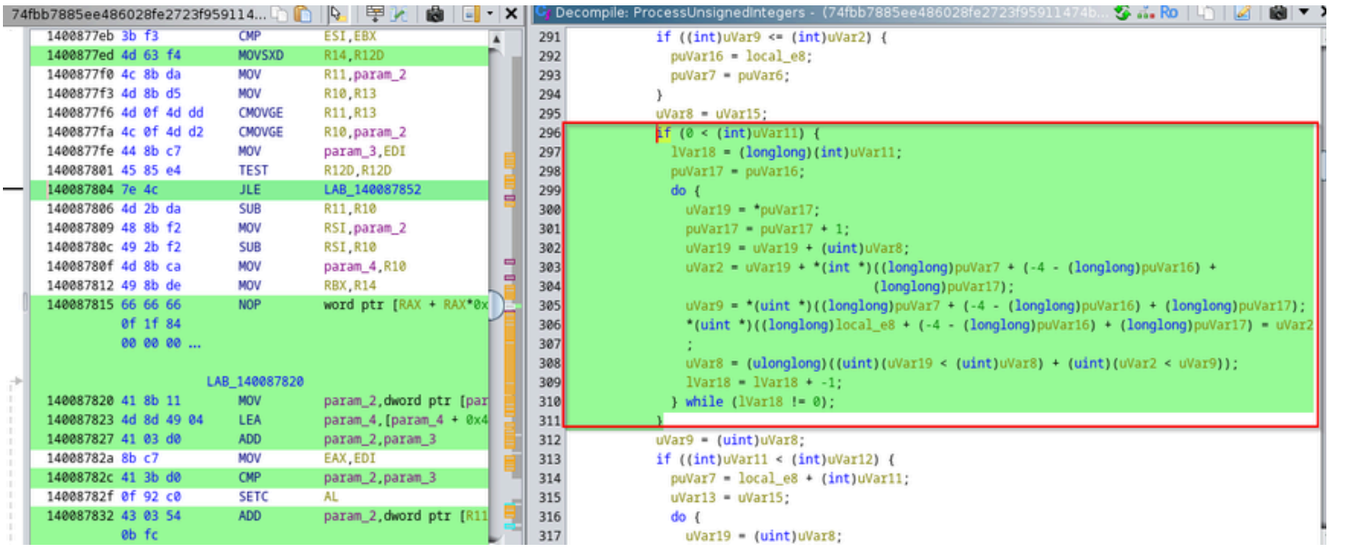


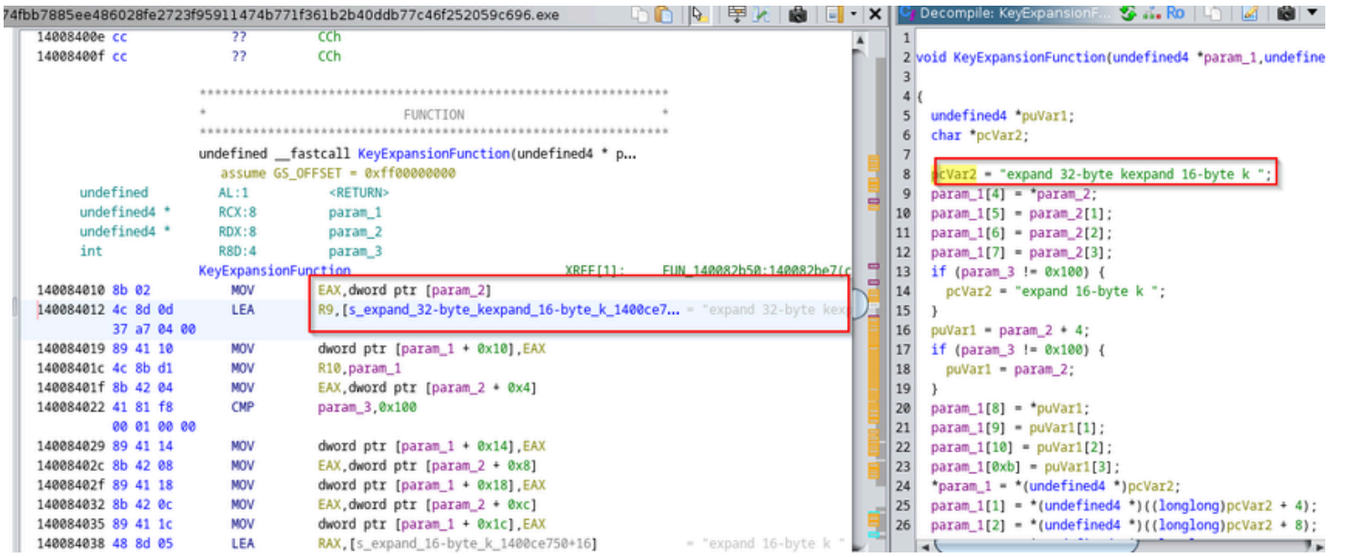
Analysis V

Within the code structure and execution structure of Akira Ransomware, it is observed that APIs such as GetSystemInfo(), DeviceIOControls(), NtQuerySystemInformation() are used to control system properties. In particular, when the code structure including the GetSystemInfo API detected on Ghidra is analyzed, it is determined that it checks that the system it is run on does not show an anomaly and terminates itself in case of an anomaly. Other APIs detected on x32dbg show virtual machine detection feature.

Detected Encryption Algorithms:







Analysis VI

It has been found that the ChaCha algorithm is used to encrypt les in the static code structure of Akira Ransomware. It was also observed that the symmetric key generated during the dynamic analysis process was encrypted with RSA 4096.

IOC (Indicator of Compromise)

File Name	Hash (SHA-256)	Description
w.exe	d2fd0654710c27dcf37b6c1437880020824e161dd0bf28e3a133ed777242a0ca 56f1014eb2d145c957f9bc0843f4e506735d7821e16355bcfbb6150b1b5f39db 6270cef0c8cc45905556c40c9273391d71ef8d73c865d44d2254a8a4943ae5b4 77fe1619aa07d2ab169a2fa23feb22d7433bf07e856cda1402cf60205beddd7f 99c1cd740fa749a163ce8cdf93722191c4ba5d97de81576623a8bbcb622473d6 ee0a27f3de6f21463f8125dbfc95268ff995ef8ea464660d67cf9f77e240e1ab	Akira ransomware
