Akira ransomware continues to evolve

By James Nutland

Published: 2024-10-21 · Archived: 2026-04-02 12:30:36 UTC

Akira continues to cement its position as one of the most prevalent ransomware operations in the threat landscape, according to Cisco Talos' findings and analysis.

Their success is partly due to the fact that they are constantly evolving. For example, after Akira already developed a new version of their ransomware encryptor earlier in the year, we just recently observed another novel iteration of the encryptor targeting Windows and Linux hosts alike.

Previously, Akria typically employed a double-extortion tactic in which critical data is exfiltrated prior to the compromised victim systems becoming encrypted. Beginning in early 2024, Akira appeared to be sidelining the encryption tactics, focusing on data exfiltration only. We assess with low to moderate confidence that this shift was due in part to the developers taking time to further retool their encryptor.

During this period, we began to see Akira ransomware-as-a-service (RaaS) operators developing a Rust variant of their ESXi encryptor, iteratively building on the payload's functions while moving away from C++ and experimenting with different programming techniques.

Most recently, we have observed a potential shift back to previous encryption methods, in conjunction with data theft extortion tactics.

Returning to this approach leverages the reliability of tested encryption techniques, while simultaneously capitalizing on data theft for additional leverage. Pivoting to a previously effective strategy post-language reimplementation with v2 indicates a refocus on stability and efficiency in affiliate operations.

We anticipate Akira will continue refining its tactics, techniques, and procedures (TTPs), developing its attack chain, adapting to shifts in the threat landscape, and striving for greater effectiveness in its RaaS operations, targeting both Windows and Linux-based enterprise environments.

Members of our team will be delving into this prickly threat actor presenting at the upcoming MITRE ATT&CKCon 5.0 in 'GoGo Ransom Rangers: Diving into Akira's Linux Variant with ATT&CK'. Join us as we uncover findings about the TTPs employed by this developing threat actor, dissect their attack chain, and actionable intelligence is vital in the threat protection pipeline.

> "The future is not a straight line. It is filled with many crossroads" Kiyoko

2024 attack chain: Leveraging exposed network appliances and vulnerable systems for rapid compromise

As Akira continuously refines its ransomware, affiliates are equally proactive in selecting and exploiting new vulnerabilities for initial access, adapting their tactics in tandem. They leverage newly disclosed CVEs, not only to

breach networks but also to escalate privileges and move laterally within compromised environments. This allows them to establish a greater foothold to swiftly deploy encryption and exfiltrate victim data for extortion.

Akira ransomware operators have utilized a variety of common infection vectors to gain initial access to targeted networks, often favoring the use of compromised VPN credentials.

Most recently, Akira ransomware affiliates have been observed targeting network appliances vulnerable to CVE-2024-40766, an exploit in the SonicWall SonicOS facilitating remote code execution on the vulnerable device. Security researchers found that software on the affected systems was vulnerable to this exploit, suggesting affiliates' swift capitalization on exposed systems.

Additional vulnerabilities leveraged by affiliates throughout 2024 include:

- CVE-2020-3259 and CVE-2023-20263: In similar Cisco security appliance exploits leveraged in early 2024, Akira was observed abusing a flaw in Cisco Adaptive Security Appliance (ASA) with CVE-2020-3259 and CVE-2023-20263 via Firepower Threat Defense (FTD) software that allowed attackers to execute arbitrary code, after initial access was established post Cisco AnyConnect SSL VPN compromise.
- CVE-2023-48788: Exposed and vulnerable FortiClientEMS software abuse by Akira was observed for initial access, enabling lateral movement and privilege escalation.

Once initial access is established, Akira operators utilize PowerShell scripts to conduct credential harvesting and privilege escalation, such as extracting Veeam backup credentials and dumping Kerberos authentication credentials. Additionally, we often see affiliates delete system shadow copies to obstruct file recovery via Windows Management Instrumentation (WMI): "Get-WmiObject Win32_Shadowcopy | Remove-WmiObject".

Operators typically utilize RDP connections and lateral tool transfers to move through the network and employ a variety of defense evasion techniques, such as binary padding, matching legitimate name or location taxonomy, and disabling or modifying security tools.

