HC3: Sector Alert

September 12, 2023 TLP:CLEAR Report: 202309121400

Akira Ransomware

Executive Summary

Akira is a Ransomware-as-a-Service (RaaS) group that started operations in March 2023. Since its discovery, the group has claimed over 60 victims, which have typically ranged in the small- to medium-size business scale. Akira has garnered attention for a couple of reasons, such as their retro 1980s-themed website (see figure below) and the considerable demands for ransom payments ranging from $200,000 to $4 million. Akira has been observed obtaining initial malware delivery through several methods, such as leveraging compromised credentials and exploiting weaknesses in virtual private networks (VPN), typically where multi-factor authentication (MFA) is not being used. Like many ransomware groups, they employed the double-extortion technique against their victims by exfiltrating data prior to encryption. It is also believed that the group may contain some affiliation with Conti due to observed overlap in their code and cryptocurrency wallets. The group has targeted multiple sectors, including finance, real estate, manufacturing, and healthcare.

Overview of Akira

The Akira ransomware was first seen in March 2023. In 2017, another ransomware named Akira was observed, but these two are not considered to be associated. The Akira ransomware targets Windows and Linux systems. The Windows variant is a 64-bit Windows binary that was written in C++, the ransomware creates a symmetric key encrypted by the RSA-4096 cipher.

Akira Data Leak Site *(Source: Bleeping Computer)*

It avoids encrypting files with .exe, .lnk, .dll, .msi, .sys, and akira_readme.txt. Additionally, it avoids the winnt, temp, thumb, $Recycle.bin, $RECYCLE.BIN, system volume information, boot, windows, and Trend

Micro folders.

The Linux version of Akira is also a 64-bit executable, which targets VMware ESXi servers and behaves similarly to the Windows variant, except the Windows version uses the Windows CryptoAPI and the Linux version uses the Crypto++ library. Bleeping Computer has noted that "Akira's encryptors do not contain many advanced features, such as the automatic shutting down of virtual machines before encrypting files using the esxcli command." The command line does contain arguments which would allow the attacker to customize their attacks:

Argument	Function
-p --encryption_path	targeted file/folder paths
-s --share_file	targeted network drive path
- n --encryption_percent	percentage of encryption
--fork	create a child process for encryption

```
.4dd, .accdb, .accdc, .accde, .accdr, .accdt, .accft, .adb, .ade, .adf, .adp, .ar
c, .ora, .alf, .ask, .btr, .bdf, .cat, .cdb, .ckp, .cma, .cpd, .dacpac, .dad, .dad
iagrams, .daschema, .db-shm, .db-wa, .db3, .dbc, .dbf, .dbs, .dbt, .dbv, .dbx, .dc
b, .dct, .dcx, .dlis, .dp1, .dqy, .dsk, .dsn, .dtsx, .eco, .ecx, .edb, .epim, .ex
b, .fcd, .fdb, .fic, .fmp, .fmp12, .fmps, .fp3, .fp4, .fp5, .fp7, .fpt, .frm, .gd
b, .grdb, .gwi, .hdb, .his, .idb, .ihx, .itdb, .itw, .jet, .jtx, .kdb, .kexi, .kex
ic, .kexis, .lgc, .lwx, .maf, .maq, .mar, .mas, .mav, .mdb, .mdf, .mpd, .mrg, .mu
d, .mwb, .myd, .ndf, .nnt, .nrmlib, .ns2, .ns3, .ns4, .nsf, .nv2, .nwdb, .nyf, .od
b, .oqy, .orx, .owc, .p96, .p97, .pan, .pdb, .pdm, .pnz, .qry, .qvd, .rbf, .rctd,
.rod, .rodx, .rpd, .rsd, .sas7bdat, .sbf, .scx, .sdb, .sdc, .sdf, .sis, .spq, .sql
ite, .sqlite3, .sqlitedb, .temx, .tmd, .tps, .trc, .trm, .udb, .usr, .v12, .vis, .
vpd, .vvv, .wdb, .wmdb, .wrk, .xdb, .xld, .xmlff, .abcddb, .abs, .abx, .accdw, .ad
n, .db2, .fm5, .hjt, .icg, .icr, .lut, .maw, .mdn, .mdt, .vdi, .vhd, .vmdk, .pvm,
.vmem, .vmsn, .vmsd, .nvram, .vmx, .raw, .qcow2, .subvo, .bin, .vsv, .avhd, .vmrs,
.vhdx, .avdx, .vmcx, .iso
```