Win.exe	dcfa2800754e5722acf94987bb03e814edcb9acebda37df6da1987bf48e5b05e b7bbfb66338a3413f981561115bd8ef8a4014479bcc320de563499cfc73a3de2 ca651d0eb676923c3b29190f7941d8d2ac8f14e4ad6c26c466069bbc59df4d1d d5558ec7979a96fe1ddcb1f33053a1ac3416a9b65d4f27b5cc9fd0a816296184 ffcddd8544bca0acde69f49abd1ea9dbee5f4eb73df51dd456b401c045a0b6af	Akira ransomware encryptor
AnyDesk.exe	bc747e3bf7b6e02c09f3d18bdd0e64eef62b940b2f16c9c72e647eec85cf0138	Remote Desktop Application
Gcapi.dll	73170761d6776c0debacfbbc61b6988cb8270a20174bf5c049768a264bb8ffaf	DLL File that assists with the execution of AnyDesk.exe
Sysmon.exe	1b60097bf1ccb15a952e5bcc3522cf5c162da68c381a76abc2d5985659e4d386	Ngrok tool for persistence
Rclone.exe	aaa647327ba5b855bedea8e889b3fafdc05a6ca75d1cfd98869432006d6fecc9	Exfiltration tool

Winscp.rnd	7d6959bb7a9482e1caa83b16ee01103d982d47c70c72fdd03708e2b7f4c552c4	Network file transfer program
Megazord	ffd9f58e5fe8502249c67cad0123ceeeaa6e9f69b4ec9f9e21511809849eb8fc dfe6fddc67bdc93b9947430b966da2877fda094edf3e21e6f0ba98a84bc53198 7f731cc11f8e4d249142e99a44b9da7a48505ce32c4ee4881041beeddb3760be 95477703e789e6182096a09bc98853e0a70b680a4f19fa2bf86cbb9280e8ec5a 0c0e0f9b09b80d87ebc88e2870907b6cacb4cd7703584baf8f2be1fd9438696d	Akira "Megazord" Ransomware