In an attack targeting a Latin American airline in June 2024, RaaS operators were able to exploit key vulnerable services and deploy the ransomware payload in a manner that drastically reduced the time to exfiltrate data. Initially gaining access via Secure Shell (SSH), it was reported that the adversary obtained access to the vulnerable Veeam backup server likely via CVE-2023-27532, resulting in the access of encrypted credentials stored in the configuration database. This foothold facilitated the swift deployment of the Akira ransomware variant and exfiltration of sensitive data.

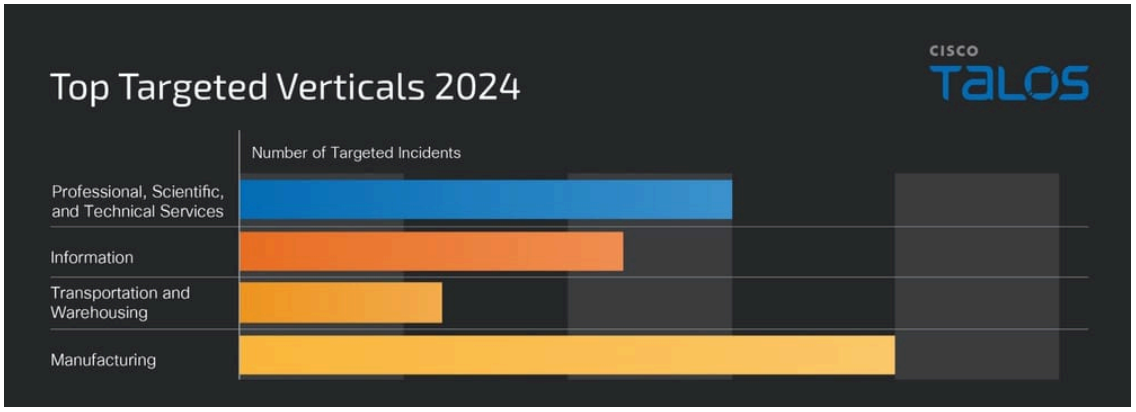
Akira ransomware affiliates have actively exploited several additional critical vulnerabilities in 2024 after achieving initial compromise, capitalizing on unpatched vulnerabilities in widely used network appliances and software to establish persistence and move laterally:

- CVE-2023-20269: Akira affiliates were suspected of targeting this vulnerability in Cisco VPN services. The exploit leverages an unauthorized access vulnerability in the remote access VPN feature of ASA and FTD software due to a misconfiguration of improper separation of authentication, authorization, and accounting (AAA) on the device.
- CVE-2024-37085: VMware ESXi vulnerability enabling unauthorized access to the hypervisor's management interface, which can lead to full control over virtual machines once the adversary has

established sufficient Active Directory Permissions.

- CVE-2024-40711: Akira ransomware was recently seen deployed post exploitation of the Veeam backup and replication service by triggering "Veeam.Backup.MountService.exe" to spawn "net.exe" and create local accounts for privilege escalation and persistence.

In terms of victimology, we assess that throughout 2024, Akira has targeted a significant number of victims, with a clear preference for organizations in the manufacturing and professional, scientific, and technical services sectors, based on our analysis of Akira's data leak site.



Top Akira targeted verticals in 2024

A look at the previous Akira v2 ESXi encryptor

Akira pivoted from their traditional TTPs at the end of 2023 and developed a new Linux encryptor. In March 2024, we shared findings with intelligence partners generated from a Cisco Talos Incident Response (Talos IR) engagement, which documented the newly discovered Akira_v2 and the co-occurring deployment of the adversaries' Megazord encryptor.

Post-encryption, we witnessed the Linux ESXi variant appended with a novel encrypted storage file extension "akiranew" dropping a ransom note in each of the directories where files were encrypted with a new nomenclature, "akiranew.txt". We discovered two additional samples of the Akira_v2 variant (version 2024.1.30) on VirusTotal that included additional modifications to extend its command line argument capabilities, highlighting further evolution in the malware's development.

