Conti and Akira: Chained Together

arcticwolf.com/resources/blog/conti-and-akira-chained-together/

by Steven Campbell, Akshay Suthar, Connor Belfiore, and Arctic Wolf Labs Team July 26, 2023

Key Takeaways

- Since March 2023, Akira ransomware has compromised at least 63 victims with approximately 80% of them being small to medium-sized businesses (SMBs).
- We assess Akira is likely an opportunistic ransomware group due to their victimology and negotiation tactics.
- Through blockchain analysis, we assess with a high degree of confidence that some Conti-affiliated threat actors are linked to the Akira ransomware group.

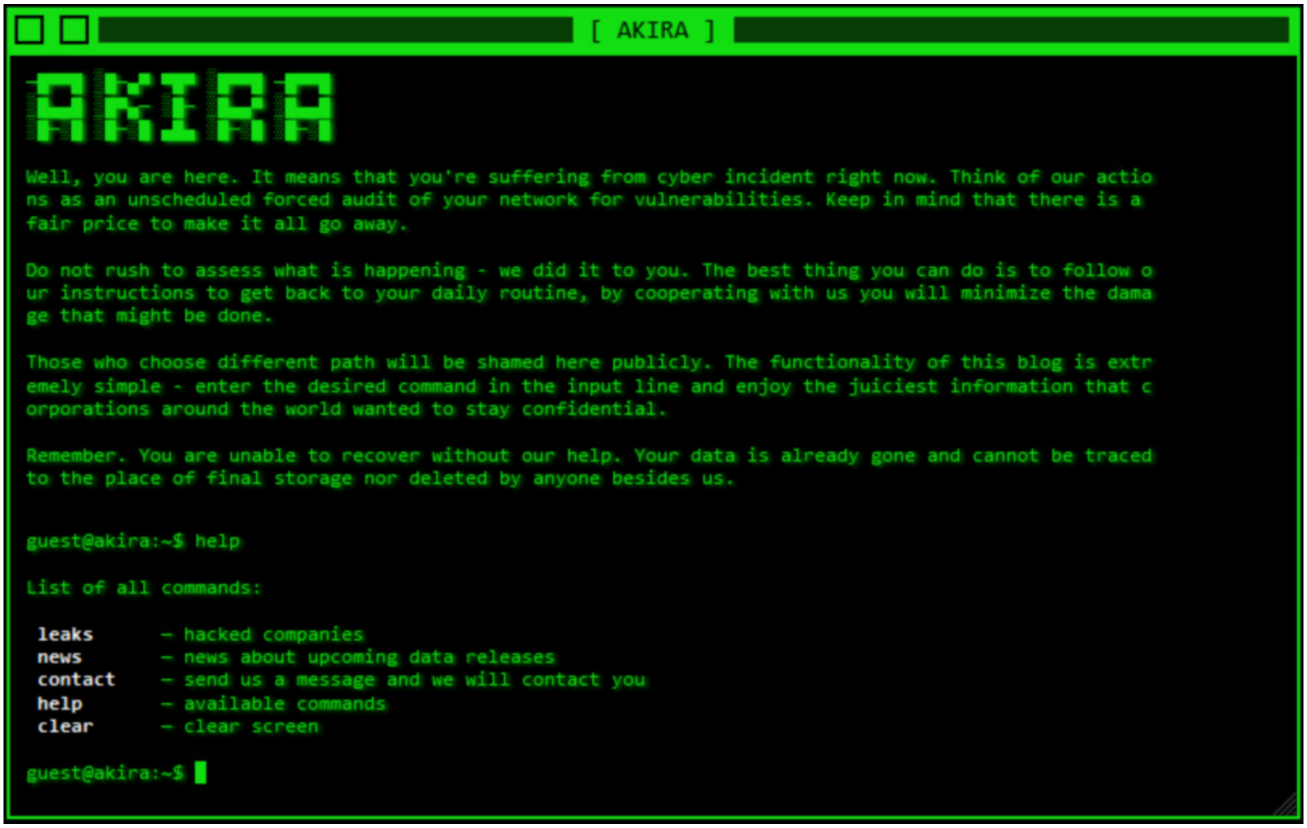
Background

Since the fallout of Conti ransomware in mid-2022, Conti-affiliated threat actors have splintered off and developed or joined other ransomware groups to continue extorting victim organizations. Due to Conti's source code being leaked, attribution back to the Conti ransomware group via code overlap is much more difficult. However, leveraging blockchain analysis, we can begin to discern what ransomware groups Conti-affiliated threat actors have worked with; one such group is Akira.

Who is Akira?

Akira is a relatively new, fast-growing ransomware group—first observed in March 2023—that leverages the ransomware-as-a-service (RaaS) business model to deploy Akira ransomware. Similar to other prominent RaaS groups, Akira exfiltrates data before encrypting victim devices and leverages it to perform double extortion. The group does not insist on a company paying for both decryption assistance and the deletion of data. Instead, Akira offers victims the opportunity to pick and choose what they would like to pay for. However, if a victim does not pay the ransom (ranging from $200K USD to over $4M USD based on Arctic Wolf® Incident Response's insights) the victim's name and data are published to Akira's leak site.

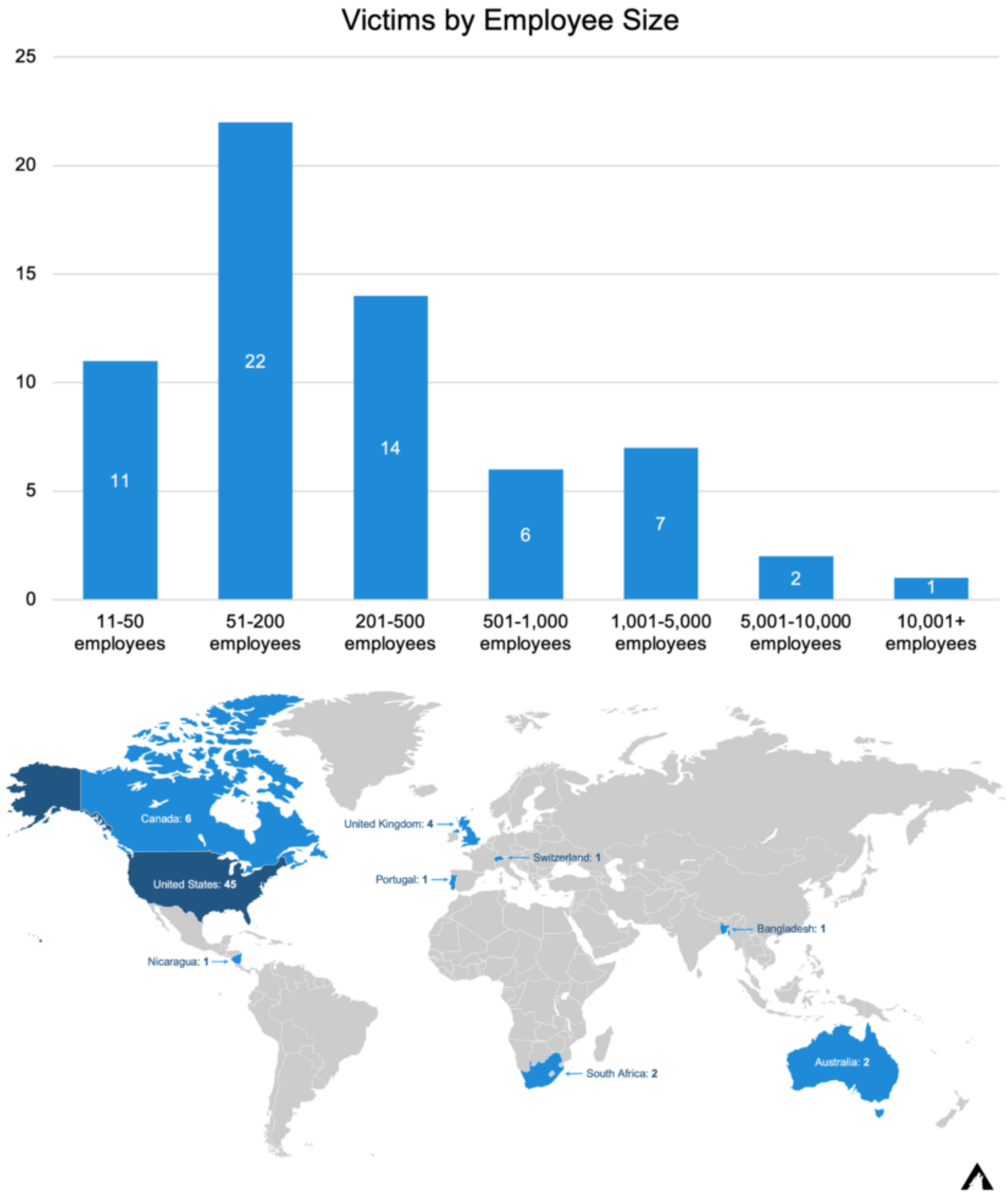
Note: In 2017, security researchers identified a ransomware variant that appended an identical file extension (.akira) to encrypted files; however, this variant is not related to the Akira ransomware group.



```
Well, you are here. It means that you're suffering from cyber incident right now. Think of our actio
ns as an unscheduled forced audit of your network for vulnerabilities. Keep in mind that there is a
fair price to make it all go away.

Do not rush to assess what is happening - we did it to you. The best thing you can do is to follow o
ur instructions to get back to your daily routine, by cooperating with us you will minimize the dama
ge that might be done.

Those who choose different path will be shamed here publicly. The functionality of this blog is extr
emely simple - enter the desired command in the input line and enjoy the juiciest information that c
orporations around the world wanted to stay confidential.

Remember. You are unable to recover without our help. Your data is already gone and cannot be traced
to the place of final storage nor deleted by anyone besides us.


guest@akira:~$ help

List of all commands:

 leaks      - hacked companies
 news       - news about upcoming data releases
 contact    - send us a message and we will contact you
 help       - available commands
 clear      - clear screen

guest@akira:~$ █
```

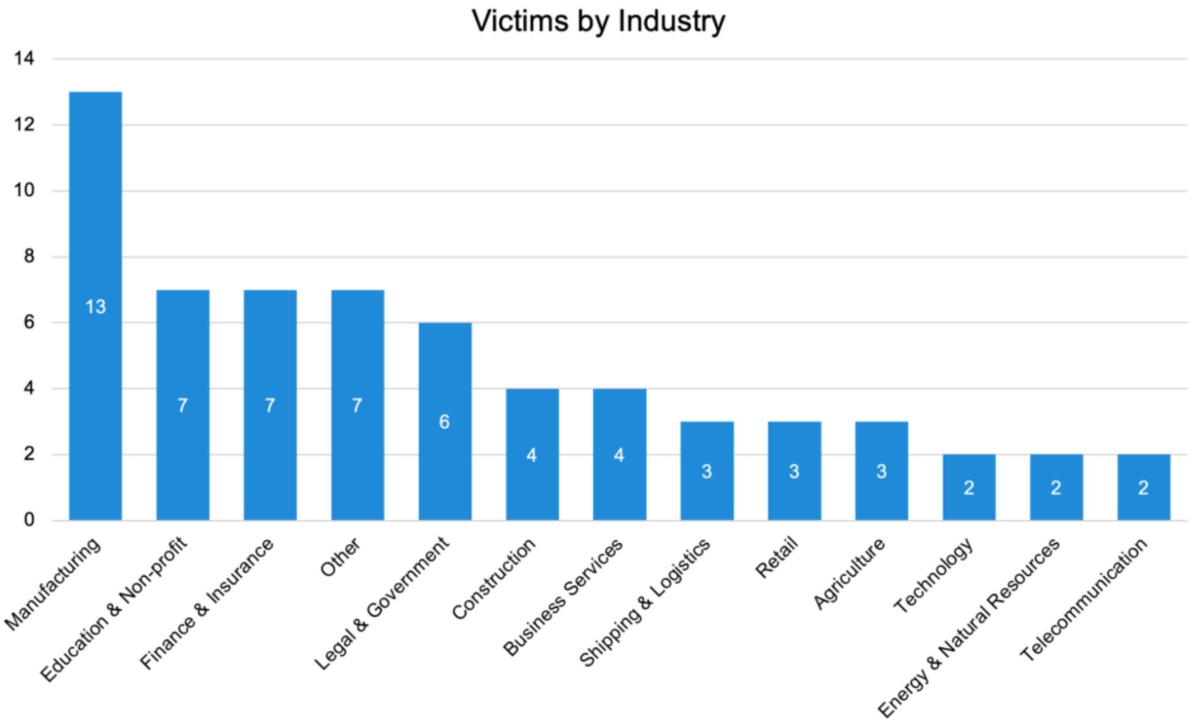
Akira Tor Leak Site

According to Akira’s leak site, the group has compromised at least 63 organizations since their inception, with approximately 80% of their victims being small to medium-sized businesses (SMBs). Notably, some of the victims have been removed from the leak site.



Victims by Employee Size and Location

We assess that Akira is likely an opportunistic ransomware group due to their victimology and negotiation tactics. In nearly every incident response case Arctic Wolf investigated, the threat actors claimed that they needed time to review the exfiltrated data to determine a ransom demand.



Victims by Industry

Tools

The Arctic Wolf Incident Response team has responded to multiple Akira ransomware intrusions since April 2023. In nearly all intrusions, the threat actors leveraged compromised credentials to obtain initial access to the victim's environment. Notably, the majority of victim organizations did not have multi-factor authentication (MFA) enabled on their VPNs. It is unclear how the threat actors obtained the compromised credentials; however, it is plausible the threat actors purchased access or credentials on the dark web.

Based on Arctic Wolf Incident Response data, Akira leverages a multitude of tools upon obtaining initial access to a victim's environment. Known tools are listed below:

Tools Leveraged by Akira Affiliates

Tactic	Tool
Discovery	
PCHunter	
Advanced IP Scanner	
AdFind	
SharpHound	

MASSCAN	
Credential Access	
Mimikatz	
LaZagne	
Command and Control	
AnyDesk	
Radmin	
Cloudflare Tunnel	
MobaXterm	
Ngrok	
Exfiltration	
WinRAR	
WinSCP	
Rclone	
FileZilla	
Impact	PsExec

Code Overlap and Similarities with Conti

Identifying code overlap between different ransomware variants typically allows analysts to attribute activity back to a specific group due to ransomware source code being tightly guarded by threat actors. However, with the Conti source code leak, multiple threat actors leveraged the code to develop or modify their own code base making attribution back to Conti threat actors much more difficult.

Although both ransomware variants differ, Akira ransomware does bear some semblance to Conti ransomware. Akira ignores the same file types and directories as Conti ransomware and has functions that are similar. Akira also used the ChaCha algorithm to encrypt files, which was implemented similarly to the one used by Conti ransomware.

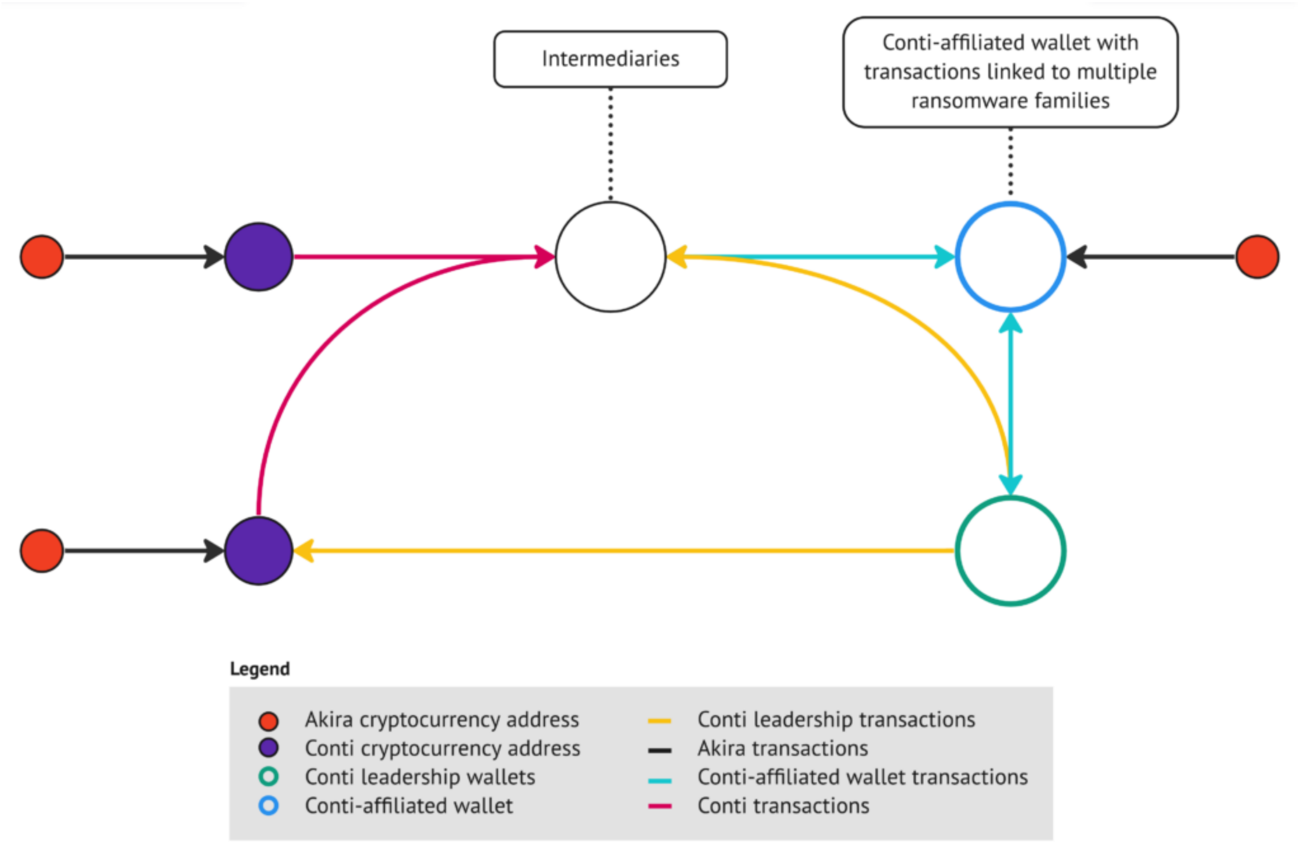
On June 29, 2023, however, Avast released a decryptor for Akira ransomware that victim organizations can use to decrypt files. Based on current intelligence, the threat actors have modified the encryption routine since the decryptor was published, indicating that it may not work if files were encrypted after June 29th.

Blockchain Analysis – Chained Together

Although cryptocurrency can be acquired without attribution back to the buyer, it is not completely anonymous. Transactions between cryptocurrency wallets are published to the blockchain ledger which is publicly viewable via a blockchain explorer.

By leveraging known threat actor cryptocurrency wallet addresses, we are able to conduct pattern analysis of the transactions and discover additional wallet addresses. In some instances, we have observed cryptocurrency address reuse between threat groups, indicating the individual controlling the address or wallet has either splintered off from the original group or is working with another group at the same time.

Based on blockchain analysis of known Akira ransomware transactions, Arctic Wolf® Labs identified overlaps between Akira and Conti threat actors on multiple occasions.


Intermediaries
Conti-affiliated wallet with transactions linked to multiple ransomware families
Legend
● Akira cryptocurrency address
● Conti cryptocurrency address
○ Conti leadership wallets
○ Conti-affiliated wallet
— Conti leadership transactions
— Akira transactions
— Conti-affiliated wallet transactions
— Conti transactions

Blockchain Transactions Between Akira and Conti Ransomware

In at least three separate transactions, Akira threat actors sent the full amount of their ransom payment to Conti-affiliated addresses; the three transactions totaled over $600K USD. From there, we observed all the Conti-affiliated addresses conduct transactions with a group of shared intermediary wallets that were used to cash out funds from the ransom payments or transfer funds within the group. Notably, two of the Conti-affiliated wallets had transactions with wallets linked to Conti's leadership team, with one housing addresses used to receive ransom payments for multiple ransomware families.

Conclusion

By following transactions discovered during blockchain analysis, we can tie individual groups together with higher fidelity based on transactions to and from known threat actor-controlled cryptocurrency addresses. Tracking ransom payments to Akira allowed Arctic Wolf Labs to identify transactions to Conti-affiliated addresses. The same analysis method allowed our team to identify connections between the Karakurt extortion group, Diavol, and the Conti ransomware group in 2022.

Although Conti disbanded after increased pressure due to internal conflict and the publishing of their source code, many of the Conti members have continued to wreak havoc on organizations in 2023 through their activity with other ransomware-as-a-service groups, including Akira. Akira continues to evolve and grow as a ransomware group by changing its tactics to evade detection. Security best practices, such as enabling MFA on VPN appliances, can greatly hinder Akira's ability to successfully compromise an organization.

References

Authors

Steven Campbell – Senior Threat Intelligence Researcher

Steven Campbell is a Senior Threat Intelligence Researcher at Arctic Wolf Labs and has more than eight years of experience in intelligence analysis and security research. He has a strong background in infrastructure analysis and adversary tradecraft.

Akshay Suthar – Senior Threat Intelligence Researcher

Akshay Suthar is a Senior Threat Intelligence Researcher at Arctic Wolf Labs focused on researching adversary tradecraft and malware analysis. He has more than seven years of experience in a multitude of domains including threat intelligence research, detection engineering, and intrusion analysis.

Connor Belfiore – Threat Intelligence Analyst

Connor Belfiore is a Threat Intelligence Analyst at Arctic Wolf Incident Response. He has more than five years of experience in threat intelligence, financial crimes investigation, and blockchain analysis.