Akira_v2	3298d203c2acb68c474e5fdad8379181890b4403d6491c523c13730129be3f750ee1d284ed663073872012c7bde7fac5ca1121403f1a5d2d5411317df282796c	Akira_v2 ransomware
WinSCP-6.1.2-Setup.exe	36cc31f0ab65b745f25c7e785df9e72d1c8919d35a1d7bd4ce8050c8c068b13c	Network file transfer program
AD32.exe	08207409e1d789aea68419b04354184490ce46339be071c6c185c75ab9d08cba	Akira Ransomware Executable
Veeam-Get Creds.ps1	18051333e658c4816ff3576a2e9d97fe2a1196ac0ea5ed9ba386c46defafdb88	PowerShell script for obtaining and decrypting accounts from Veeam servers
hessen.exe	7d5da695e6f9a421e3d3a94e384ce00e8ec58fac5b895b4cba5b66a6de7fafd5	Akira Ransomware Executable Cryptor
vrsaki.exe	c9a1d8240147075cb7ffd8d568e6d3c517ac4cfdddccd5bb37857e7bde6d2eb7	Akira Ransomware Executable Cryptor
akira.exe	e5c8888f51369c2105d47a4998ad9b4053471bd98b4fd73a854207da09206ee2	Akira Ransomware Executable Cryptor

Hash (SHA-256)
0b5b31af5956158bfbd14f6cbf4f1bca23c5d16a40dbf3758f3289146c565f43
0d700ca5f6cc093de4abba9410480ee7a8870d5e8fe86c9ce103eec3872f225f
a2df5477cf924bd41241a3326060cc2f913aff2379858b148ddec455e4da67bc
03aa12ac2884251aa24bf0ccd854047de403591a8537e6aba19e822807e06a45
2e88e55cc8ee364bf90e7a51671366efb3dac3e9468005b044164ba0f1624422
40221e1c2e0c09bc6104548ee847b6ec790413d6ece06ad675fff87e5b8dc1d5
5ea65e2bb9d245913ad69ce90e3bd9647eb16d992301145372565486c77568a2
643061ac0b51f8c77f2ed202dc91afb9879f796ddd974489209d45f84f644562
6f9d50bab16b2532f4683eeb76bd25449d83bdd6c85bf0b05f716a4b49584f84
f1f82d3b62f92f4fe8af320afea6c346210bb51774bb1567149e308469d40c92
74fbb7885ee486028fe2723f95911474b771f361b2b40ddb77c46f252059c696

TTPs for Akira Ransomware Group

Tactic	Technique	Technique ID	Description
Initial Access	Phishing: Spear Phishing Attachment	T1566.001	Uses phishing emails with malicious attachments to gain initial access to target networks.
	Exploit Public-Facing Applications	T1190	Exploits vulnerabilities in internet-facing applications, such as VPN services without MFA or unpatched systems.
Execution	User Execution: Malicious File	T1204.002	Relies on victims executing malicious files delivered via email or compromised systems.
Persistence	Valid Accounts	T1078	Uses stolen credentials to maintain access within victim networks.
Privilege Escalation	OS Credential Dumping	T1003	Utilizes tools like Mimikatz and LaZagne to dump credentials and escalate privileges.
	OS Credential Dumping: LSASS Memory	T1003.001	Akira threat actors attempt to access credential material stored in the process memory of the LSASS.

Defense Evasion	Obfuscated Files or Information	T1027	Uses encrypted or obfuscated payloads to bypass detection.
	Indicator Removal on Host	T1070	Deletes logs and other artifacts to remove evidence of activities.
	Proxy: External Proxy	T1090.002	Uses external proxies to obscure command-and-control traffic.
Credential Access	Credential Dumping	T1003.001	Dumps credentials from memory or the security accounts manager (SAM) database.
Discovery	Network Service Scanning	T1046	Scans for active systems and services in the network using tools like SoftPerfect Network Scanner.
	System Network Configuration Discovery	T1016	Akira threat actors use tools to scan systems and identify services running on remote hosts and local network infrastructure.
	Domain Trust Discovery	T1482	Akira threat actors use the net Windows command to enumerate domain information.

	Permission Groups Discovery: Local Groups	T1069.001	Akira threat actors use the **net localgroup /dom** to find local system groups and permission settings.
	Create Account: Domain Account	T1136.002	Akira threat actors attempt to abuse the functions of domain controllers by creating new domain accounts to establish persistence.
Lateral Movement	Remote Services: SMB/Windows Admin Shares	T1021.002	Moves laterally across the network via SMB or admin shares.
	Exploitation of Remote Services	T1210	Exploits vulnerabilities in services such as VMware ESXi for lateral movement.
Collection	Archive Collected Data: Compress Data for Exfiltration	T1560.001	Uses tools like WinRAR to compress data before exfiltration.
Exfiltration	Exfiltration Over Web Service	T1567.002	Uses cloud-based tools like Rclone to transfer stolen data to attacker-controlled infrastructure.
	Exfiltration Over Alternative Protocol	T1048.002	Transfers data using alternative protocols to evade detection.