Arguments	Description
--path <string>	Start path. Default value: /vmfs/volumes
--id <string>	Build ID

--stopvm	Stop VMs
--vmonly	Crypt only .vmdk, .vmem, .vmx, .log, .vswp, .vmsd, .vmsn files
--threads <int>	Number of threads (1-1000). Default: number of logical CPU cores
--ep <int>	Percent of crypt. Default - 15%
--fork	Work in background
--logs <string>	Print logs. Valid values for: trace, debug, error, info, warn. Default: off
--exclude <string>	Skip files by "regular" extension. Example: --exclude="startfilename(.*).(.*)" using this regular expression will skip all files starting with startfilename and having any extensions. Multiple regular expressions using "|" can also be processed: --exclude="(win10-3(.*).(.*))|(win10-4(.*).(.*))|(win10-5(.*).(.*))"
-h, --help	Show help

The original Linux encryptor was written in C++, with Akira leveraging the Crypto++ library for encryption processes, whereas the v2 Rust variant makes use of rust-crypto 0.2.36 library crate for encryption processes.

The Build ID for the v2 (version 2024.1.30) was found at offset 0x41970 for 10 bytes.

```
00041940  3A 20 20 57 72 6F 6E 67 20 72 65 67 65 78 70 20  :  Wrong regexp
00041950  70 72 6F 76 69 64 65 64 3A 20 20 4E 6F 20 65 78  provided:  No ex
00041960  63 6C 75 64 65 20 65 78 70 72 65 73 73 69 6F 6E  clude expression
00041970  56 44 62 41 59 5A 6B 64 49 42 76 69 6D 2D 63 6D  VDbAYZkdIBvim-cm
00041980  64 20 76 6D 73 76 63 2F 67 65 74 61 6C 6C 76 6D  d vmsvc/getallvm
00041990  73 20 7C 20 74 61 69 6C 20 2D 6E 20 2B 32 20 7C  s | tail -n +2 |
000419A0  20 61 77 6B 20 27 7B 73 79 73 74 65 6D 28 22 76   awk '{system("v
000419B0  69 6D 2D 63 6D 64 20 76 6D 73 76 63 2F 70 6F 77  im-cmd vmsvc/pow
```

In the v2 version targeting ESXi hosts, by default, the encryptor targets the “/vmfs/volumes/” path and will navigate into subdirectories. If this path does not exist or a path is not specified, the ransomware will fail to execute.

Akira (The Return) to old TTPs

From our recent analysis, we suspect that Akira may be transitioning from the use of the Rust-based Akira v2 variant and returning to previous TTPs using Windows and Linux encryptors written in C++. This could be because of a potential refocus on incremental iterations with stability and reliability in their operations over innovation. The cross-platform consistency indicates the adversaries' focus on an adaptable payload, enabling the threat actor to target multiple operating systems with minimal changes.

In early September 2024, we identified multiple new ransomware samples written in C++, where encrypted files are given the ".akira" extension and a ransom note named "akira_readme.txt" is dropped on the device, consistent with pre-August 2023 versions of the Akira ransomware group's encryptor. These findings support our assessment of a tactical pivot, signaling a deliberate return to effective techniques, consistent with public reporting on the threat actors' initial Linux variant.

We assess with moderate confidence that the Megazord variant, previously used by the threat actor targeting Windows environments, alongside Akira v2 for Linux, has gradually faded away, further supporting a consolidation of tooling by the adversary.

The newly observed Windows variant has been updated and appears to substitute the previously seen -remote argument for -localonly and --exclude and excludes paths, including "$Recycle.Bin" and "System Volume Information", in the encryption process. Within the Linux variant, the –fork argument, which creates a child process for encryption, is still included along with the --exclude argument.

Analysis of the recent binaries suggests that the threat actor has pivoted to utilizing the ChaCha8 stream cipher. The ChaCha8 algorithm is faster and more efficient than the previously leveraged ChaCha20 in Akira v_2 due to the reduced number of quarter-round operations in the cipher, possibly indicating a further focus on swift encryption and exfiltration operations such as seen in recent Akira attacks.