Linux file extensions targeted by Akira *(Source: Bleeping Computer)*

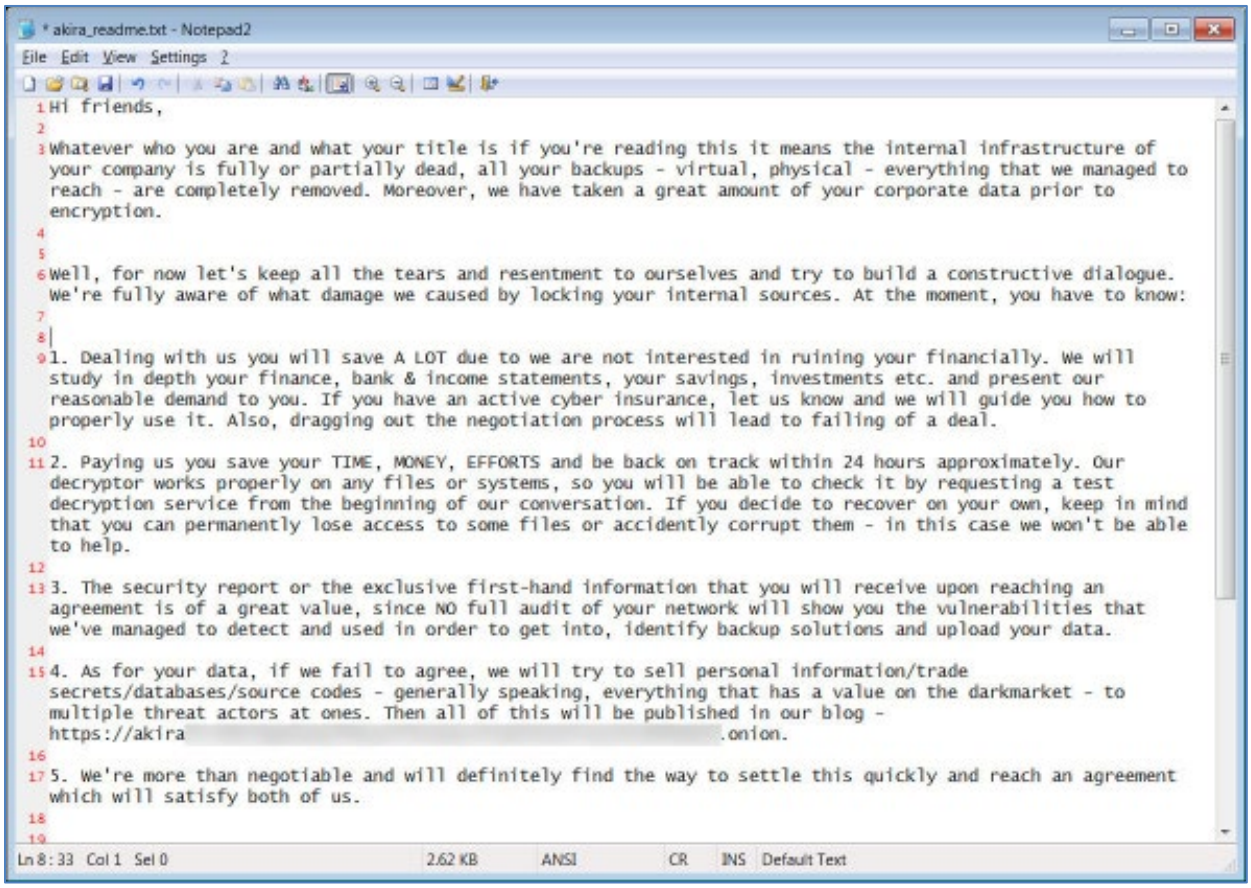
Akira has obtained many of its initial compromises by leveraging compromised credentials. Additionally, many of the targeted organizations did not have multi-factor authentication (MFA) enabled on their virtual private networks (VPN). It is unknown how the credentials were originally obtained, but it is possible that they were purchased from the dark web. Additional distribution methods have included phishing emails, malicious websites, drive-by download attacks, and trojans. Once infected, the malware will launch PowerShell to remove shadow volume copies, and once encryption is complete, the file's extension will be reassigned with the ".akira" extension. The attackers also attempt lateral movement and privilege escalation through LSASS credential dumps.

Before encryption, the ransomware group exfiltrates the victim's data to employ the double-extortion tactic on their victims. If the ransom is not paid, the group threatens to release the sensitive information to the public. The group also offers victims a lower-cost option to not pay for a decryptor and to not have the especially sensitive information published.

HC3: Sector Alert

September 12, 2023 TLP:CLEAR Report: 202309121400

While the ransom note is written in English, it contains several grammatical errors within it. The note instructs the victims to contact them via their TOR site, where each victim is given a unique login password for conducting negotiations. The ransom note also offers organizations a full security report from Akira, which claims to release an audit of the victims network and the vulnerabilities that the group was able to exploit.



