Threat Assessment: Howling Scorpius (Akira Ransomware)

By Yoav Zemah

Published: 2024-12-02 · Archived: 2026-04-05 18:27:55 UTC

Executive Summary

Emerging in early 2023, the Howling Scorpius ransomware group is the entity behind the Akira ransomware-as-a-service (RaaS), which has consistently ranked in recent months among the top five most active ransomware groups. Its double extortion strategy significantly amplifies the threat it poses. Unit 42 researchers have been monitoring the Howling Scorpius ransomware group over the past year.

Howling Scorpius targets small to medium-sized businesses in North America, Europe and Australia, across various sectors. Affected industries include education, consulting, government, manufacturing, telecommunications, technology and pharmaceuticals.

Our research reveals that Howling Scorpius maintains and operates encryptors for Windows and Linux operating systems. We identified variants specifically designed for ESXi hosts. In addition, our findings have shown that this group is actively upgrading and enhancing its tool set, thus posing a greater risk for organizations.

Palo Alto Networks customers are better protected against Akira ransomware from the Howling Scorpius ransomware group through the following products and services:

- **Cortex XDR** and **XSIAM**
- **Cloud-Delivered Security Services** for the **Next-Generation Firewall**, such as **Advanced WildFire**
- **Cortex Xpanse**

The Unit 42 Incident Response team has responded to several Howling Scorpius ransomware incidents since the group first emerged in 2023. If you think you might have been compromised or have an urgent matter, contact the **Unit 42 Incident Response team**.

Howling Scorpius Overview

First observed in March 2023 [PDF], Akira is a RaaS group we track as Howling Scorpius. This group employs a double extortion strategy, exfiltrating critical data from a network before executing its encryption process. This double extortion tactic allows the group to leak stolen data even if victims recover their systems without paying, maximizing the pressure to comply.

Howling Scorpius operates a Tor-based leak site for Akira ransomware. The group uses the site to list victims and exfiltrate stolen data if they refuse to comply with ransom demands.

The Akira leak site has a retro-green look. Howling Scorpius also operates a separate Tor-based negotiation site, which victims can access using a dedicated password provided by the group. Figure 1 shows a screenshot of the

Akira ransomware leak site.

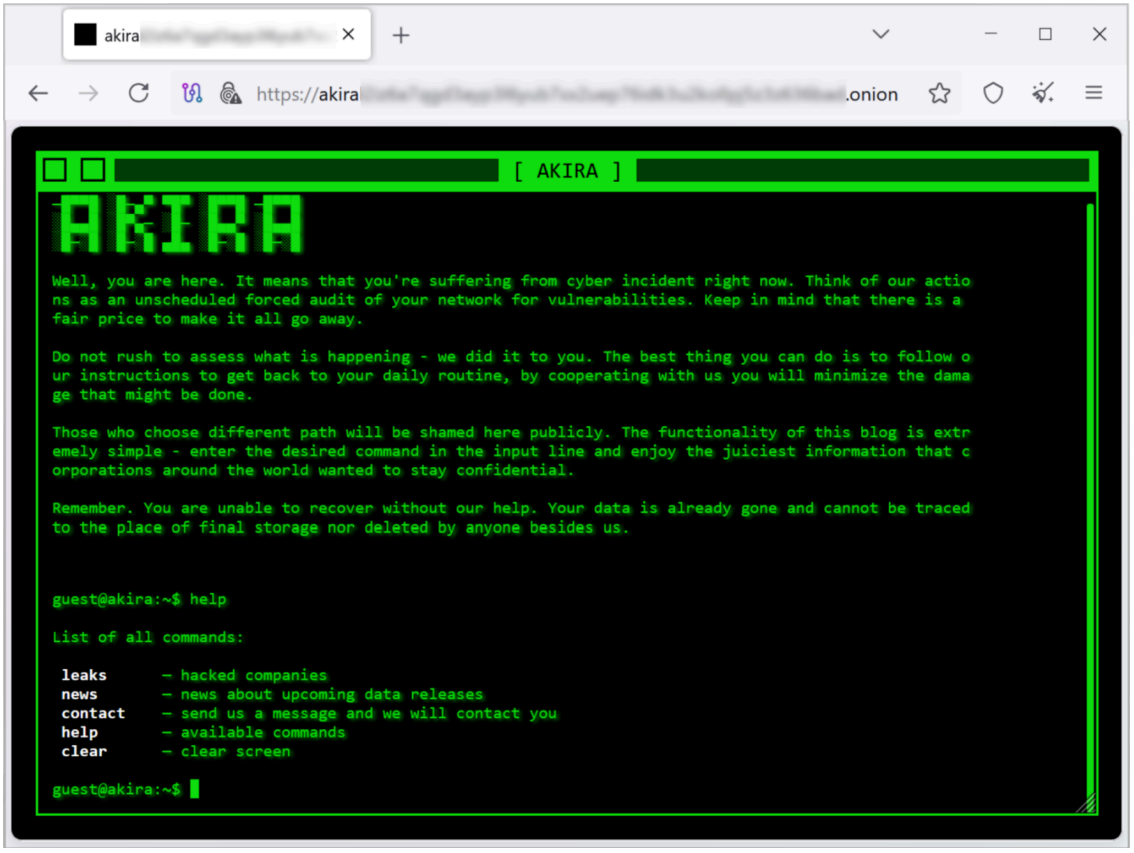

Figure 1. Screenshot of the Akira Ransomware leak site in a Tor browser, from November 2024.

The Akira ransomware leak site displays a text-based console with a list of commands. The leaks command returns a list of victims who did not pay and includes links to download .torrent files. Viewers can then use these .torrent files to download the released data for those victims who did not pay their ransom.

This console also includes a news command that lists all compromised companies that it says date back as far as April 2023. The site describes the news command as “upcoming data releases,” and the results end with the most recent victims.

The group primarily targets small to medium-sized businesses across various regions and industries.

Targeted Regions

While Howling Scorpius has targeted organizations globally since 2023, the U.S. has emerged as the most affected country, according to Akira leak site data. Figure 2 highlights the top 10 affected countries based on this leak site data from March 2023-October 2024.

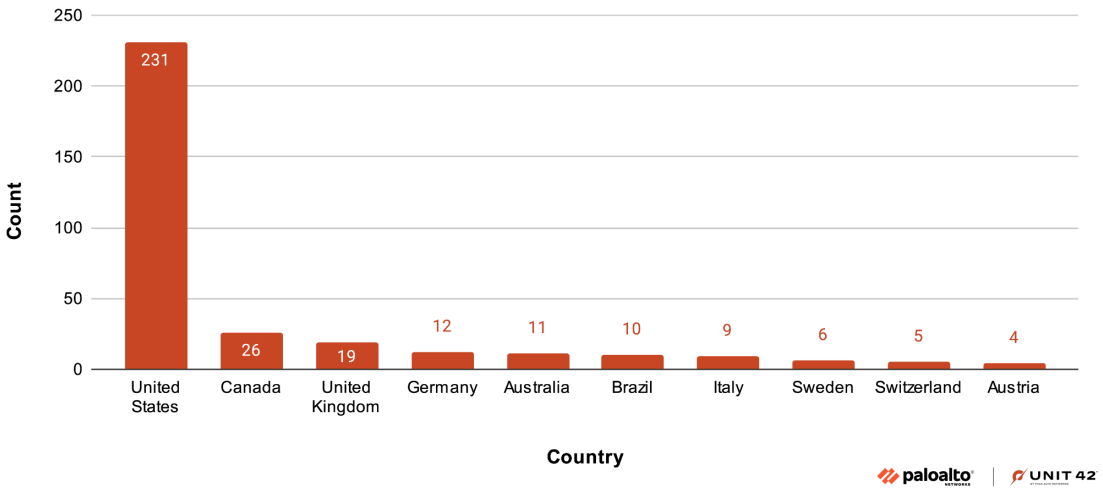

Figure 2. A column chart showing the countries impacted by Howling Scorpius from March 2023-October 2024.