New extensions targeted in recently observed Linux variants:

.4d	.abd	.abx	.ade
.ckp	.db	.dd	dpl
.dx	.edb	.fo	.ib
.idb	.mdn	.mud	.nv
.pdb	.sq	.te	.ud

.vdh			

Both newly observed encryptor variants employ exclusion paths that ignore identical Windows directories before the encryption process, a return to previous TTPs by the adversary.

tmp	wint	temp	thumb
$Recycle.Bin	$RECYCLE.BIN	System Volume Information	Boot
Windows	Trend Micro		

Future developments in Akira's TTPs

Future campaigns are likely to see Akira continuing to prioritize the exploitation of high-impact CVEs while reinforcing its double extortion model to increase ransom leverage.

The exploration of the Rust programming language in recent Linux encryptors signals the threat actor's willingness to experiment with different coding frameworks, potentially leading to more developed and resilient ransomware variants. While the return to an earlier variant indicates a potential tactical shift from this code migration, it also demonstrates that the developers remain highly adaptable, willing to reemploy tried-and-tested techniques when necessary to ensure operational stability. Pragmatic adaptability is providing significant advantages for ransomware groups operating in a dynamic threat landscape, as it allows them to maintain a robust and reliable codebase while continually seeking new ways to evade detection and enhance functionality.

It is possible that Akira's pivot to pure data-theft extortion at the end of 2023 and beginning of 2024 was a temporary shift during the codebase refactoring, allowing the group to maintain pressure on victims and generate revenue while developmental resources were allocated to refining the encryptor's functionality.

We assess that Akira and its affiliates will continue prioritizing attacks against VMWare's ESXi and Linux environments throughout 2024, echoing a broader trend observed across the ransomware landscape. Adversary targeting of these platforms is driven by their prevalence in enterprise infrastructure, hosting critical infrastructure and high-value data, and their capacity for mass encryption and disruption with minimal lateral movement. Targeting ESXi and Linux hosts allows ransomware operators to compromise multiple virtual machines and critical workloads simultaneously, maximizing operational impact while bypassing traditional endpoint security controls.

- Virtualization is essential to large-scale deployments of cloud computing and storage resources, making ransomware attacks on ESXi hypervisors highly disruptive.
- Encrypting the ESXi file system provides rapid, widespread data encryption, minimizing the need for extensive lateral movement and credential theft, due to the ease of encrypting a single vmdk, rather than all the files.
- ESXi hypervisors often lack comprehensive security protection due to security department overhead, making them attractive targets for ransomware operators seeking fruitful targets.

Recommendations

Conduct regular vulnerability assessments and timely application of security patches to identify outdated software versions and unpatched vulnerabilities on ESXi hosts and implement a formal threat-informed patch management policy that includes a defined prioritization and schedule for routine updates and emergency patching of critical vulnerabilities.

Implement strict password policies that require complex, unique passwords for each account. Additionally, enforce multi-factor authentication (MFA) to add an extra layer of security.

Deploy a Security Information and Event Management (SIEM) system to continuously monitor and analyze security events, in addition to the deployment of EDR/XDR solutions on all clients and servers to provide advanced threat detection, investigation, and response capabilities.

Enable secure configuration and access controls to limit access to ESXi management interfaces such as by restricting them to trusted IPs, enforcing MFA, and ensuring role-based access control (RBAC) is properly configured.

Disable unnecessary WMI access by restricting or disabling WMI access for non-administrative users, and monitor/audit WMI commands, particularly those related to shadow copy deletion.

Credential dumping prevention via implementing Windows Defender Credential Guard to protect Kerberos ticket data and prevent credential dumping from the Local Security Authority (LSA), ensuring to audit and apply necessary configuration changes to applications/plug-ins that aren't compatible due to reliance on direct access to user credentials.

Coverage

Ways our customers can detect and block this threat are listed below.

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org. SIDs for this threat:

Snort3: 300924

Snort3 Rules: 1:301007:1:0

Snort2: 63541, 63540

Snort2 Rules: 1:63976:1:0, 1:63977:1:0

ClamAV detections are also available for this threat:

Multios.Ransomware.Akira-10036536-0

Multios.Ransomware.Megazord-10021030-1

IOCs

IOCs for this research can be found in our GitHub repository here.