Akira ransom note *(Source: Bleeping Computer)*

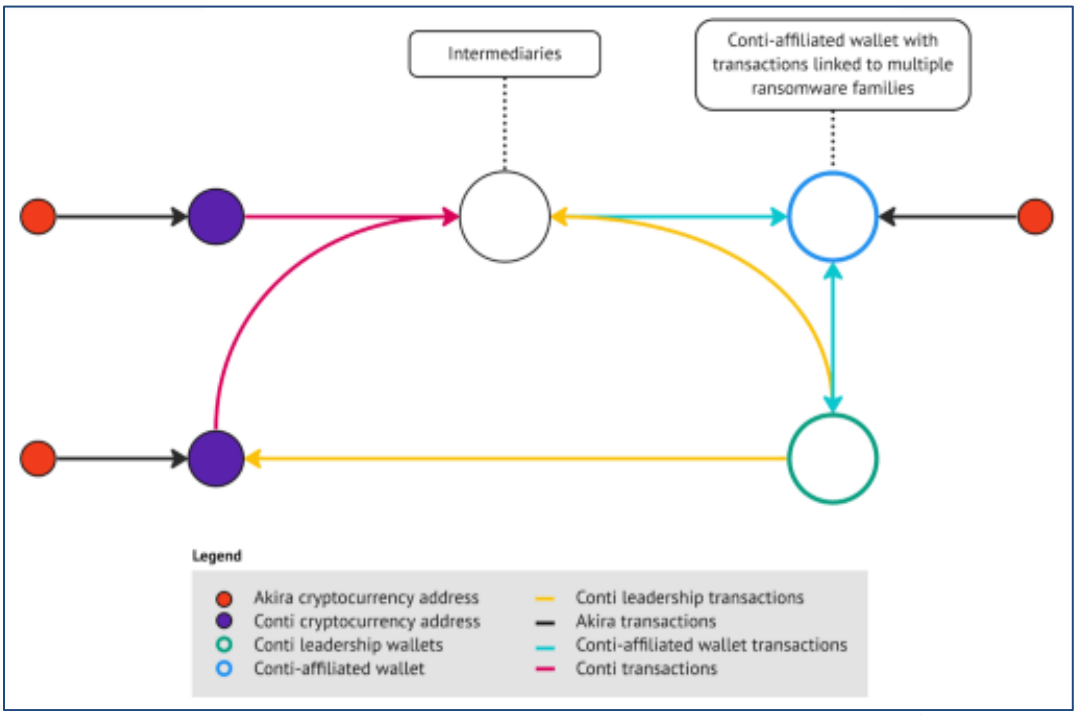
The group utilizes a range of tools during the course of the incident, as indicated from incident response data. Some of these include the PCHunter toolkit, port scanner MASSCAN, Mimikatz for credential harvesting, WinSCP, and PsExec to name a few.

Affiliation With Other Groups

Security researchers have noticed that the Akira ransomware has some similarities with the disbanded Conti ransomware group. This was a result of some identified code overlap and the implementation of ChaCha 2008, as well as the code for key generation, both of which resemble the one used by Conti. The list directory exclusions that it avoids encrypting, including winnt and Trend Micro, are also the same in both ransomware strains.

In a pattern analysis of cryptocurrency wallets, researchers were able to identify overlap in the wallets between Akira and Conti. In two of these transactions, the wallets had previously been affiliated with

Conti's leadership team.



Blockchain transactions between Akira and Conti *(Source: Artic Wolf)*

Indicators of Compromise

Avast's Indicators of Compromise
Windows Version
5c62626731856fb5e669473b39ac3deb0052b32981863f8cf697ae01c80512e5
3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c
678ec8734367c7547794a604cc65e74a0f42320d85a6dce20c214e3b4536bb33
7b295a10d54c870d59fab3a83a8b983282f6250a0be9df581334eb93d53f3488
8631ac37f605daacf47095955837ec5abbd5e98c540ffd58bb9bf873b1685a50
1b6af2fbbc636180dd7bae825486ccc45e42aefbb304d5f83fafca4d637c13cc
9ca333b2e88ab35f608e447b0e3b821a6e04c4b0c76545177890fb16adcab163
d0510e1d89640c9650782e882fe3b9afba00303b126ec38fdc5f1c1484341959
6cadab96185dbe6f3a7b95cf2f97d6ac395785607baa6ed7bf363deeb59cc360

