Akira Ransomware

Executive Summary
Akira ransomware is a relatively new ransomware gang that has demonstrated aggressive and capable targeting of the U.S. health sector in its short lifespan. U.S. healthcare organizations are advised to follow the steps in this alert to minimize their risk of attack.

Overview
Akira ransomware was first identified in May of 2023, and in less than a year, it has claimed at least 81 victims. It should not be confused with another ransomware variant known as Akira, which was briefly observed in 2017 but is believed to be unrelated to the most recent and active variant, which is the subject of this paper. There is research suggesting that Akira has connections to the now-defunct Conti ransomware gang. The technical details of this include similarities in their exploitation approach, the selection of certain types of files and directories for targeting, their choice of application for encryption algorithms, their use of ransom payment addresses, and the incorporation of comparable functions. While any formal relationship or connection between the two groups has not been confirmed, such a connection could indicate a degree of sophistication to Akira’s operations, and reinforce the idea that they are highly capable and should be considered a serious threat.

Akira leverages many common features for their targeting and operations. They operate as ransomware-as-a-service (RaaS), which is to say they focus on the ransomware operations, but partner with other cybercriminals for individual attacks and share the extorted fees. They also conduct double extortion; they steal sensitive data, deploy their ransomware, and then charge two fees. The first fee restores the encrypted systems, and the second fee ensures no leaks of stolen data. They are highly reliant on credential compromise as an infection vector, which provides them initial access into their target networks. Akira also operates a leak site where they publicly post information on their victims. Their targeting includes both Windows and Linux infrastructure, and while organizations in the United States are their focus, their targeting is global. They are also known to target the United Kingdom, Canada, Australia, New Zealand and other countries.

Targeting and Scope of Attacks
Research indicates that geographically, while Akira is global in their targeting, their focus continues to be on the United States. Their targeting within the United States has been focused on organizations in California, Texas, Illinois, and the East Coast, especially the Northeast. This appears to be due to the geographic locations of specific targets, rather than deliberately targeting these states. Akira’s most-targeted industries include materials, manufacturing, goods and services, construction, education, finance, legal, and healthcare. Open source reporting

Figure 1: Akira victim distribution by country. (Source: Trellix)
and analysis consistently shows the health sector being one of the top industries targeted by Akira.

**Tactics, Techniques, and Procedures (TTPs)**
The following is a list of known tactics and techniques commonly used by the Akira ransomware gang, mapped against the MITRE ATT&CK framework. This list represents a significant collection of the most frequent activities by Akira, however it is not a comprehensive list. The references section of this report contains resources where additional details on Akira attacks, including other tactics and techniques, can be found.

**Initial Access**
- T1566.001 - Spearphishing Attachment
- T1566.002 - Spearphishing Link
- T1078 - Valid Accounts
- T1190 - Exploit Public-Facing Application
- T1195 - Supply Chain Compromise

**Privilege Escalation**
- T1078 - Valid Accounts
- T1136.002 – Create Account: Domain Account
- T1547.009 - Shortcut Modification
- T1547.001 - Registry Run Keys / Startup Folder

**Persistence**
- T1078 - Valid Accounts
- T1547.009 - Shortcut Modification
- T1547.001 - Registry Run Keys / Startup Folder

**Lateral Movement**
- T1570 – Lateral Tool Transfer

**Data Collection**
- T1114.001 - Local Email Collection

**Data Exfiltration**
- T1567 - Exfiltration Over Web Service
- T1041 - Exfiltration Over C2 Channel
- T1537 - Transfer Data to Cloud Account
- T1029 - Scheduled Transfer
- T1020 - Automated Exfiltration

**Execution**
- T1059.001 - PowerShell
- T1569.002 - Service Execution
- T1059.003 - Windows Command Shell

**Impact**
Defensive Evasion

T1078 - Valid Accounts
T1027.001 - Binary Padding
T1036.005 - Match Legitimate Name or Location
T1562.001 – Impari Defenses: Disable or Modify Tools