Windows (The Return)

78d75669390e4177597faf9271ce3ad3a16a3652e145913dbfa9a5951972fcb0

2c7aeac07ce7f03b74952e0e243bd52f2bfa60fadc92dd71a6a1fee2d14cdd77

88da2b1cee373d5f11949c1ade22af0badf16591a871978a9e02f70480e547b2

566ef5484da0a93c87dd0cb0a950a7cff4ab013175289cd5fccf9dd7ea430739

ccda8247360a85b6c076527e438a995757b6cdf5530f38e125915d31291c00d5

87b4020bcd3fad1f5711e6801ca269ef5852256eeaf350f4dde2dc46c576262d

988776358d0e45a4907dc1f4906a916f1b3595a31fa44d8e04e563a32557eb42

Linux (The Return)

3805f299d33ef43d17a5a1040149f0e5e2d5db57ec6f03c5687ac23db1f77a30

abba655df92e99a15ddcde1d196ff4393a13dbff293e45f5375a2f61c84a2c7b

a546ef13e8a71a8b5f0803075382eb0311d0d8dbae3f08bac0b2f4250af8add0

6005dcbe15d60293c556f05e98ed9a46d398a82e5ca4d00c91ebec68a209ea84

43c5a487329f5d6b4a6d02e2f8ef62744b850312c5cb87c0a414f3830767be72

8e9a33809b9062c5033928f82e8adacbef6cd7b40e73da9fcf13ec2493b4544c

bcae978c17bcddc0bf6419ae978e3471197801c36f73cff2fc88cecbe3d88d1a

3805f299d33ef43d17a5a1040149f0e5e2d5db57ec6f03c5687ac23db1f77a30

Windows v1

678ec8734367c7547794a604cc65e74a0f42320d85a6dce20c214e3b4536bb33

6cadab96185dbe6f3a7b95cf2f97d6ac395785607baa6ed7bf363deeb59cc360

3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c

1b6af2fbbc636180dd7bae825486ccc45e42aefbb304d5f83fafca4d637c13cc

5c62626731856fb5e669473b39ac3deb0052b32981863f8cf697ae01c80512e5

Megazord

dfe6fddc67bdc93b9947430b966da2877fda094edf3e21e6f0ba98a84bc53198

28cea00267fa30fb63e80a3c3b193bd9cd2a3d46dd9ae6cede5f932ac15c7e2e

a6b0847cf31ccc3f76538333498f8fef79d444a9d4ecfca0592861cf731ae6cb

b55fbe9358dd4b5825ce459e84cd0823ecdf7b64550fe1af968306047b7de5c9

c9c94ac5e1991a7db42c7973e328fceeb6f163d9f644031bdfd4123c7b3898b0

0c0e0f9b09b80d87ebc88e2870907b6cacb4cd7703584baf8f2be1fd9438696d

95477703e789e6182096a09bc98853e0a70b680a4f19fa2bf86cbb9280e8ec5a

e3fa93dad8fb8c3a6d9b35d02ce97c22035b409e0efc9f04372f4c1d6280a481

68d5944d0419bd123add4e628c985f9cbe5362ee19597773baea565bff1a6f1a

8816caf03438cd45d7559961bf36a26f26464bab7a6339ce655b7fbad68bb439

c0c0b2306d31e8962973a22e50b18dfde852c6ddf99baf849e3384ed9f07a0d6

7f731cc11f8e4d249142e99a44b9da7a48505ce32c4ee4881041beeddb3760be

2f629395fdfa11e713ea8bf11d40f6f240acf2f5fcf9a2ac50b6f7fbc7521c83

9f393516edf6b8e011df6ee991758480c5b99a0efbfd68347786061f0e04426c

9585af44c3ff8fd921c713680b0c2b3bbc9d56add848ed62164f7c9b9f23d065

131da83b521f610819141d5c740313ce46578374abb22ef504a7593955a65f07

Akira_v2:

3298d203c2acb68c474e5fdad8379181890b4403d6491c523c13730129be3f75

0ee1d284ed663073872012c7bde7fac5ca1121403f1a5d2d5411317df282796c

---