Follow-On Extortion Campaign Targeting Victims of Akira and Royal Ransomware

arcticwolf.com/resources/blog/follow-on-extortion-campaign-targeting-victims-of-akira-and-royal-ransomware/

by Stefan Hostetler, Steven Campbell

January 4, 2024

Key Takeaways

- Arctic Wolf Labs has investigated several cases of Royal and Akira ransomware victims being targeted in follow-on extortion attacks starting in October 2023.
- It is not clear whether these follow-on extortion attempts were officially sanctioned by the groups responsible for the original ransomware attacks, given the low payment demands, in addition to other unique campaign elements.
- Based on our analysis of common elements between these cases, Arctic Wolf Labs assesses with moderate confidence that a common threat actor was responsible for these follow-on extortion attempts.

Summary

Arctic Wolf Labs is aware of several instances of ransomware cases where the victim organizations were contacted after the original compromise for additional extortion attempts. In two cases investigated by Arctic Wolf Labs, threat actors spun a narrative of trying to help victim organizations, offering to hack into the server infrastructure of the original ransomware groups involved to delete exfiltrated data.

As far as Arctic Wolf Labs is aware, this is the first published instance of a threat actor posing as a legitimate security researcher offering to delete hacked data from a separate ransomware group. While the personalities involved in these secondary extortion attempts were presented as separate entities, we assess with moderate confidence that the extortion attempts were likely perpetrated by the same threat actor.

What We Know

Case 1: Royal Ransomware Compromise and Ethical Side Group Data Deletion Extortion

In early October 2023, an entity describing themselves as Ethical Side Group (ESG) contacted a Royal ransomware victim by email and claimed to have obtained access to victim data originally exfiltrated by Royal. Notably, in prior negotiations in 2022, Royal claimed to have deleted the data.

Interestingly, in their initial communications, ESG had falsely attributed the original compromise to the TommyLeaks ransomware group instead of Royal ransomware.

ESG ultimately offered to hack into Royal ransomware's server infrastructure and permanently delete the targeted organization's data for a fee.

Case 2: Akira Ransomware Compromise and xanonymoux Data Deletion Extortion

In early November 2023, an entity describing themselves as xanonymoux contacted an Akira ransomware encryption victim and claimed to have obtained access to a server hosting victim data exfiltrated by Akira. Notably, when Akira was contacted a few weeks before xanonymoux's email, the group claimed not to have exfiltrated any data and that they had only encrypted systems.

xanonymoux claimed to have compromised Akira's server infrastructure. The threat actor offered to aide in either deleting the victim's data or providing them with access to their server. Additionally, xanonymoux claimed that Akira was associated with Karakurt, a criminal group known for data exfiltration and extortion.

Case Comparison and Analysis

As described in these cases, similar elements were observed between both campaigns, despite presenting as separate entities and relating to different named ransomware groups. Stylistic analysis of the communications between both organizations identified clear similarities between the two cases.

Common Threat Actor Behaviors Between Follow-On Extortion Cases
Presented as a security researcher
Claimed to access server infrastructure hosting data from past compromise
Communicated via Tox
Offered to provide proof of access to exfiltrated data
Insinuated risk of future attacks if security issues are not addressed
Specified amount of data previously exfiltrated

Minimal payment demand (<= 5BTC)
10 overlapping phrases used in initial email
Use of file.io to provide evidence of access to victim data

The elements of the campaigns described here are unique in their low ransom demands, posing as a legitimate security researcher as a pretext, and offers to delete data to avoid potential future attacks. However, follow-on extortion as a concept is not new to attacks associated with Conti and Karakurt. In 2021, we published research revealing Karakurt re-extortion attempts for victims that had previously been targeted in ransomware attacks by Conti. Additionally, our past research has also identified connections between Conti and Akira. Royal emerged on the ransomware scene in 2022, and connections have been noted by other researchers, such as Will Bushido, between Royal and Conti.

Conclusion

It is challenging to make sense of the tangled web of connections woven by ransomware groups, given that ransomware-as-a-service (RaaS) affiliates tend to operate multiple encryption payloads over time, sometimes even deploying several at once. The best we can do as researchers is to piece together parts of the bigger picture by looking for common denominators between attacks.

Based on the common elements identified between the cases documented here, we conclude with moderate confidence that a common threat actor has attempted to extort organizations who were previously victims of Royal and Akira ransomware attacks with follow-on efforts. However, it is still unclear whether the follow-on extortion cases were sanctioned by the initial ransomware groups, or whether the threat actor acted alone to garner additional funds from the victim organizations.

This research highlights the risks of relying on criminal extortion enterprises to delete exfiltrated data, even after payment.

If your organization has a presence in the U.S., and you’ve been affected by any of these types of attacks, please contact your nearest FBI field office.

References

- https://arcticwolf.com/resources/blog/conti-and-akira-chained-together/
- https://blog.bushidotoken.net/2022/11/the-continuity-of-conti.html
- https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

By Stefan Hostetler, Steven Campbell

Stefan Hostetler | Senior Threat Intelligence Researcher

Stefan is a Senior Threat Intelligence Researcher at Arctic Wolf. With over a decade of industry experience under his belt, he focuses on extracting actionable insight from novel threats to help organizations protect themselves effectively.

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.

About Arctic Wolf Labs

Arctic Wolf Labs is a group of elite security researchers, data scientists, and security development engineers who explore security topics to deliver cutting-edge threat research on new and emerging adversaries, develop and refine advanced threat detection models with artificial intelligence, including machine learning, and drive continuous improvement in the speed, scale, and detection efficacy of Arctic Wolf's solution offerings. With their deep domain knowledge, Arctic Wolf Labs brings world-class security innovations to not only Arctic Wolf's customer base, but the security community at large.

Learn what's new, what's changed, and what's ahead for the cybersecurity threat landscape with the Arctic Wolf Labs 2024 Predictions Report.