The below diagram is a step-by-step illustration of an Akira attack, leveraging several of the tactics and techniques described immediately above. In the below example, the Akira gang exploits a vulnerability in virtual private network software to gain initial access to their target. They then create an account (ostensibly via the VPN application) in order to establish persistent access to the network. After using appropriate tools to attempt to obscure their activities from detection, they immediately begin conducting network reconnaissance (discovery) to understand their operational environment. They leverage tools to acquire existing credentials, move around the infrastructure and establish communications (command and control) back to their infrastructure. They finally steal data and deploy ransomware.

Figure 3: Akira attack diagram with typical MITRE-mapped tactics and techniques. (Source: Trend Micro)
Due to the nature of their operations, ransomware operators are enticed by data storage – both in-house and outsourced – and this can be seen in some of the more recent targeting by Akira. For example, in January of 2024, Akira successfully targeted the Finnish IT software and service company, Tietoevry, and more specifically, their cloud hosting infrastructure. Furthermore, the Finnish National Cybersecurity Center reported on a campaign in December of 2023, where Akira was targeting network-attached storage devices in order to completely wipe them of data, allowing them to potentially ramp up extortion pressure even further. In the latter case, Akira exploited an unauthorized access vulnerability in the VPN feature in Cisco’s Adaptive Security Appliance and Firepower Threat Defense platforms, tracked as CVE-2023-20269. This allows unauthorized attackers – in this case, Akira – to carry out brute force attacks (see Figure 4 as an example of an attempt to compromise a Cisco VPNs) and locate existing user credentials. Following initial access, observed activity in this campaign included network reconnaissance and mapping, compromising credentials, and data encryption. Some of the usernames utilized for device compromise in this campaign included: admin, adminadmin, backupadmin, kali, cisco, guest, accounting, developer, ftp user, training, test, printer, echo, security, inspector, test temp, and snmp. Upon successful authentication, set.bat was sometimes deployed, which installed and executed the remote desktop tool AnyDesk, with a configured password "greenday#@!". In some instances, nd.exe was executed on systems to dump NTDS,DIT, and the SAM and SYSTEM hives. As noted in this campaign, this may have given the adversary access to additional domain credentials. This was followed by lateral movement and binary executions on other systems to increase the scope of compromise. In several cases, the final result of the attack was the deployment of Akira ransomware.
Financials
As previously mentioned, there are technical indicators that the Akira ransomware gang might have some connection to the Conti ransomware gang. Conti discontinued operations shortly after the Russian incursion into Ukraine in February of 2022, and the subsequent leaking of the Conti code, which was ostensibly prompted by infighting within the group caused by divided alliances related to the Russia-Ukraine war. In addition to similarities between operational procedures and technical aspects of the ransomware code, an additional connection exists: financial infrastructure. Cryptocurrency transactions are not completely anonymous. This is due to the fact that all of them—Bitcoin and the altcoins—all operate on a blockchain, which is a distributed, public digital ledger. The public nature of blockchain makes transactions open to examination by the public. While certain technologies can make this more complicated, such as the use of privacy coins, mixers or privacy wallets, a cryptocurrency transaction could not be conducted with 100% certainty of privacy. To some extent, attribution is almost always possible, even if exceptionally challenging in some cases. According to analysis of the transaction details between Akira victims and the Akira group itself, there is shared infrastructure between Akira and Conti, bolstering the case that there is an overlap of talent between the two groups. In an examination of Akira's known cryptocurrency wallet addresses, pattern analysis of the transactions allows for the discovery of additional

Figure 6: Overlapping financial infrastructure between Akira and Conti. (Source: Arctic Wolf)
wallet addresses, and in some cases, this effort has uncovered instances of certain wallets being reused between both Akira and Conti. This potentially indicates that one or more individuals who were active members of Conti subsequently joined Akira after the dissolution of Conti. This determination cannot be made definitively, but when considered along with previous technical overlaps between the two groups, the possibility of talent utilized across both groups becomes increasingly likely. This assessment is important in understanding the level of sophistication within the Akira group. Conti was an established and highly-capable ransomware gang, believed to be the predecessor to or overlapping with a previous ransomware gang named Ryuk. This indicates that Akira includes members who have a long and successful history of operating ransomware, making the group a significant threat to potential victims.

