Are Akira Ransomware's Crypto-Locking Malware Days Numbered?

bankinfosecurity.com/blogs/akira-ransomware-apparently-in-decline-but-still-threat-p-3480

Fraud Management & Cybercrime , Ransomware

Ransomware-Building Group Lost Royal-Organized Competition, Researchers Say Mathew J. Schwartz (euroinfosec) • July 27, 2023

Akira's retro-looking data leak site

Is the Akira ransomware story coming to an end?

See Also: OnDemand Panel | Securing Operational Excellence: Thwarting CISOs 5 Top Security Concerns

Bursting onto the ransomware scene in late March, Akira quickly racked up a growing list of victims. Files encrypted by the ransomware strain have `.akira` appended to their name.

Sophos reported in May that it had investigated two different Akira attacks in April against victim organizations as part of its incident response efforts.

Ransomware incident response firm Coveware reported that during the second quarter of this year, Akira was the fifth-most-common strain of ransomware it saw, saying it had been responsible for 5% of successful attacks it investigated. While that's less than BlackCat and Black Basta - each at 16%, Royal at 10% and LockBit at 6%, it's still notable.

The ransomware group claims on its data leak site to have hit at least 63 organizations since its launch, security operations provider Arctic Wolf said in a Wednesday blog post. Whether or not those victims are real remains unclear. Ransomware groups regularly lie to try and boost their reputations.

In June, researchers reported that the Akira group had developed and begun to use a "sophisticated" Linux version of their malware.

The ransomware shares its name with a 1988 cyberpunk animated film, and its data leak site channels a retro '80s look. Another ransomware strain active in 2017 also used the name, but the newer strain "bears no code similarity" and seems to be unrelated, Sophos reported.

In fact, the code has overlaps with Ryuk ransomware, which likely also helps explain the choice of an anime name, writes Yelisey Bohuslavskiy, partner and head of R&D at New York-based threat intelligence firm Red Sense, in a LinkedIn post.

Based on internal Royal communications Red Sense obtained, Akira's developers appear to have been one of several groups asked by the Conti spinoff to participate in a competition it had organized to select a next-generation crypto-locker malware, for which they retained the original Ryuk developer to be judge, he said.

Ryuk is a god of death in Japanese mythology and a protagonist in the early 2000s manga-turned-anime series "Death Note." The developer of Ryuk ransomware is known to be a manga buff.

Whoever built Akira appears to have based the malware on the original version of the Ryuk crypto-locking malware code and to have picked its name to curry favor with the judge, Bohuslavskiy said. Each of the contestants, which also included BlackSuit, also appear to have received a batch of initial accesses to victims' networks.

Unfortunately for Akira, it doesn't seem to have made the cut. "Despite a spike in activity, Akira failed to secure victory in the competition, and by May, they communicated to Royal that they were running out of targets," Bohuslavskiy said. "Subsequently, in June, Royal called off the competition, leading to a sharp drop in Akira's activity."

Another nail in Akira's coffin came in late June, when security firm Avast released a free decryptor for the ransomware that can decrypt both Windows and Linux files.

Still, predicting the demise of ransomware groups is a fraught activity. Ransomware-tracking experts say many groups go on vacation over the summer, leading to a decline in attack volumes. Akira's fate may not be clear until months from now. In addition, just because one ransomware group doesn't succeed, that doesn't mean that anyone involved in running the group and attracting employees or business partners, as well as developers and affiliates, won't carry on working for someone else or under a different name.

As ransomware groups continue to collectively earn hundreds of millions of dollars in illicit profits via crypto-locking malware, it's no wonder so many criminals keep wanting a piece of the action.

On that front, it's not yet clear who - if anyone so far - won Royal's competition. Bohuslavskiy told me that the entire effort got extremely "confusing" with BlackSuit in play, AresLoader also developing a loader, and Royal having a close working relationship with BlackCat and

continuing to borrow its loader. "Finally, the original Ryuk developer is likely involved, so it's a big competition," he said, and Royal likely hasn't yet made up its mind what to do next. Stay tuned.