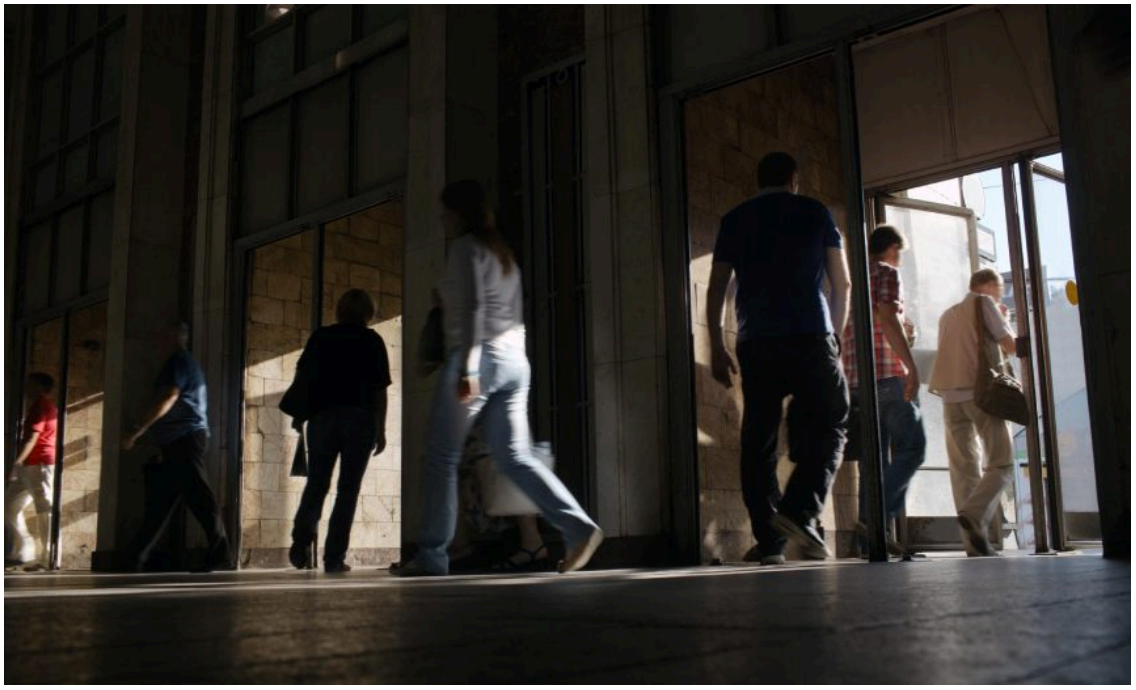
Ransomware Talent Surges to Akira After LockBit's Demise

By Mathew J. Schwartz

Archived: 2026-04-05 12:45:07 UTC

Fraud Management & Cybercrime , Ransomware

US Healthcare Entities Are Firmly in Akira Ransomware Group's Sights, Expert Warns (euroinfosec) • March 12, 2024



Ransomware groups come and go, but the cybercriminals behind them are a constant. (Image: Shutterstock)

Would LockBit by any other name be as dour? Russian-speaking ransomware groups come and go, but the individuals involved coalesce behind whatever brand name remains a going concern.

See Also: AI Pushes Cyberattacks to New Speed Levels

Hence a reported flow of top talent from LockBit, which was recently disrupted by law enforcement, to Akira, which is apparently alive and well.

"The Akira ransomware collective is receiving a major influx of talented post-Conti pentesters who appear to have their sights set on hitting 'healthcare entities in the U.S.,'" said Yelisey Bohuslavskiy, chief research officer at RedSense, in a LinkedIn post.

The term pentesters is ransomware group double-speak for black hat hackers who infiltrate targets and deploy crypto-locking malware as a prelude to extortion. The extortion payment, they say, is merely a postpaid charge for

penetration testing services.

What this means for potential victims, including in the healthcare sector, is that the criminals who previously worked for LockBit will be trying the same tricks, only now under Akira's banner. From a defensive standpoint, security experts said, the pentesters involved have a predilection for targeting known vulnerabilities in Cisco devices, hitting outdated VMware ESXi virtual machines, and tricking victims into installing remote monitoring and management software, through which the attackers try to push ransomware.

Post-Conti Ransomware Groups

From 2018 until February 2022, Ryuk and its successor Conti dominated the ransomware scene. Then Conti's leadership publicly backed Russia's invasion of Ukraine, instigating a worldwide backlash against paying the group extortion money.

Conti subsequently splintered, and its various internal teams started up fresh operations under new names, including Zeon, Royal and Black Basta (see: *Conti's Legacy: What's Become of Ransomware's Most Wanted?*).