Command and Control	Remote Access Software	T1219	Akira threat actors use legitimate desktop support software like AnyDesk to obtain remote access to victim systems.
	Proxy	T1090	Akira threat actors utilized Ngrok to create a secure tunnel to servers that aided in exfiltration of data.
Impact	Date Encrypted for Impact	T1486	Akira threat actors encrypt data on target systems to interrupt availability to system and network resources.
	Inhibit System Recovery	T1490	Akira threat actors delete volume shadow copies on Windows systems.
	Financial Theft	T1657	Akira threat actors use a double-extortion model for financial gain.

Akira's sophisticated attack chain, emphasizing their focus on persistence, lateral movement, and data exltration to maximize impact on victims.

Yara Rule

```
rule Akira_Ransomware_and_Tools
{
    meta:
        author = "ThreatMon AI"
        description = "Detects Akira ransomware and associated tools"
        date = "2024-12-19"

    strings:
       // Hash list of Akira Ransomware
        $hash_w_exe =
"d2fd0654710c27dcf37b6c1437880020824e161dd0bf28e3a133ed777242a0ca"
        $hash_win_exe =
"dcfa2800754e5722acf94987bb03e814edcb9acebda37df6da1987bf48e5b05e"
        $hash_anydesk_exe =
"bc747e3bf7b6e02c09f3d18bdd0e64eef62b940b2f16c9c72e647eec85cf0138"
        $hash_gcapi_dll =
"73170761d6776c0debacfbbc61b6988cb8270a20174bf5c049768a264bb8ffaf"
        $hash_sysmon_exe =
"1b60097bf1ccb15a952e5bcc3522cf5c162da68c381a76abc2d5985659e4d386"
        $hash_rclone_exe =
"aaa647327ba5b855bedea8e889b3fafdc05a6ca75d1cfd98869432006d6fecc9"
        $hash_winscp_rnd =
"7d6959bb7a9482e1caa83b16ee01103d982d47c70c72fdd03708e2b7f4c552c4"
        $hash_megazord_1 =
"ffd9f58e5fe8502249c67cad0123ceeeaa6e9f69b4ec9f9e21511809849eb8fc"
        $hash_megazord_2 =
"dfe6fddc67bdc93b9947430b966da2877fda094edf3e21e6f0ba98a84bc53198"
        $hash_megazord_3 =
"7f731cc11f8e4d249142e99a44b9da7a48505ce32c4ee4881041beeddb3760be"
        $hash_megazord_4 =
"95477703e789e6182096a09bc98853e0a70b680a4f19fa2bf86cbb9280e8ec5a"
        $hash_megazord_5 =
"0c0e0f9b09b80d87ebc88e2870907b6cacb4cd7703584baf8f2be1fd9438696d"
        $hash_akira_v2_1 =
"3298d203c2acb68c474e5fdad8379181890b4403d6491c523c13730129be3f75"
        $hash_akira_v2_2 =
"0ee1d284ed663073872012c7bde7fac5ca1121403f1a5d2d5411317df282796c"
        $hash_winscp_setup =
"36cc31f0ab65b745f25c7e785df9e72d1c8919d35a1d7bd4ce8050c8c068b13c"
```

```
        $hash_veeam_ps1_1 =
"18051333e658c4816ff3576a2e9d97fe2a1196ac0ea5ed9ba386c46defafdb88"
        $hash1 =
"0b5b31af5956158bfbd14f6cbf4f1bca23c5d16a40dbf3758f3289146c565f43"
        $hash2 =
"0d700ca5f6cc093de4abba9410480ee7a8870d5e8fe86c9ce103eec3872f225f"
        $hash3 =
"a2df5477cf924bd41241a3326060cc2f913aff2379858b148ddec455e4da67bc"
        $hash4 =
"03aa12ac2884251aa24bf0ccd854047de403591a8537e6aba19e822807e06a45"
        $hash5 =
"2e88e55cc8ee364bf90e7a51671366efb3dac3e9468005b044164ba0f1624422"
        $hash6 =
"40221e1c2e0c09bc6104548ee847b6ec790413d6ece06ad675fff87e5b8dc1d5"
        $hash7 =
"5ea65e2bb9d245913ad69ce90e3bd9647eb16d992301145372565486c77568a2"
        $hash8 =
"643061ac0b51f8c77f2ed202dc91afb9879f796ddd974489209d45f84f644562"
        $hash9 =
"6f9d50bab16b2532f4683eeb76bd25449d83bdd6c85bf0b05f716a4b49584f84"

      // OP Codes, belongs to analyzed akira ransomware sample
      $op1 = {4E 75 6D 62 65 72 20 6F 66 20 74 68 72 65 61 64 73 20 74 6F 20 65 6E 63 72 79 70 74}
      $op2 = {48 89 45 60 48 8d 05 7c e3 08 00 48 89 45 68 48 8d 45 60 48 89 44 24 60}
      $op3 = {48 8d 05 55 e1 08 00 48 89 85 b0}
      $op4 = {4? 8d 15 a2 0f 02 00 4? 8d 8b a0 09 00 00}
      $op5 = {4? 8d 25 06 d6 08 00 4? 3b c6 76 16 4? 8d 04 06}
      $op6 = {4? 8b d4 4? 8b ce e8 33 15 04 00}
      $op7 = {4? 8d 15 2b d2 08 00 4? 8d 8d 60 02 00 00 }
      $op8 = {4? 0f 43 4c ?4 40 ff 15 06 96 08 00 8b c8 83 f8 01}
      $op9 = { 41 BA 05 00 00 00 41 80 FB 32 44 0F 42 D0 33 D2 48 8B C?
               49 F7 F2 4C 8B C8
               ( B? 02 00 00 00 [0-4] 41 B? 04 00 00 00 |
                 41 B? 04 00 00 00 [0-4] B? 02 00 00 00 )
               41 80 FB 32 44 0F 42 C? 41 8B C8 4? 0F AF C? 48 2B F9 33 D2
               48 8B C7 49 F7 F2 }
    condition:
        any of ($hash*) or all of ($op*)
}
```