Defense and Mitigations
The following resources and guidance are provided by various elements of the federal government to assist the health sector in defending against, mitigating the effects of, and reporting ransomware attacks:

- **DHS/CISA Stop Ransomware**: https://www.cisa.gov/stopransomware
- **FBI Cybercrime**: https://www.fbi.gov/investigate/cyber
- **FBI Internet Crime Complaint Center (IC3)**: https://www.ic3.gov/Home/ComplaintChoice/default.aspx/
- **H-ISAC White Papers**: https://h-isac.org/category/h-isac-blog/white-papers/
- **405(d) Resource Library**: https://405d.hhs.gov/resources
- **HC3 Products**: https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html

Furthermore, the FBI recommends the following steps:

- Review domain controllers, servers, workstations, and active directories for new or unrecognized user accounts.
- Regularly back up data, air gap, and password-protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Review Task Scheduler for unrecognized scheduled tasks. Additionally, manually review operating system-defined or system-recognized scheduled tasks for unrecognized “actions.” (For example, review the steps each scheduled task is expected to perform.)
- Review anti-virus logs for indications that they were unexpectedly turned off.
- Implement network segmentation.
- Require administrator credentials to install software.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (e.g., hard drive, storage device, the cloud).
- Install updates/patch operating systems, software, and firmware as soon as updates/patches are released.
- Use multi-factor authentication where possible.
- Regularly change the passwords to network systems and accounts and avoid re-using passwords for different accounts.
- Implement the shortest acceptable timeframe for password changes.
HC3: Analyst Note  
February 7, 2024     TLP:CLEAR     Report: 202402071200

- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Install and regularly update anti-virus and anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a virtual private network (VPN).
- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails.

Also, the 3-2-1 rule is important to implement across the enterprise. This means:
- Maintain at least three copies of all important files.
- Store these files on two different media types.
- Ensure one copy is offsite and preferably offline.

In addition to the above generic ransomware guidance, the following resources will assist the health sector in defending against and mitigating the effects of Akira ransomware attacks:

**Indicators of compromise:**
- Kaspersky: 0885b3153e61caa56117770247be0444
- Kaspersky: 02cda932f5a9dafb0a328d0f9788bd89c
- Kaspersky: 00141f86063092192baf046fd998a2d1
- Rapid7 IP addresses can be found here.
- Avast hashes listed below can be found here.
- Sophos has developed a Yara rule which can be found here.
- Trend Micro hashes can be found here.

**Health sector organizations would be well-advised to take the following steps to defend against Akira attacks:**

- Ensure identity and access management capabilities are in place, robust, and properly configured.
  - This is especially applicable to multi-factor authentication (MFA) for VPNs. Akira has a history of compromising VPNs that are not protected with MFA.
- Akira is heavily focused on exploiting legitimate remote access tools in addition to previously-mentioned VPNs, which include AnyDesk and tools that leverage the Remote Desktop Protocol.
  - Patch management for these tools (as well as other applications, especially those that are Internet-facing) is critical.
- Ensure credentials are properly protected and appropriate password maintenance/update policies are in place and enforced. Akira has a history of compromising credentials stored in Active Directory and dumping LSASS process memory.
  - Adding user accounts to security-enabled local groups will help prevent against Akira’s compromise of accounts to establish persistent access.
  - Monitoring for account compromise and unusual activity, and ensuring old, unused accounts are automatically deleted after a period of time can help reduce the attack surface.
Avast released a decryptor for Akira which can be found [here](#).