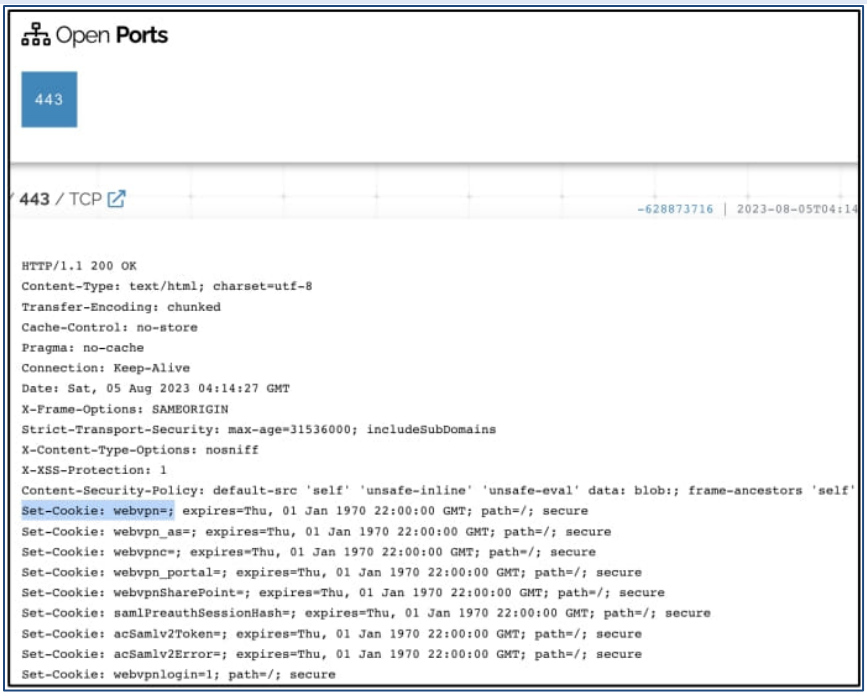
Avast's Indicator of Compromise
Linux Version
1d3b5c650533d13c81e325972a912e3ff8776e36e18bca966dae50735f8ab296

Recent Reporting

On August 22, 2023, reports have shown that Akira has started to target Cisco VPN products to gain access to corporate networks, reportedly on those that do not have MFA enabled.

HC3: Sector Alert

September 12, 2023 TLP:CLEAR Report: 202309121400



Cisco VPN trait seen in eight Akira attacks *(Source: Bleeping Computer)*

Researchers from SentinelOne have also observed newer tactics, techniques, and procedures (TTPs) from the ransomware gang, such as SQL database manipulation, disabling firewalls, and disabling LSA protection. Additionally, the group has used RustDesk, a legitimate remote access tool. Since RustDesk is a legitimate tool, it is less likely to trigger any alarms for defenders, all while allowing attackers to maintain remote access.

Mitigations

The Akira ransomware has been delivered through several methods, and HC3 encourages the following mitigations to help protect your organization:

- Implement a strong password policy
- Educate and train users
- Enable multi-factor authentication
- Update and patch systems regularly
- Implementing account lockout policies to defend against brute force attacks
- Implementing a recovery and incident response plan
- Implement network segmentation

References

Abrams, Lawrence. “Meet Akira — A new ransomware operation targeting the enterprise”. Bleeping Computer. May 7, 2023. https://www.bleepingcomputer.com/news/security/meet-akira-a-new-ransomware-operation-targeting-the-enterprise/

Antoniuk, Daryna. “Akira ransomware compromised at least 63 victims since March, report says”. July 26,

2023. The Record. https://therecord.media/akira-ransomware-early-victims-conti-links

“Akira Ransomware: In-Depth Analysis, Detection, and Mitigation”. SentielOne. https://www.sentinelone.com/anthology/akira/

“Akira ransomware targets Linux”. Devel. July 4, 2023. https://devel.group/blog/akira-ransomware-targets-linux/#:~:text=Recent%20research%20reveals%20that%20the,actively%20targeting%20multiple%20organizations%20worldwide.

Cluley, Graham. “Akira ransomware - what you need to know”. Tripwire. May 11, 2023. https://www.tripwire.com/state-of-security/akira-ransomware-what-you-need-know

Belfiore, Connor. Campbell, Steven. Suthar, Akshay. “Conti and Akira: Chained Together”. Artice Wolf. July 26, 2023. https://arcticwolf.com/resources/blog/conti-and-akira-chained-together/

“Decrypted: Akira Ransomware”. Avast. Threat Research Team. June 29, 2023. https://decoded.avast.io/threatresearch/decrypted-akira-ransomware/

Toulas, Bill. “Akira ransomware targets Cisco VPNs to breach organizations”. Bleeping Computer. August 22, 2023. https://www.bleepingcomputer.com/news/security/akira-ransomware-targets-cisco-vpns-to-breach-organizations/

Toulas, Bill. “Linux version of Akira ransomware targets VMware ESXi servers”. Bleeping Computer. June 28, 2023. https://www.bleepingcomputer.com/news/security/linux-version-of-akira-ransomware-targets-vmware-esxi-servers/

Walter, Jim. “From Conti to Akira | Decoding the Latest Linux & ESXi Ransomware Families”. August 23, 2023. SentielOne. https://www.sentinelone.com/blog/from-conti-to-akira-decoding-the-latest-linux-esxi-ransomware-families/

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