Targeted Industries

Akira leak site data shows the group has impacted several industries, including manufacturing, professional and legal services, wholesale, retail and construction. Figure 3 shows the top 10 industries affected by this ransomware from March 2023-October 2024.

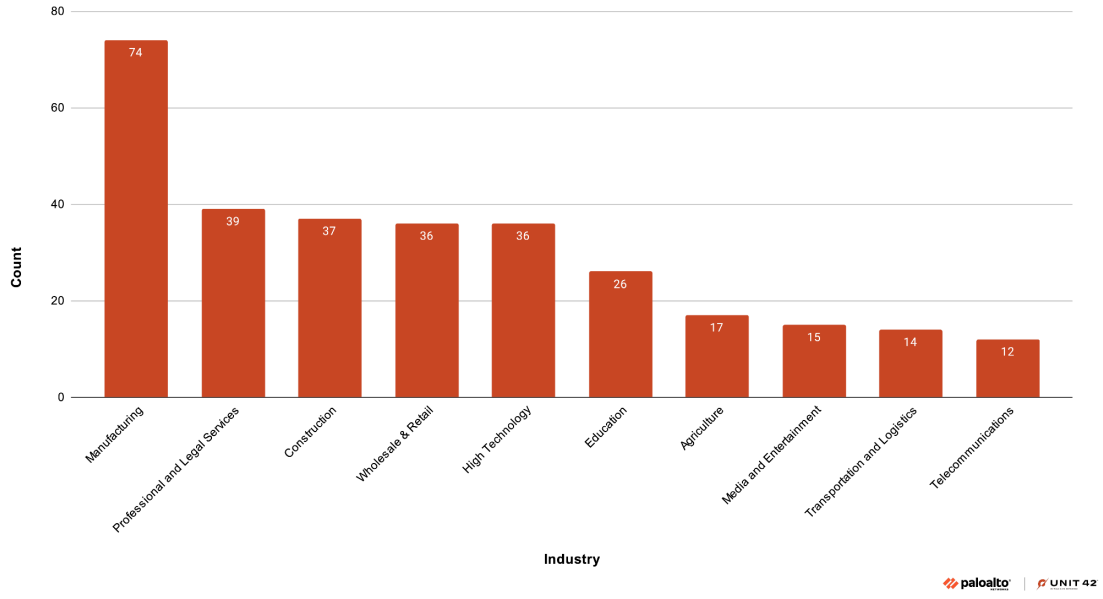

Figure 3. The distribution of the top 10 sectors affected by Howling Scorpius from March 2023-October 2024.

Technical Analysis of the Akira Ransomware Attack Lifecycle

Below is a technical analysis of Howling Scorpius operations mapped to the different stages of a cyberattack's lifecycle.

Initial Access

Howling Scorpius affiliates employ various methods to gain initial access to organizations. These include exploiting vulnerable virtual private network (VPN) services that lack multi-factor authentication (MFA) using valid accounts, often purchased through initial access brokers on the dark web.

Affiliates also target external-facing services like Remote Desktop Protocol (RDP), and they conduct spear phishing campaigns.

Figure 4 shows an alert raised by Cortex XDR for an example of a remote service creation. This specific alert involves using a service component of PsExec named PSEXESVC.exe to run a process from a remote system.

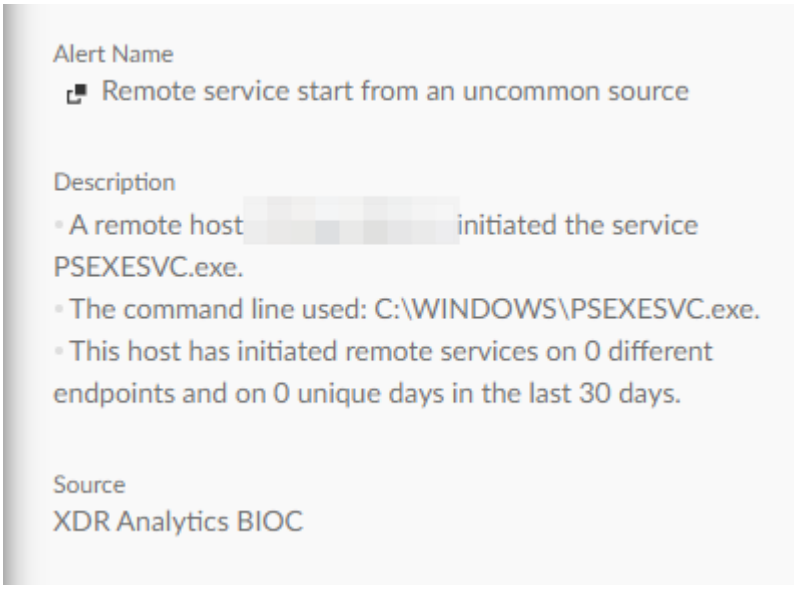

Figure 4. Cortex XDR alert for remote service creation from an uncommon source.

The security community has documented Howling Scorpius exploiting vulnerabilities in Cisco products, such as CVE-2020-3259 and CVE-2023-20269.

Credentials Access

Local Credential Access Techniques

Howling Scorpius affiliates employ various credential access techniques to extract credentials for privilege escalation. Mimikatz and LaZagne are their primary tools.

Affiliates also often create a MiniDump of the LSASS process memory leveraging comsvcs.dll. Figure 5 shows an example of Cortex XDR detecting an example of comsvcs.dll used for this type of memory dump.

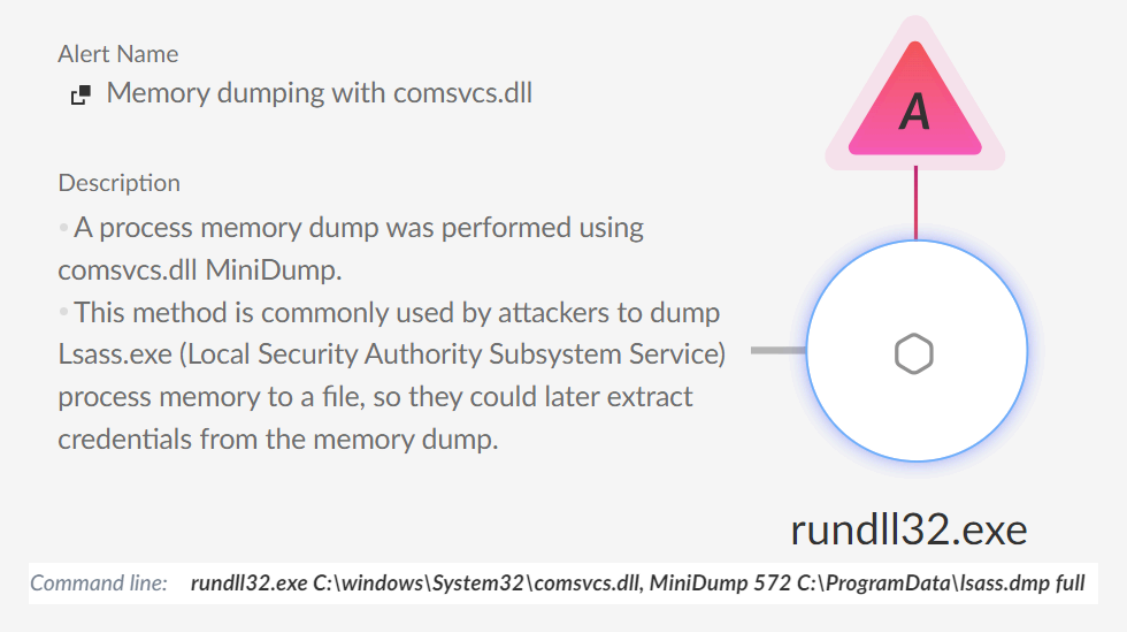

Figure 5. Cortex XDR detection alert of comsvcs.dll MiniDump of LSASS.

Kereberoasting

Howling Scorpius affiliates employ the Kerberoasting attack to achieve control over service accounts and exploit credentials stored in memory.

Extracting Credentials for Domain Control

The group's affiliates focus on extracting credentials from the Active Directory database to pursue comprehensive domain control. They copy the SYSTEM registry hive and NTDS.dit file from the domain controller (DC) to obtain a complete listing of user accounts and their corresponding domain password hashes.

Exploiting Compromised vCenter Instances

In cases where affiliates compromise a vCenter instance, they will perform the following activities:

- Shutting down the DC's virtual machine (VM)
- Copying the DC's Virtual Machine Disk (VMDK) files to another VM they created beforehand
- Extracting the NTDT.dit and SYSTEM registry hive files (as reported by Rewterz)

Persistence

Howling Scorpius affiliates created new domain accounts to establish persistence. These accounts give these affiliates another form of access that does not require them to deploy tools or malware on the targeted systems. In addition, CISA reported [PDF] that the affiliates created new administrative domain accounts named itadm.

Discovery and Lateral Movement

Howling Scorpius affiliates' lateral movement within compromised networks primarily involves exploiting remote services such as Remote Desktop Procol (RDP) and Server Message Block (SMB). The group also employs remote service creation and Windows Management Instrumentation (WMI) to further its reach.

These affiliates use network scanning tools like NetScan and Advanced IP Scanner to map the network and identify potential critical assets in the targeted organization for lateral movement. They also execute PowerShell and Windows Net Commands to query Active Directory for information on additional users and administrators.

Defense Evasion

Bring Your Own Driver

Howling Scorpius affiliates use tools that abuse the Zemana antimalware driver to terminate antimalware-related processes. Figure 6 below shows information from an alert raised in Cortex XDR for attempting to create the malicious Zemana driver.

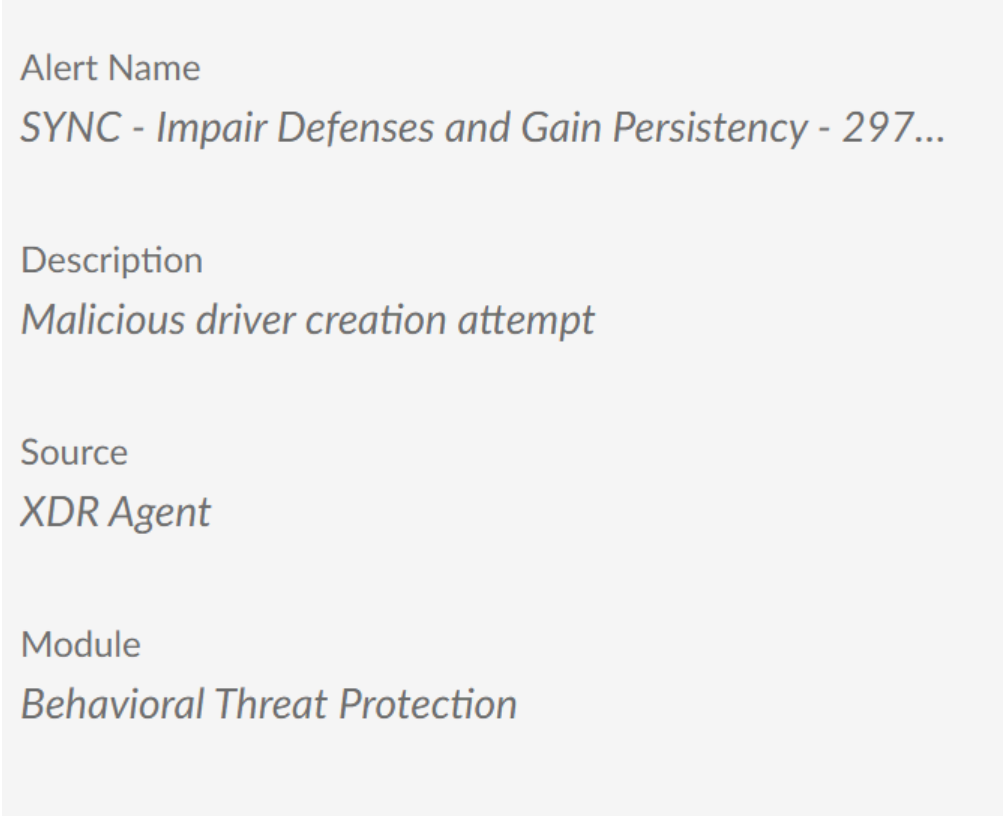

Figure 6. Cortex XDR alert for the attempt to use the Zemana antimalware driver.

Anti Virus Disablement

Affiliates have also tried to disable Windows Defender Real-Time Protection using PowerShell, and they tried to uninstall the EDR agents installed on infected systems.

Bring Your Own VM

Affiliates sometimes create their own VMs. Within these VMs, they disable security tools. They then mount the hypervisor host's storage drives onto the VM, shutting down any processes using those files to unlock running VM files. After successfully mounting the drives and unlocking all targeted files, they execute the ransomware within the new VM (as reported by CyberCX), bypassing the host's security tools.

Exfiltration

Howling Scorpius affiliates usually exfiltrate data from compromised hosts using WinRAR and a combination of WinSCP, RClone and FileZilla, through the File Transfer Protocol (FTP). Below is an example of a data exfiltration attempt we observed:

```
"C:\Program Files\WinRAR\WinRAR.exe" a -ep1 -scul -r0 -iext -imon1 -- . "[REDACTED]\Company\[REDACTED]" [REDACTED]\Company\HR "[REDACTED]\Company\Human Resources Management - HR"
```

Akira Ransomware Encryptors

This section details the different encryptors for Akira ransomware that Howling Scorpius uses for Windows and Linux operating systems.

Ransom Note

Upon successful encryption, Akira ransomware encryptors create a ransom note named akira_readme.txt that provides victims instructions for how to interact with the group. This file includes links to both the leak site and the negotiation site.

The file also contains a unique code that victims must enter on the negotiation site to facilitate communication with the attackers and potential ransom discussions. Figure 7 shows an example of the akira_readme.txt file.

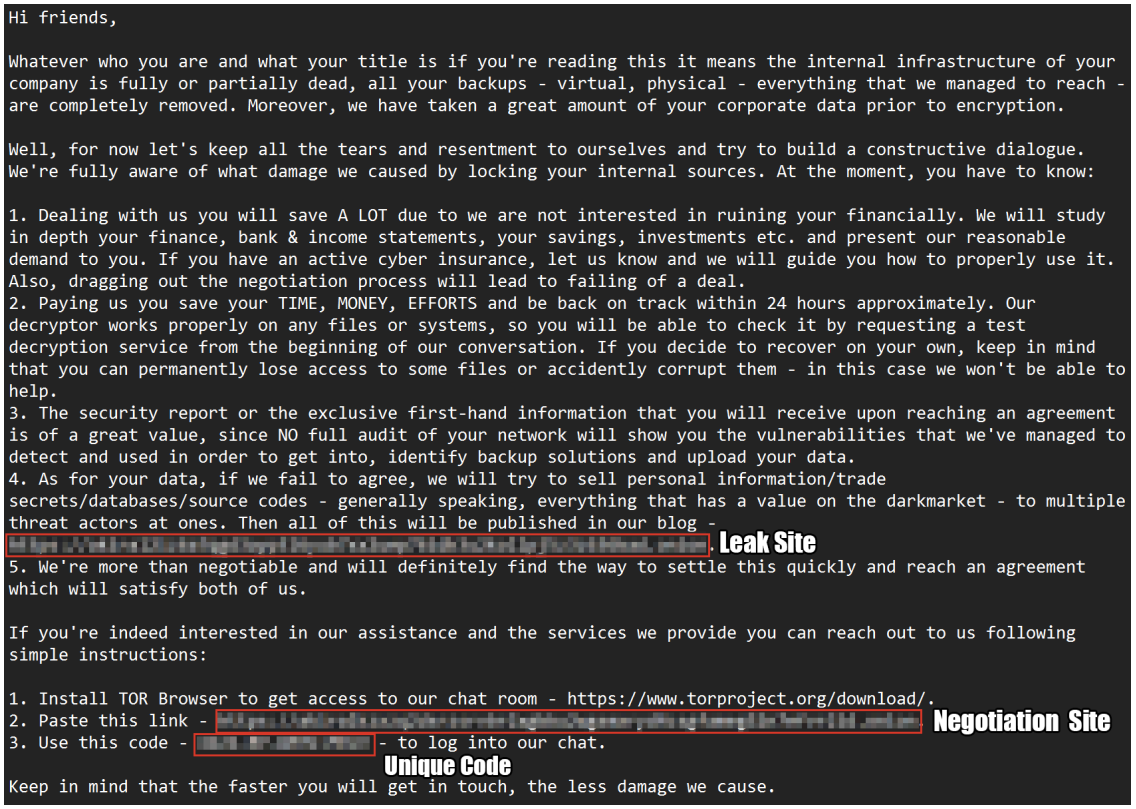

Figure 7. An example of the akira_readme.txt file content.

Windows Variant

Execution

Upon execution, the Windows variant of the Akira ransomware encryptor will attempt to delete shadow copies using the following PowerShell command:

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

Command-Line Arguments

The Windows variant of the Akira ransomware encryptor uses the following command-line arguments:

- -p\--encryption_path – Contains the root directory of the encryption process
- -s\--share_file – Contains the targeted network drive path
- -n\--encryption_percent – Controls the amount of data to be encrypted within each file
- --fork – Creates a child process for the encryption process
- -l – Writes the list of drives into the log file
- -localonly – Prevents the encryption of remote drives
- -e/–exclude – Contains files to exclude from the encryption process

Figure 8 below shows the Windows encryptor for the Akira ransomware detected and prevented by Cortex XDR.

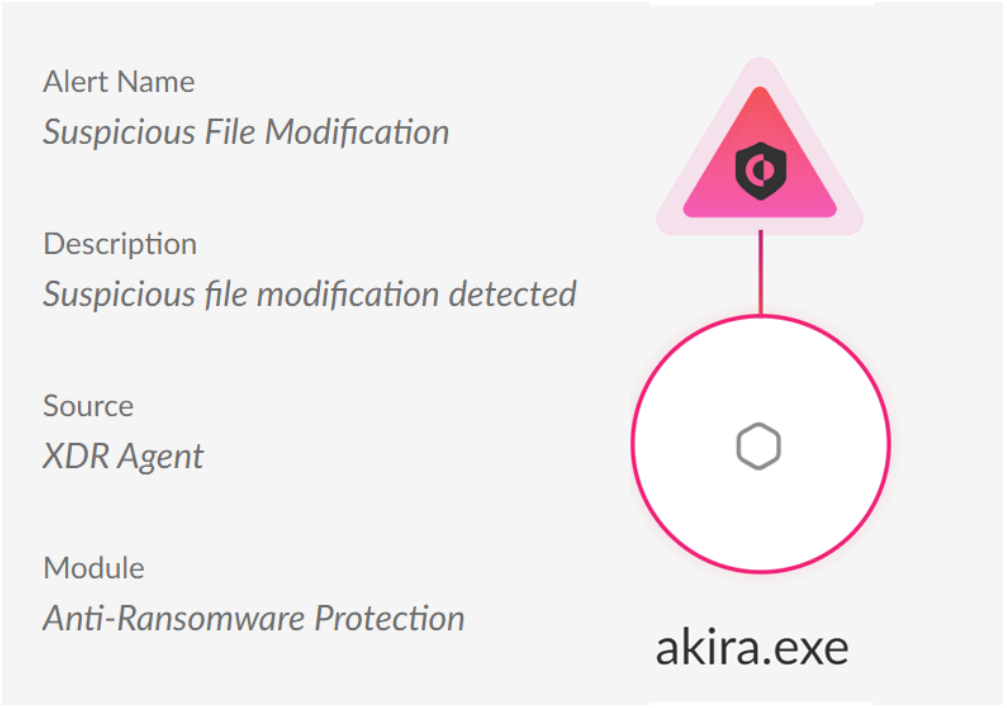

Figure 8. Windows encryptor for Akira ransomware detected by Cortex XDR.

Encryption

Akira ransomware's Windows variant uses a hybrid approach to encrypt data. It encrypts the content of the files using the ChaCha20 algorithm.

The threat then encrypts the ChaCha20 key using a hard-coded RSA public key. The encryptor supports full and partial encryption, controlled through the aforementioned command-line parameter.

Avast published a decryptor in June 2023 exploiting a vulnerability in Akira's encryption scheme. However, CyberCX found a sample in VirusTotal that revealed that Howling Scorpius had patched this vulnerability within three days of its public disclosure.

In February 2024, we identified updates in the Howling Scorpius codebase. These updates included implementing support for the KCipher2 algorithm alongside ChaCha20. Encrypted files would use the .akira extension.

The list of the targeted file extensions and excluded directories the Howling Scorpius Windows encryptor uses can be found in Appendix A.

The Megazord Variant

In August 2023, a new strain of ransomware called Megazord appeared. This strain, written in Rust, has a ransom note with content similar to that of Akira ransomware and points to the same negotiation site. This indicates Howling Scorpius is also the same group behind Megazord.

Besides being written in Rust, Megazord variants differ from Akira encryptors by the following characteristics:

- Using a different file extension for encrypted files – .powerranges

- Using a different name for the ransom note – powerranges.txt

In addition, Megazord encryptors execute several commands to terminate and stop a list of services and processes that could affect the encryption process. For the complete list of commands executed by Megazord encryptors, please view Appendix B.

The Megazord strain has a new layer of protection, requiring a password as an execution condition (defined by the –id command-line argument). Figure 9 demonstrates how Cortex XDR detects and prevents Megazord.

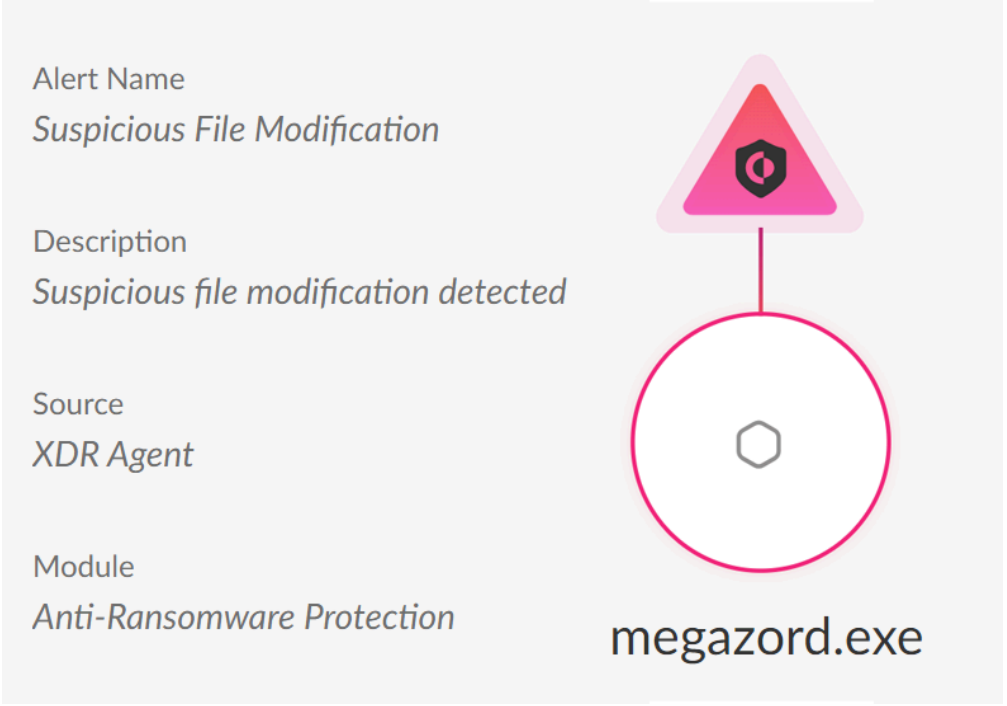

Figure 9. Megazord encryptor detected by Cortex XDR.

Updated Version

While looking for additional Megazord encryptors, we came across two samples that were compiled in March 2024, which had two new command-line arguments affecting the execution flow of the encryptor. The command-line argument –proc allows the attackers to turn off the termination of processes and services, and the –dirs command-line argument allows the attackers to ignore blocklisted directories.

Figure 10 shows the updated help menu from a Megazord sample.

```
Name:
        megazord

Usage:
        cli [args]

Flags:
        --path <string> : Start path
        --id <string>   : Build ID
        --threads <int> : Number of threads (1-1000). Default: number of logical CPU cores
        --ep <int>      : Percent of crypt. Default - 15%
        --logs <string> : Print logs. Valid values for: trace, debug, error, info, warn. Default: off
        --proc <string> : Stopping processes and services from the list. Valid values for: on, off. Default: on
        --dirs <string> : Skipping dirs frot blacklist. Valid values for: on, off. Default: on
        -h, --help      : Show help

Version:
        2023.9.5
```

Figure 10. Megazord variant help menu.

The Possibility of Different Operators Sharing the Megazord Ransomware

Another unique sample we found differs primarily by its ransom note. This new ransom note raises the possibility that Megazord might not be exclusive to Howling Scorpius, although we cannot confirm this yet.

The new ransom note contains distinct language and a different means of communicating via Telegram, which hints at the involvement of a different threat actor. Figure 11 shows the new ransom note.

```
[redacted]
Nothing is working and there's nothing you can do about it? That's because we've
paralyzed your systems.
It's unlikely you can recover your network. You have two ways: call the
police/FBI/President/your mom or whoever and get your business into even more
trouble than it is now.
Or you can contact us and resolve the problem without subjecting yourself to
dirty PR through being presented on our website. It is up to you.
Your data is already stored on one of our drives and is awaiting for your wise
decision. Want to know the volume? Terms? Ask us here [redacted]
or here tox id -
[redacted]. We
can assure you that nobody is aware of the leak and your data is
keeping fully confidential.
But we cannot guarantee the same, if you don't contact us.
```

Figure 11. The new Megazord ransom note.

Linux/ESXi Variant

Based on the internal strings and naming conventions we observed in the Linux/ESXi variants of Akira ransomware, we assess that these samples were initially designed to run on ESXi systems. Some samples we encountered executed ESXCLI commands, strengthening our assessment. Figure 12 shows an example of an internal string found in one of the Linux/ESXi variants.

```
LOAD:00000000005E6B60 aMntDVcprojects db '/mnt/d/vcprojects/Esxi_Build_Esxi7/argh.h',0
```

Figure 12. An example of an internal string of Linux/ESXi samples.

Execution

In some of the Akira Linux variants we have encountered, attackers changed the syslog logs directory to /tmp. It's likely they did this to disable logging and disable the Core Dump file using the following ESXCLI commands:

- /bin/sh -c 'esxcli system syslog config set --logdir=/tmp'
- /bin/sh -c 'esxcli system syslog reload'
- /bin/sh -c 'esxcli system coredump file set --unconfigure'

Command-Line Arguments

The Linux/ESXi variant of the Akira ransomware encryptor uses the following command-line arguments:

- -p\--encryption_path – Specifies the root directory of the encryption process
- -s\--share_file – Specifies the targeted network drive path
- -n\--encryption_percent – Controls the amount of data to be encrypted within each file
- --fork – Creates a child process for the encryption process

Figure 13 demonstrates the detection and prevention of the Linux/ESXi variant by Cortex XDR.

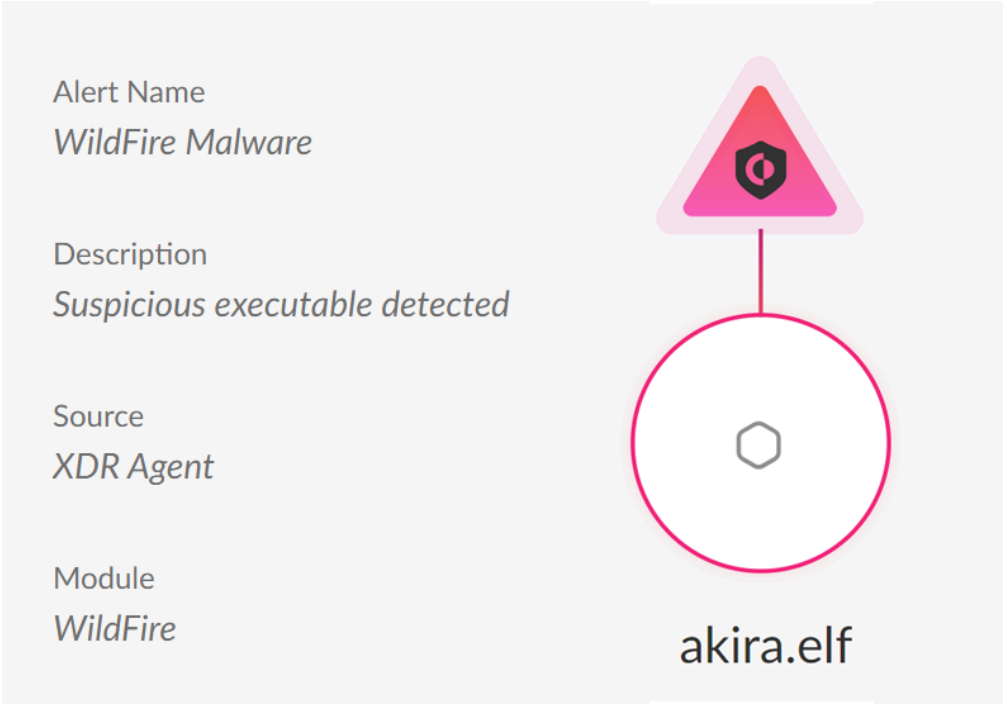

Figure 13. Howling Scorpius Linux/ESXi encryptor detected by Cortex XDR.

Encryption

Akira ransomware's Linux/ESXi variant uses a hybrid encryption approach to lock data, the same as its Windows variant. The Linux/ESXi variant encrypts the symmetric key used to encrypt the content of the targeted files with an embedded RSA public key.

This variant uses several symmetric encryption algorithms for the targeted file encryption, such as AES, CAMELLIA, DES and IDEA. Like the Windows version, this variant supports full and partial encryption controlled through the aforementioned command-line parameters.

The list of targeted file extensions and excluded directories by Akira ransomware's Linux/ESXi encryptor can be found in Appendix C.

Akira v2

In April 2024, CISA's #StopRansomware efforts [PDF] revealed a new variant of the Akira ransomware's Linux/ESXi encryptor called Akira_v2. This Rust-based variant introduces a new command-line argument set and expanded capabilities.

Like Megazord, Akira_v2 also adds a new layer of protection by requesting a password using the –id argument as a run condition. In addition, by using the --vmonly argument, Akira_v2 adds the ability to encrypt VM files only.

Figure 14 shows the help menu unique to this variant.

Figure 14. Akira_v2 help menu.

This variant targets the following file extensions:

- .vmdk
- .vmem
- .vmx
- .log
- .vswp
- .vmsd
- .vmsn

By using the –stopvm argument, the variant adds the ability to turn off running VMs. It does so by executing the following command:

- vim-cmd vmsvc/getallvms | tail -n +2 | awk '{system("vim-cmd vmsvc/power.off " $1)}'.

Also, Akira_v2 uses yet another ransom note file, named akiranew.txt, which still points to the same negotiation site used for the original version of Akira ransomware. Akira_v2 also changes the extension added to encrypted files to .akiranew.

Figure 15 demonstrates how Cortex XDR detects and prevents the Akira_v2 variant.

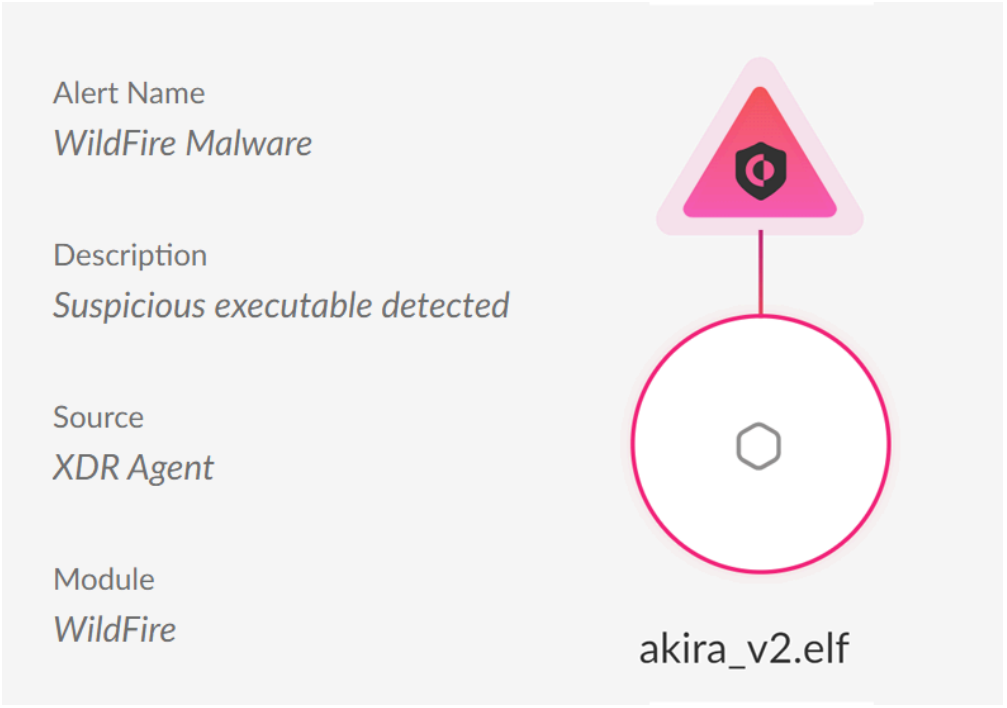

Figure 15. Howling Scorpius's Akira_v2 encryptor detected by Cortex XDR.

Conclusion

This threat assessment demonstrates how Akira ransomware operates, solidifying Howling Scorpius' position among the top five most active ransomware groups despite its relatively recent emergence. The group's developers and affiliates appear to be actively developing new strains and capabilities, as well as making ongoing changes to the toolkit, which contributes to the persistence and prevalence of the ransomware.

We showed how the group used different ransomware variants in tandem, its infection vectors and activity within an infected organization. This group's recent focus on virtualization hosts to affect more endpoints and circumvent security measures means organizations should take the threat seriously and prepare against it.

Palo Alto Networks Protection and Mitigations

For Palo Alto Networks customers, our products and services provide the following coverage associated with this group:

- **Advanced WildFire** cloud-delivered malware analysis service accurately identifies known samples as malicious.
- **Cortex XDR** and **XSIAM** are designed to:
  - Prevent the execution of known malware and also prevent the execution of unknown malware using **Behavioral Threat Protection** and machine learning based on the Local Analysis module.
    - **Anti-Ransomware Module**: It can target encryption-based activities associated with ransomware. It can analyze and halt ransomware activity before data loss occurs, providing proactive protection against the threat discussed in this article.
  - Detect post-exploit activity, including **credential-based attacks**, with behavioral **analytics** through Cortex XDR Pro and XSIAM.

- **Cortex Xpanse** can detect internet-exposed RDP servers and VPN services that have been identified as common initial access targets for this group. **XSIAM** customers with the ASM module also have access to these detection capabilities.

If you think you might have been impacted or have an urgent matter, get in touch with the **Unit 42 Incident Response team** or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings, including file samples and indicators of compromise, with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and disrupt malicious cyber actors systematically. Learn more about the **Cyber Threat Alliance**.

Indicators of Compromise

SHA256 hashes for examples of Akira ransomware's Windows variant

- 08207409e1d789aea68419b04354184490ce46339be071c6c185c75ab9d08cba
- 2727c73f3069457e9ad2197b3cda25aec864a2ab8da3c2790264d06e13d45c3d
- 2db4a15475f382e34875b37d7b27c3935c7567622141bc203fde7fe602bc8643
- 56f1014eb2d145c957f9bc0843f4e506735d7821e16355bcfbb6150b1b5f39db
- 58e9cd249d947f829a6021cf6ab16c2ca8e83317dbe07a294e2035bb904d0cf3
- 678ec8734367c7547794a604cc65e74a0f42320d85a6dce20c214e3b4536bb33
- 1ba1ccfacffbb6be9480380f5535a30d3eee1dd7787f3c649ebf8ea2a6a5de51
- 9f873c29a38dd265decb6517a2a1f3b5d4f90ccd42eb61039086ea0b5e74827e
- 1b6af2fbbc636180dd7bae825486ccc45e42aefbb304d5f83fafca4d637c13cc
- cc970bd2673e46c7e0df5430ab617bc2a9214b4d5c2c44252af681a08ff526a8

SHA256 hashes for examples of Megazord

- 131da83b521f610819141d5c740313ce46578374abb22ef504a7593955a65f07
- 28cea00267fa30fb63e80a3c3b193bd9cd2a3d46dd9ae6cede5f932ac15c7e2e
- 2f629395fdfa11e713ea8bf11d40f6f240acf2f5fcf9a2ac50b6f7fbc7521c83
- 68d5944d0419bd123add4e628c985f9cbe5362ee19597773baea565bff1a6f1a
- 7f731cc11f8e4d249142e99a44b9da7a48505ce32c4ee4881041beeddb3760be
- 8816caf03438cd45d7559961bf36a26f26464bab7a6339ce655b7fbad68bb439
- 95477703e789e6182096a09bc98853e0a70b680a4f19fa2bf86cbb9280e8ec5a
- 9585af44c3ff8fd921c713680b0c2b3bbc9d56add848ed62164f7c9b9f23d065
- 9f393516edf6b8e011df6ee991758480c5b99a0efbfd68347786061f0e04426c
- a6b0847cf31ccc3f76538333498f8fef79d444a9d4ecfca0592861cf731ae6cb
- b55fbe9358dd4b5825ce459e84cd0823ecdf7b64550fe1af968306047b7de5c9
- c0c0b2306d31e8962973a22e50b18dfde852c6ddf99baf849e3384ed9f07a0d6

- c9c94ac5e1991a7db42c7973e328fceeb6f163d9f644031bdfd4123c7b3898b0
- dfe6fddc67bdc93b9947430b966da2877fda094edf3e21e6f0ba98a84bc53198
- e3fa93dad8fb8c3a6d9b35d02ce97c22035b409e0efc9f04372f4c1d6280a481
- 28cea00267fa30fb63e80a3c3b193bd9cd2a3d46dd9ae6cede5f932ac15c7e2e
- dfe6fddc67bdc93b9947430b966da2877fda094edf3e21e6f0ba98a84bc53198
- 0c0e0f9b09b80d87ebc88e2870907b6cacb4cd7703584baf8f2be1fd9438696d

SHA256 hashes for examples of Akira ransomware's Linux/ESXi variant

- 1d3b5c650533d13c81e325972a912e3ff8776e36e18bca966dae50735f8ab296
- 300bc2769c6d62ba9d228cc45e126cd458e1a23fd23092da258053afd82f2755
- 3805f299d33ef43d17a5a1040149f0e5e2d5db57ec6f03c5687ac23db1f77a30
- 3999a25f8f0fd8252aa9250fa9bd70aae202f181812cc6c230c8ea2842340f18
- 3dc7d4023c7380ed740ac5ac7d82a4ba6f587f430b2b7b66f1d34a44f89c39cb
- 43c5a487329f5d6b4a6d02e2f8ef62744b850312c5cb87c0a414f3830767be72
- 6005dcbe15d60293c556f05e98ed9a46d398a82e5ca4d00c91ebec68a209ea84
- 74f497088b49b745e6377b32ed5d9dfaef3c84c7c0bb50fabf30363ad2e0bfb1
- 7ca3e6b4dd4d98506faa92ab590108cacb2945b8c27dcf1ac75b0df4a206493a
- 82e25f32e01f1898ccce2b6d5292245759733c22a104443a8a9c7db1ebf05c57
- 8e9a33809b9062c5033928f82e8adacbef6cd7b40e73da9fcf13ec2493b4544c
- bcae978c17bcddc0bf6419ae978e3471197801c36f73cff2fc88cecbe3d88d1a
- 5f72bdb14e138f10c1658248fdaf10db2fd1e812240966e009bbcf8d463e099c
- 67f82a54ea49c6f286681d179cc7afc8b41b6b34284cc17bdd52916cc3656160
- 6a5e547756ef1256f1eb9df0249245c35461affd009be8f046559bc007cafcf2
- e702a572b514984deacaa54408059c6eac28e46111cb6f0f4190a3a6a72dd41d

SHA256 hashes for examples of Akira_v2

- 0ee1d284ed663073872012c7bde7fac5ca1121403f1a5d2d5411317df282796c
- 3298d203c2acb68c474e5fdad8379181890b4403d6491c523c13730129be3f75

Additional Resources

- Ransomware Spotlight: Akira – Trend Micro Research
- #StopRansomware: Akira Ransomware [PDF] – CISA
- Akira Ransomware is “bringin’ 1988 back” – Sophos
- Akira, again: The ransomware that keeps on taking – Sophos
- Ransomware Roundup - Akira – Fortinet
- Megazord ransomware analysis – Cynet

Appendices

Appendix A: Akira Ransomware Windows Variant: Targeted File Extensions

Howling Scorpius Windows encryptors will avoid encrypting files with the following extensions:

- .exe
- .dll
- .lnk
- .sys
- .msi
- .akira

Additionally, the Windows encryptor will avoid the following directories:

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

Akira ransomware's Windows encryptors target the following extensions:

Letter Range	Extension
A-L	.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, .fdb, .fic, .fm5, .fmp, .fmp12, .fmpsl, .fol, .fp3, .fp4, .fp5, .fp7, .fpt, .frm, .gdb, .grdb, .gwi, .hdb, .his, .hjt, .ib, .icg, .icr, .idb, .ihx, .iso, .itdb, .itw, .jet, .jtx, .kdb, .kexi, .kexic, .kexis, .lgc, .lut, .lwx
M-Z	.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, .temx, .tmd, .tps, .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

Appendix B: Megazord Termination Commands

- cmd.exe /c net stop "IBM Domino Diagnostics (CProgramFilesIBMDomino)"
- cmd.exe /c net stop "IBM Domino Server (CProgramFilesIBMDominodata)"