**Conclusions**
The Akira ransomware gang, despite having only operated for a short period of time, has proved to be a significant threat to the U.S. public and private health sectors. While many of the recommend defense and mitigation actions apply universally to most ransomware gangs, there are Akira-specific details in this alert which should also be implemented. Finally, while the technical details and actions contained in this alert are up-to-date, it is also worth noting that cybercriminals, especially major ransomware operators such as Akira, evolve over time. It will be important for any healthcare organization that wishes to stay secure in cyberspace to keep up with Akira’s latest tactics, techniques and procedures (TTPs). HC3 will continue to release products as appropriate on a number of cybercriminal threats, including Akira, but it is critical for healthcare organizations to continuously monitor open-source reporting on Akira and consider any commercial threat intelligence support to augment public information as appropriate.

**References**
Meet Akira — A new ransomware operation targeting the enterprise

Akira, again: The ransomware that keeps on taking

Ransomware-spotlight: Akira

Akira Ransomware is “bringin’ 1988 back”

Akira Ransomware
[https://www.trellix.com/about/newsroom/stories/research/akira-ransomware/](https://www.trellix.com/about/newsroom/stories/research/akira-ransomware/)

Akira Ransomware: What SOC Teams Need to Know
[https://cyberint.com/blog/research/akira-ransomware-what-soc-teams-need-to-know/](https://cyberint.com/blog/research/akira-ransomware-what-soc-teams-need-to-know/)

Akira Stealer : An Undetected Python Based Info-stealer

Ransomware Roundup - Akira
[https://www.fortinet.com/blog/threat-research/ransomware-roundup-akira](https://www.fortinet.com/blog/threat-research/ransomware-roundup-akira)

Akira Ransomware
[https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2023-2113](https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2023-2113)

Cisco ASA Zero-Day Exploited in Akira Ransomware Attacks

[TLPCLEAR, ID#202402071200, Page 8 of 13]
Akira Ransomware Targeting VPNs without Multi-Factor Authentication

From Conti to Akira | Decoding the Latest Linux & ESXi Ransomware Families

Akira ransomware targets Cisco VPNs to breach organizations

Conti and Akira: Chained Together
https://arcticwolf.com/resources/blog/conti-and-akira-chained-together/

Blockchain data shows Conti gang tied to Akira and spate of ransomware attacks

Free Akira ransomware decryptor helps recover your files

Decrypted: Akira Ransomware
https://decoded.avast.io/threatresearch/decrypted-akira-ransomware/

Linux version of Akira ransomware targets VMware ESXi servers

Akira ransomware - what you need to know

Unraveling Akira Ransomware
https://cyble.com/blog/unraveling-akira-ransomware/

Finland warns of Akira ransomware wiping NAS and tape backup devices

Under Siege: Rapid7-Observed Exploitation of Cisco ASA SSL VPNS

**Appendix A: Additional Supporting Data Points**
The following information is intended to augment/reinforce the main content of this alert.

According to research from **Trend Micro** and **Avast**, Akira does not encrypt the following file types:
Akira also avoids encrypting the following directories:

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

Akira is known to encrypt the following file types:

- .4dd
- .cpd
- .dsk
- .gdb
- .mav
- .owc
- .spq
- .xld
- .4dl
- .dacpac
- .dsn
- .grdb
- .mdb
- .p96
- .sql
- .xmlff
- .accdb
- .dad
- .dtsx
- .gwi
- .msd
- .p97
- .sqlite
- .abcddbb
- .accdbc
- .dadiagrams
- .dxl
- .hdb
- .mpd
- .pan
- .sqlite3
- .abs
- .accde
- .daschema
- .eco
- .his
- .mrg
- .pdb
- .sqlitedb
- .abx
- .accdr
- .db
- .ex
- .ib
- .mud
- .pdm
- .te
- .accdw
- .acctdt
- .db-shm
- .edb
- .idb
- .mbw
- .pnz
- .tem
- .adn
- .accft
- .db-wal
- .epim
- .ihx
- .myd
- .qry
- .tmd
- .db2
- .adb
- .db3
- .exb
- .ltdb
- .ndf
- .qvd
- .tps
- .fm5
- .ade
- .dbc
- .fcd
- .itd
- .nt
- .rbd
- .tcr
- .hjt
- .adf
- .dbf
- .fdb
- .jet
- .nrmli
- .rcfd
- .tmd
- .icg
- .adp
- .dbs
- .fch
- .jtx
- .nrmlib
- .rd
- .udb
- .icr
- .arc
- .db
- .fmp
- .kdb
- .ns3
- .rodx
- .udl
- .kdb
- .ora
- .dbv
- .fmp12
- .kexi
- .ns4
- .rdp
- .usr
- .lut
- .alf
- .dxx
- .fmps
- .kexic
- .nsf
- .rsd
- .v12
- .maw
- .ask
- .dcb
- .fol
- .kexis
- .nv
- .sas7bdat
- .vis
- .mdn
- .btr
- .dct
- .fol
- .lgc
- .nv2
- .sbf
- .vdp
- .mdt
- .bd
- .dxx
- .fp4
- .lwx
- .nwb
- .scx
- .v4
- .cat
- .ddl
- .fp5
- .maf
- .nfy
- .sdb
- .wdb
- .cd
- .dis
- .fp7
- .maq
- .odb
- .sdc
- .wdb
- .ckp
- .dp1
- .fpt
- .mar
- .oqy
- .sdf
- .wmdb
- .cma
- .dny
- .frm
- .mas
- .orx
- .sis
- .xdb

The following graphic by Trellix shows the how commands and arguments are processed:
The below histogram from **Trellix** shows the published victim count from April to November of 2023:

![Histogram showing published victim count from April to November 2023](image)

The below diagram from **Trend Micro** walks through many of the steps of a typical Akira attack:
Initial Access
Akira ransomware actors are known to use compromised VPN credentials to gain initial access. They've also been observed to target vulnerable Cisco VPNs by exploiting CVE-2023-20269, a zero-day vulnerability that affects Cisco ASA and FTD.

Persistence
Akira operators have been observed creating a new domain account on the compromised system to establish persistence.

Defense Evasion
For its defense evasion, Akira ransomware actors have been observed using PowerTool or a KillAV tool that abuses the Zemana AntiMalware driver to terminate AV-related processes.

Discovery
The actors behind the Akira ransomware have been observed using the following to gain knowledge on the victim’s system and its connected network:
- PCHunter and SharpHound to gather system information
- AdFind alongside the net Windows command and nttstat to obtain domain information
- Advanced IP Scanner and MASSCAN to discover other remote systems

Credential Access
Akira ransomware operators use Mimikatz, LaZagne, or a specific command line to gather credentials.

Lateral Movement
Akira actors use Windows RDP to move laterally within the victim’s network.

Command and control
To gain remote access on other targeted systems, malicious actors may use any or a combination of the following tools:
- AnyDesk
- MobaXterm
- Radmin
- RustDesk
- Cloudflare Tunnel
- Nginx

Exfiltration
Akira ransomware operators have been observed using the third-party tool and web service RClone to exfiltrate stolen information. Moreover, they have also been observed using either FileZilla or WinSCP to exfiltrate stolen information via File Transfer Protocol (FTP).

Impact
Akira ransomware encrypts targeted systems using a hybrid encryption algorithm that combines ChaCha20 and RSA. Additionally, the Akira ransomware binary, like most modern ransomware binaries, has a feature that allows it to inhibit system recovery by deleting shadow copies from the affected system.

Global and U.S. targeting data from Trellix are contained in the two diagrams below:
Contact Information
If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback