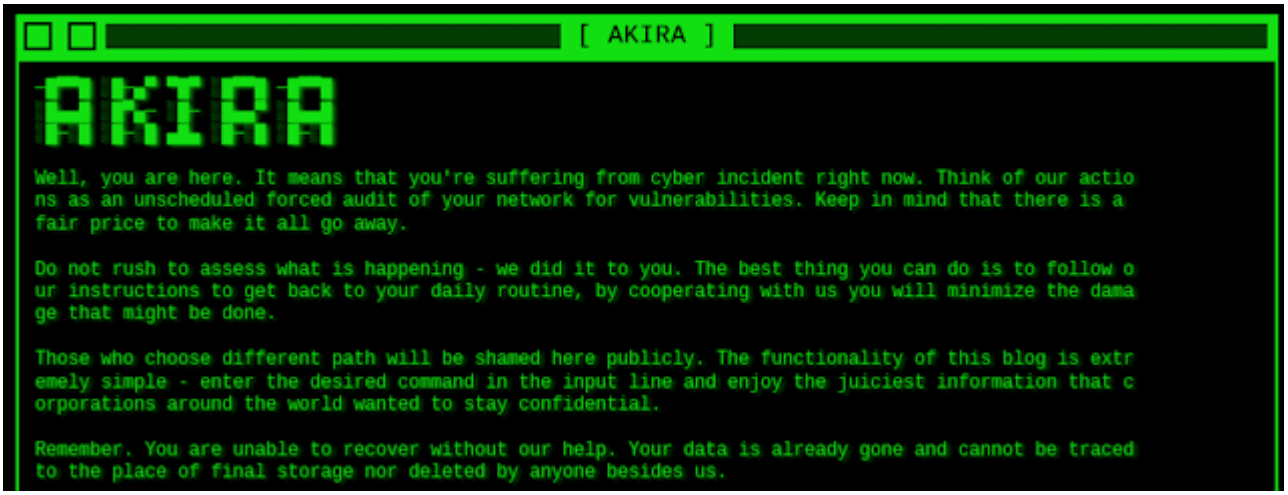
Tracking Adversaries: Akira, another descendent of Conti

By BushidoToken

Published: 2023-09-16 · Archived: 2026-04-05 23:02:30 UTC



The dozens of cybercriminals that made up the Conti group continue to launch campaigns unabated. Previously in 2022, I blogged about how following the Conti Leaks, the operators of Conti continued on via multiple rebranded ransomware campaigns, such as Royal, BlackBasta, and Quantum, among others.

Since my last two blogs on the Conti/TrickBot gang, multiple members have been officially sanctioned by the US and UK government in February 2023 and September 2023, formally confirming attribution to Russia-based threat actors. The sanctions are a vital step in the right direction and helps the public and law makers understand what organized cybercrime looks like and the scale of the fight on our hands.

In this blog, however, I wanted to explore the ransomware campaign called Akira that appeared in March 2023 and focus on how Akira is connected to Conti. Akira is a rapidly growing threat to civil society and critical infrastructure and is the ransomware group I believe researchers and governments should be monitoring more closely.

Background on Akira

Adversaries and Victims

Firstly, the operators of Akira ransomware are financially motivated cybercriminals. They are in it for the money and have made a lot of it already in 2023, how much exactly is not clear. But public media reports state that between March and July 2023, the group has compromised at least 63 victims, which is around four organizations hit by Akira ransomware per week — that we know about. From negotiations seen by BleepingComputer, the ransomware gang demands ransoms ranging from 200,000 to millions of US dollars.

The group performs the usual double extortion campaigns, whereby the victim's files are encrypted and information is stolen and published to their Tor data leak site (DLS) if the ransom is not paid. Private cybersecurity vendors track the Akira operators as Punk Spider (CrowdStrike) and Gold Sahara (Secureworks).

Alongside being connected to Conti, the Akira operators are likely affiliated with other ransomware operations too, including Snatch and BlackByte. In an August 2023, researchers found an open directory of tools used by an Akira operator that were also likely being used by a threat actor with connections to Snatch ransomware. In July 2023, media reports shared that Yamaha's Canadian music division was listed on the Akira DLS, which was after they were listed on BlackByte's DLS in June 2023. The connections between Akira and other ransomware gangs highlight that those who deploy Akira are potentially working with more than one ransomware crew, as Microsoft found is usually the case among affiliates.

Akira's victims have been located around the world, but most that have appeared on their Tor DLS have been from North America. Akira attacks have impacted a wide range of industries, such as education, financial services, manufacturing, professional services, and healthcare, among others. Most of the victims have been small-to-medium businesses (SMBs) with a few recognizable brand names, such as Yamaha.

Capabilities and Infrastructure

There have been multiple versions of the Akira ransomware family and it has been deployed across Windows domains and Hyper-V virtual infrastructure, as well as VMware ESXi hypervisors with Linux virtual machines (VMs). The first version of Akira was written in C++ and appended files with the ".akira" extension and dropped a ransom note called "akira_readme.txt" that is at least partially based on Conti's V2 source code, according to malware analysts who also released a decryptor for Akira on 29 June 2023. However, a new version was shortly released that patched the decryption flaw on 2 July 2023. Since then, in late August 2023, a new revamped version of Akira appeared developed in Rust. This time it was called "megazord.exe" and appended ".powerranges" extension to encrypted files.

The most common initial access vector the Akira operators have used appears to be via brute-forcing Cisco VPN devices with single-factor authentication only. The Akira operator that was tied to Snatch was also found exploiting Fortinet devices vulnerable to CVE-2019-6693 and CVE-2022-40684 for initial access. Incident responders have also said that they believe Akira operators likely purchase VPN credentials from cybercrime marketplaces fuelled by infostealer malware botnets and they may potentially source them from initial access brokers (IABs) too, such as EXOTIC LILY that controls the Bumblebee malware.

By extracting tools and tradecraft from numerous threat reports on Akira, the operators have been known to leverage the same arsenal of tools time and time again, but may substitute some depending on the environment. These can be broken down into the following categories:

- **External Reconnaissance:** Masscan and ReconFTW
- **Internal Enumeration:** PCHunter64, Advanced IP Scanner, LANsweeper, SharpHound, AdFind, SoftPerfect NetScan, and Windows Nltest
- **Credential Theft:** Minidump, Mimikatz, LaZagne, and DonPAPI

- **Persistence:** RMM tools, such as AnyDesk, RustDesk, Radmin, and ScreenConnect, as well as disabling firewalls followed by enabling RDP, and PuTTy. The SystemBC crimeware RAT has also been used Akira.
- **Defense Evasion:** Disable EDR tools with Terminator.exe and ToolPow, as well as batch scripts for disabling LSA Protection and Windows Defender
- **Lateral Movement:** Impacket (wmiexec.py and atexec.py), RDP, and SSH
- **Collection:** Searching and downloading files from Microsoft SharePoint
- **Exfiltration:** Compression tools (7zip, WinRAR, etc) as well as Rclone, FileZilla, and WinSCP
- **Command-and-control:** Cloudflare Tunnel (Cloudflared), MobaXterm, and Ngrok
- **Impact:** Akira ransomware, usually launched via PsExec

After the ransomware has been deployed and the data is stolen, Akira begins the negotiations. This includes requesting the victim to visit Akira's Green MS-DOS style Tor Negotiation site (akiralkzxzq2dsrzsrvbr2xgbbu2wgsmxryd4csgfameg52n7efvr2id[.]onion) via the ransom note. And if the victim refuses to pay the ransom, they are listed on Akira's DLS (akiral2iz6a7qgd3ayp3l6yub7xx2 uep76idk3u2kollpj5z3z636bad[.]onion).

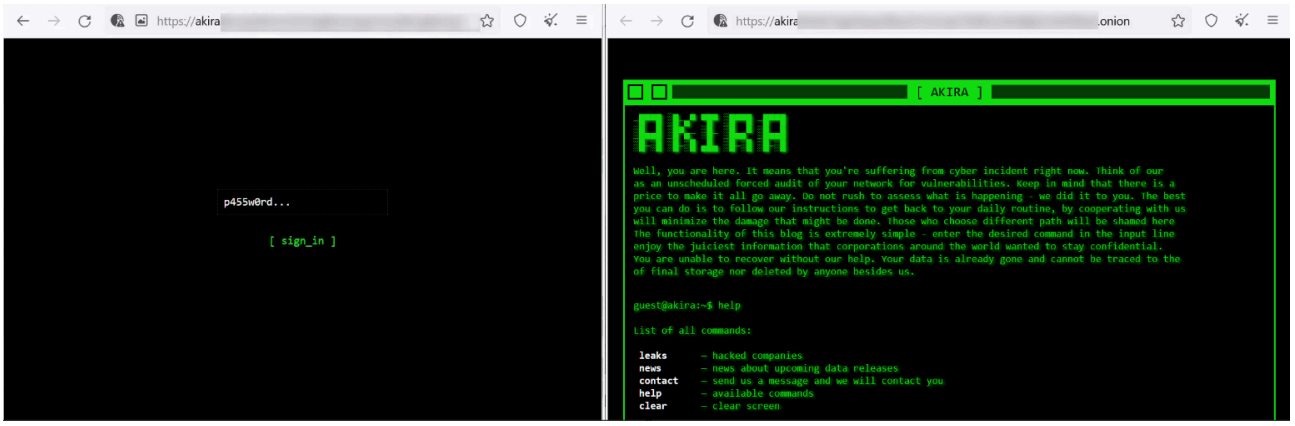


Figure 1: Akira's Negotiation Portal (left) and Data Leak Site (right)

Finally, something to note about Akira's DLS is that it does not actually host the stolen data like other ransomware Tor DLSs. This gang has decided to use Magnet Links that require Torrenting software to download and view stolen data. This is a trend that other ransomware groups have followed, such as CL0P following the MOVEit breaches earlier in 2023.

Figure 2: Victim post on Akira's DLS with Magnet Links

Akira's similarities with Conti

Now, let’s lay all the evidence out and examine the similarities and overlaps between Conti and Akira. The main notable links are as follows:

- To start, both Conti and Akira are double extortion ransomware groups and Akira appeared almost a year after Conti shut down its Tor DLS. Many of Akira’s victims are the same type as Conti’s, those being primarily North American businesses. Plus, much like Conti, there are versions of Akira ransomware that can target Windows domains or VMware ESXi hypervisors with Linux VMs.
- Malware analysts have noted several code similarities between Conti and Akira ransomware, such as the list of file type and directory exclusions, the structure of the file tail, the implementation of ChaCha 2008, and the code for key generation.
- Examples of negotiation chats between Akira and their victims have also been made public. These logs revealed that Akira operators use a script to begin negotiations just as Conti did, demonstrating behavioral similarity in campaign style and how they conduct operations.
- In August 2021, a disgruntled member of Conti leaked the gang’s playbook for launching templated attacks. Conti created this playbook to scale up operations and launch ransomware attacks more frequently, earning them more money. Akira campaigns have followed a very similar set of TTPs as the Conti playbook. The following tools used by Akira operators that are also mentioned in the Conti playbook include: Minidump, Mimikatz, AdFind, PChunter, PsExec, NetScan, Windows nltest, PuTTy, WinSCP, FileZilla, and AnyDesk.
- Malware that leads to Akira has also been commonly leveraged by Conti/Ryuk operators. The SystemBC crimeware RAT has been used by Conti and Ryuk operators. Microsoft also highlighted that it a specific operator they track as DEV-0237 shifted to SystemBC from Cobalt Strike during Conti campaigns. The Bumblebee loader and EXOTIC LILY that have reportedly provided access to Akira operators are also closely associated with Conti campaigns.

- Blockchain analytics on Akira's Bitcoin transactions by incident responders also revealed that on at least three occasions, Akira operators have sent ransom funds to addresses affiliated with known Conti wallets. These transactions also equalled more than 600,000 USD.

Based on the evidence gathered about Akira, it is my assessment that the operators behind Akira ransomware are linked to Conti with high confidence. The are numerous links at multiple levels, with a combination of technical and behavioral ties between the two groups.

One of the most telling connections is arguably the bitcoin transactions between Akira and known Conti wallets. The lack of any serious blockchain obfuscation techniques, such as using a mixing service or chain hopping, has made it trivial for investigators trace Akira ransom payments ultimately back to Conti with high confidence.

Even without these Bitcoin transactions as damning evidence, there are clear similarities between Akira and Conti TTPs. However, due to the Conti ransomware source code getting leaked as well as the playbook getting leaked, it is possible for some threat actors to imitate Conti's success. But the fact Akira is sending funds back to Conti, does make it seem they are almost certainly working with former Conti members (who are sanctioned).

Conclusion

If you are a victim of Akira and you are considering paying the ransom, you are potentially dealing with the sanctioned Russian men mentioned at the start of this blog. Paying the ransom is funding the Russia-based organized cybercrime syndicates that threaten our civil society and critical infrastructure. Think about that next time a hospital is ransomed. Company executives at victim organizations need to realize that paying a sanctioned Russia-based cybercriminal group for a decryption key is hardly different from terrorist financing.