- cmd.exe /c net stop "Simply Accounting Database Connection Manager"
- cmd.exe /c net stop IISADMIN
- cmd.exe /c net stop MSExchangeADTopology
- cmd.exe /c net stop MSExchangeFBA
- cmd.exe /c net stop MSExchangeIS
- cmd.exe /c net stop MSExchangeSA
- cmd.exe /c net stop MSSQL$ISARS
- cmd.exe /c net stop MSSQL$MSFW
- cmd.exe /c net stop MSSQLServerADHelper100
- cmd.exe /c net stop MSSQLServerADHelper100
- cmd.exe /c net stop QBCFMonitorService
- cmd.exe /c net stop QBPOSDBServiceV12
- cmd.exe /c net stop QBVSS
- cmd.exe /c net stop QuickBooksDB1
- cmd.exe /c net stop QuickBooksDB10
- cmd.exe /c net stop QuickBooksDB11
- cmd.exe /c net stop QuickBooksDB12
- cmd.exe /c net stop QuickBooksDB13
- cmd.exe /c net stop QuickBooksDB14
- cmd.exe /c net stop QuickBooksDB15
- cmd.exe /c net stop QuickBooksDB16
- cmd.exe /c net stop QuickBooksDB17
- cmd.exe /c net stop QuickBooksDB18
- cmd.exe /c net stop QuickBooksDB19
- cmd.exe /c net stop QuickBooksDB2
- cmd.exe /c net stop QuickBooksDB20
- cmd.exe /c net stop QuickBooksDB21
- cmd.exe /c net stop QuickBooksDB22
- cmd.exe /c net stop QuickBooksDB23
- cmd.exe /c net stop QuickBooksDB24
- cmd.exe /c net stop QuickBooksDB25
- cmd.exe /c net stop QuickBooksDB3
- cmd.exe /c net stop QuickBooksDB4
- cmd.exe /c net stop QuickBooksDB5
- cmd.exe /c net stop QuickBooksDB6
- cmd.exe /c net stop QuickBooksDB7
- cmd.exe /c net stop QuickBooksDB8
- cmd.exe /c net stop QuickBooksDB9
- cmd.exe /c net stop ReportServer$ISARS
- cmd.exe /c net stop SPAdminV4
- cmd.exe /c net stop SPSearch4
- cmd.exe /c net stop SPTimerV4

- cmd.exe /c net stop SPTraceV4
- cmd.exe /c net stop SPUserCodeV4
- cmd.exe /c net stop SPWriterV4
- cmd.exe /c net stop SQLAgent$ISARS
- cmd.exe /c net stop SQLAgent$MSFW
- cmd.exe /c net stop SQLBrowser
- cmd.exe /c net stop SQLWriter
- cmd.exe /c net stop ShadowProtectSvc
- cmd.exe /c net stop WinDefend
- cmd.exe /c net stop firebirdguardiandefaultinstance
- cmd.exe /c net stop ibmiasrw
- cmd.exe /c net stop mr2kserv
- cmd.exe /c powershell -command "Get-VM | Stop-VM -Force"
- cmd.exe /c taskkill /f /im CNTAoSMgr*
- cmd.exe /c taskkill /f /im IBM*
- cmd.exe /c taskkill /f /im Notifier*
- cmd.exe /c taskkill /f /im Ntrtscan*
- cmd.exe /c taskkill /f /im TmListen*
- cmd.exe /c taskkill /f /im bes10*
- cmd.exe /c taskkill /f /im black*
- cmd.exe /c taskkill /f /im chrome*
- cmd.exe /c taskkill /f /im copy*
- cmd.exe /c taskkill /f /im ds_monitor*
- cmd.exe /c taskkill /f /im dsa*
- cmd.exe /c taskkill /f /im excel*
- cmd.exe /c taskkill /f /im firefox*
- cmd.exe /c taskkill /f /im iVPAgent*
- cmd.exe /c taskkill /f /im iexplore*
- cmd.exe /c taskkill /f /im mysql*
- cmd.exe /c taskkill /f /im outlook*
- cmd.exe /c taskkill /f /im postg*
- cmd.exe /c taskkill /f /im putty*
- cmd.exe /c taskkill /f /im robo*
- cmd.exe /c taskkill /f /im sage*
- cmd.exe /c taskkill /f /im sql*
- cmd.exe /c taskkill /f /im ssh*
- cmd.exe /c taskkill /f /im store.exe
- cmd.exe /c taskkill /f /im tasklist*
- cmd.exe /c taskkill /f /im taskmgr*
- cmd.exe /c taskkill /f /im vee*
- cmd.exe /c taskkill /f /im veeam*
- cmd.exe /c taskkill /f /im wrsa*

- cmd.exe /c taskkill /f /im wrsa.exe

Appendix C: Akira Ransomware Linux\ESXi Variant: Targeted File Extensions

Akira ransomware's Linux\ESXi encryptors will avoid encrypting files with the following extensions, the same as the Windows encryptors:

- .exe
- .dll
- .lnk
- .sys
- .msi
- .akira

Additionally, the Linux\ESXi encryptor will avoid the following directories:

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

Akira ransomware's Linux\ESXi encryptors target the following extensions:

Letter Range	Extension
A-L	.4dd, .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-shm, .db-wa, .db2, .db3, .dbc, .dbf, .dbs, .dbt, .dbv, .dbx, .dcb, .dct, .dcx, .dlis, .dp1, .dqy, .dsk, .dsn, .dtsx, .eco, .ecx, .edb, .epim, .exb, .fcd, .fdb, .fic, .fm5, .fmp, .fmp12, .fmps, .fp3, .fp4, .fp5, .fp7, .fpt, .frm, .gdb, .grdb, .gwi, .hdb, .his, .hjt, .icg, .icr, .idb, .ihx, .iso, .itdb, .itw, .jet, .jtx, .kdb, .kexi, .kexic, .kexis, .lgc, .lut, .lwx
M-Z	.maf, .maq, .mar, .mas, .mav, .maw, .mdb, .mdf, .mdn, .mdt, .mpd, .mrg, .mud, .mwb, .myd, .ndf, .nnt, .nrmlib, .ns2, .ns3, .ns4, .nsf, .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, .sqlite, .sqlite3, .sqlitedb, .subvo, .temx, .tmd, .tps, .trc, .trm,

	.udb, .usr, .v12, .vdi, .vhd, .vhdx, .vis, .vmcx, .vmdk, .vmem, .vmrs, .vmsd, .vmsn, .vmx, .vpd, .vsv, .vvv, .wdb, .wmdb, .wrk, .xdb, .xld, .xmlff

Table of Contents

-
- Executive Summary
- Howling Scorpius Overview
  - Targeted Regions
  - Targeted Industries
- Technical Analysis of the Akira Ransomware Attack Lifecycle
  - Initial Access
  - Credentials Access
    - Local Credential Access Techniques
    - Kereberoasting
    - Extracting Credentials for Domain Control
    - Exploiting Compromised vCenter Instances
  - Persistence
  - Discovery and Lateral Movement
  - Defense Evasion
    - Bring Your Own Driver
    - Anti Virus Disablement
    - Bring Your Own VM
  - Exfiltration
- Akira Ransomware Encryptors
  - Ransom Note
  - Windows Variant
    - Execution
    - Command-Line Arguments
    - Encryption
  - The Megazord Variant
    - Updated Version
    - The Possibility of Different Operators Sharing the Megazord Ransomware
  - Linux/ESXi Variant
    - Execution
    - Command-Line Arguments
    - Encryption
    - Akira v2
- Conclusion
  - Palo Alto Networks Protection and Mitigations
- Indicators of Compromise
- Additional Resources

- Appendices
  - Appendix A: Akira Ransomware Windows Variant: Targeted File Extensions
  - Appendix B: Megazord Termination Commands
  - Appendix C: Akira Ransomware Linux\ESXi Variant: Targeted File Extensions

Related Articles

- Suspected China-Based Espionage Operation Against Military Targets in Southeast Asia
- From Linear to Complex: An Upgrade in RansomHouse Encryption
- 01flip: Multi-Platform Ransomware Written in Rust