Akira appears to have "close ties with the Ryuk side of post-Conti," which led to a relationship with Zeon - formerly Conti Team One, which ran TrickBot - including Akira's "original pentesters deploying Ryuk in the syndicate's early days," RedSense said.

Last summer, IBM X-Force reported that various post-Conti groups or factions appeared to maintain "a high level of communication and cooperation," including sharing resources such as cryptors. All of this, X-Force said, challenged "the assumption that the new factions are all separate or distinct groups."

"We obtained credible primary source intelligence directly related to post-Ryuk leadership, indicating that Zeon is operating as a group of elite pentesters for both Akira and LockBit, with the latter being their main focus," said Bohuslavskiy in December.

Disrupting Ransomware

Law enforcement recently turned the pentesting tables on two major ransomware groups, infiltrating and disrupting Alphv/BlackCat in December and LockBit in January. Following the takedowns, each group separately claimed to reboot before appearing to go dark.

They may be back. Ransomware groups regularly spin up fresh infrastructure or reboot under a different name. Alphv/BlackCat, for example, previously operated as BlackMatter, which changed its name from DarkSide after hitting Colonial Pipeline in May 2021.

Many of the individuals involved - operators, affiliates and contractors - as well as essential service providers, such as initial access brokers and money launderers, operate from Russia, which never extradites its citizens. Even when a ransomware group gets disrupted, experienced practitioners simply sign up with a different service or launch a new one.

That doesn't mean law enforcement agencies and security experts aren't celebrating the recent disruptions, including of LockBit. The group perpetrated some of the biggest ransomware attacks of recent years, functioning

as a ransomware-as-a-service operation, meaning it provided crypto-locking malware to vetted affiliates, who used the malware to amass victims and then shared in the resulting profits.

The group also hit smaller businesses - comprising 500 or fewer employees - hard, said cybersecurity firm Sophos. In 2023, 28% of the small business ransomware incident response engagements Sophos handled traced to LockBit, followed by Akira at 16% and Alphv/BlackCat at 14%.

At some point last year, LockBit appears to have quietly altered its approach. Marley Smith, principal threat researcher at RedSense, said that by the end of 2023, the vast majority of LockBit's revenue appeared to trace not to affiliates but to highly skilled teams or "ghost groups" that worked quietly on LockBit's behalf and bolstered its image.

Bohuslavskiy said LockBit's ghost groups were largely comprised of highly experienced pentesters from Zeon who have extensive experience with big-game hunting as well as scaring victims into thinking their systems have been infected by ransomware and then tricking them into installing it.

The latter scheme is a variation of a gambit known as BazarCall, which is a "callback phishing" tactic pioneered by the Conti ransomware group that typically involves attackers trying to trick technical support teams into installing remote-control software, which they use to push malware into a victim's network.

Many attacks conducted by Zeon on LockBit's behalf led to victims rapidly meeting attackers' ransom demands, and the attacks never came to light publicly, RedSense said.

Zeon devoting more resources to Akira isn't welcome news. Ransomware incident response firm Coveware said that in the second half of last year, Akira was already the most-seen strain in incidents it worked. During the last three months of 2023, Akira accounted for 17% of all incidents it investigated, followed by BlackCat at 10% and LockBit at 8%.

Essential Defenses

For defenders who want to block attacks by Akira and its associates, rapid patching remains essential. Security researchers have previously tied the group to:

- The targeting of Cisco VPN accounts that lacked multifactor authentication;
- The exploitation of the CVE-2023-20269 zero-day vulnerability in multiple Cisco products' remote VPN access features, including in the Cisco Adaptive Security Appliance software and Cisco Firepower Thread Defense software, to hit managed service providers and others;
- The targeting of known vulnerabilities in VMware ESXi virtual machines.

In January, following a spate of Akira attacks that hit Finnish organizations, cybersecurity officials in Finland urged defenders to review their backup strategies. They said Akira appeared to be expert at searching for and destroying backups, including network-attached storage servers and tape backups, to prevent victims from simply restoring their systems.

Pentesters working with Zeon will likely continue trying to trick victims into installing remote management and monitoring software and to target ESXi and cloud environments, Bohuslavskiy said.

Keeping software fully patched and updated appears to remain a top defense against Zeon hackers. "While the group is capable of targeting ESXi and cloud environments, well-updated hypervisors and cloud backup frameworks present a major challenge for them, which we have been seeing by observing their internal chatter," Bohuslavskiy said.

In addition, "network segmentation and segregation significantly complicate Zeon/Akira infiltration movements" and make their attacks much easier to detect, he said.