Akira Ransomware Group: Conclusion and Key Insights

The Akira ransomware group has emerged as a sophisticated cybercrime organization that has demonstrated a growing capability to target organizations across multiple sectors globally. The following is a detailed analysis and conclusion based on the provided report:

1. Overview and Characteristics of Akira Group
   - **Emergence**: Akira ransomware group was first identified in March 2023 and has been rapidly evolving since.
   - **Primary Motive**: The group's primary goal is financial extortion, with ransom demands ranging from $200,000 to $4 million.
   - **Target Sectors**: Akira has predominantly targeted organizations in healthcare, finance, education, manufacturing, and critical infrastructure. Specific emphasis has been placed on financial services and government entities in countries like the United States, Canada, and Ecuador.
   - **Geographical Reach**: While its operations are global, notable attacks have been concentrated in North and South America, Europe, and select regions in Africa.

2.Attack Methodology
   - **Double-Extortion Model**: The group encrypts data and exfiltrates sensitive information, threatening to publish the data if the ransom is not paid.
     - Earlier ransomware variants appended the ".akira" extension, but later versions, such as "megazord.exe," appended ".powerranges."
   - **Ransom Notes**: The ransom notes like "akira_readme.txt" share similarities with Conti ransomware, suggesting overlaps in techniques or source code.

3.Sophisticated Techniques
   - **Initial Access**: Akira relies on phishing campaigns and exploiting public-facing vulnerabilities in systems like VPNs and unpatched servers.
     - Notable CVEs: CVE-2023-20269, CVE-2022-40684, CVE-2024-40766.
   - **Lateral Movement**: The group exploits vulnerabilities such as CVE-2024-40711 and CVE-2023-27532 to expand access within networks.
   - **Persistence**: Tools such as AnyDesk, Ngrok, and advanced credential dumping techniques like Mimikatz and LaZagne are employed.
   - **Data Exfiltration**: Using tools like RClone and WinSCP, Akira transfers exfiltrated data to attacker-controlled infrastructure before encryption.

4.Tools and Malware

- Akira uses a diverse set of tools, categorized for specific purposes:
  - **Discovery:** Masscan, SoftPerfect Network Scanner.
  - **Credential Theft:** DonPAPI, LaZagne, Mimikatz.
  - **Exfiltration:** RClone, WinSCP, OpenSSH.
  - **Networking:** Cloudflared, Ngrok, and Temp[.]sh for creating secure tunnels.
  - **Defense Evasion**: Zemana Anti-Rootkit, PowerTool.
- Notably, Akira has leveraged both off-the-shelf tools and custom malware like “megazord.exe” and “akira_v2.exe” to enhance its attack capabilities.

5. Exploited Vulnerabilities

- Akira actively exploits a range of high-severity vulnerabilities in software from major vendors, which demonstrates their technical proficiency:
  - **Cisco ASA & FTD**: CVE-2023-20269, CVE-2020-3259.
  - **Fortinet FortiOS**: CVE-2022-40684, CVE-2019-6693.
  - **Veeam Backup & Replication**: CVE-2024-40711, CVE-2023-27532.
  - **VMware ESXi & vSphere Client**: CVE-2024-37085, CVE-2021-21972.
  - **SonicWall SonicOS SSL-VPN**: CVE-2024-40766.
- By leveraging both older and newly discovered vulnerabilities, Akira showcases its ability to adapt its techniques based on evolving security landscapes.

6.TTPs (Tactics, Techniques, and Procedures)

- Akira’s attack methodology aligns closely with the MITRE ATT&CK framework. Some key tactics include:
  - **Initial Access**: Spear-phishing (T1566.001), exploiting public-facing applications (T1190).
  - **Execution**: Malicious file execution (T1204.002).
  - **Persistence**: Using valid accounts (T1078) and creating domain accounts (T1136.002).
  - **Lateral Movement**: Exploiting remote services (T1210), leveraging SMB/Windows Admin Shares (T1021.002).
  - **Exfiltration**: Compressing data for exfiltration (T1560.001), transferring over web services (T1567.002).
  - **Impact**: Encrypting data for impact (T1486), inhibiting system recovery (T1490).

7.Latest Attacks

- The report highlights Akira's global impact, with attacks on organizations in the United States, Brazil, Italy, and Poland, among others. Noteworthy incidents include:
  - **Xtrim TVCable (Ecuador, Nov 2024)**: Akira leaked sensitive financial and customer data after ransom negotiations failed.
  - **Cipla (South Africa)**: Akira targeted this healthcare provider, disrupting critical services.
  - **Great Plains Bank (United States)**: A financial institution attack emphasizing Akira's focus on high-value targets.

Mitigations, Defense Recommendations and Risk Analysis Table

Risk Analysis Table:

Risk Factor	Likelihood	Impact	Descriptions
System infiltration	High	High	Exploitation of vulnerabilities in remote access services and stolen credentials.
Data encryption and loss	Critical	High	Encryption of files using the ChaCha and RSA algorithms and deletion of backups.
Data theft and exposure	Critical	High	Theft of sensitive data with threats of selling or leaking the information.
Operational disruption	High	High	Blocking access to critical systems and data, halting business processes.
Double extortion	High	High	Demand for ransom with the threat of data leakage or sale on the dark web.
Debugger and virtual machine evasion	High	Low	Detection of debugging tools and virtual machine environments to avoid analysis.
Targeted attack on key industries	Critical	Critical	Targeting industries like healthcare, IT, and finance for maximum impact.
Phishing	High	High	Delivery of malicious links or attachments to employees, leading to credential theft or malware execution.

Mitigation Strategies:

Risk	Mitigation Strategy
System infiltration	- Implement multi-factor authentication (MFA). - Regularly update and patch software. - Use robust VPN configurations.
Data encryption and loss	- Maintain secure and offline backups. - Implement endpoint detection and response (EDR) solutions.
Data theft and exposure	- Employ network segmentation to limit access. - Use data loss prevention (DLP) tools.
Operational disruption	- Develop and regularly test an incident response plan. - Use redundant systems to ensure business continuity.
Double extortion	- Avoid direct negotiation with threat actors. - Notify law enforcement and cyber insurance providers.
Debugger and virtual machine evasion	- Use behavior-based monitoring tools.
Targeted attack on key industries	- Conduct regular cybersecurity training for employees. - Perform frequent risk assessments and penetration tests.
Phishing	- Conduct phishing awareness training, implement email filtering, and deploying attachment scanning solutions..

Additional Mitigation Strategies Against Ransomware Attacks:

- Implement application whitelisting to prevent unauthorized or malicious software from running on your systems by only allowing approved programs to run.
- Integrate ThreatMon ThreatFeed into your security products, providing information about emerging ransomware threats.
- Use ThreatMon's News section and ThreatMon AI to set early warning alerts for ransomware campaigns targeting your industry or region. These alerts can help your organization prepare for potential attacks before they reach you.
- Ensure data is backed up regularly and maintain multiple copies, one offline or on a cloud service.