BlackCat Ransomware 'Unseizing' a Dark Web Stunt

Ransomware Group Declares Nothing Off Limits Outside of CIS Countries

BY David Perera (@daveperera) • December 19, 2023 (link)

The BlackCat ransomware-as-a-service operation's putative "unseizing" of its leak site from the FBI is a stunt made possible by way the dark web handles address resolution, security researchers said Tuesday. The stunt was a "tactical error" that could alienate affiliates.

U.S. authorities as part of an international law enforcement operation announced Monday morning that they had seized dark web infrastructure of the BlackCat ransomware-as-a-service group (see: *FBI Seizes BlackCat Infrastructure; Group Has New Domain*).

The Russian-speaking group established a new dark web leak site and replaced the FBI seizure notice on its previous leak site with a Russian-language note. "This website has been unseized," it declared. In the note, the ransomware gang said that no targets are now off limits, except those inside the Commonwealth of Independent States, a Russia-dominated association roughly compromised of countries formerly part of the Soviet Union.

"You can now block hospitals, nuclear power plants, anything, anywhere," the site said, according to machine translation.

BlackCat, also known as Alphv, was able to substitute its own notice for the FBI seizure notice because the gang likely preserved a copy of the public-private key associated with that dark web domain. Domain name resolution for .onion sites - websites accessible through the Tor network - isn't similar to the hierarchical system of the open web.

"There isn't a central location. It's all based on who has the key pair, and the way the protocol works is whichever server is the most recent to have the key pair is the one that the traffic gets redirected to," said Allan Liska, a ransomware expert at Recorded Future. "They didn't 'unseize' it in the way that they're using the term." Law enforcement still should have possession of the original server.

The FBI told Information Security Media Group it has no further comment on today's events beyond the Justice Department press release.

The ransomware actors were able to retain the public-private key pair in advance of their server's seizure likely because of leaks about the law enforcement operation, Liska told ISMG (see: *Ransomware Group Offline: Have Police Seized Alphv/BlackCat?*).

Brett Callow, a threat analyst at Emsisoft, called BlackCat's posted note a "tactical error" that could alienate affiliates - the hackers who work on commission to spread the group's malware. "If Cyber Command weren't looking at them before, they certainly are now, and declarations like this make them public enemy number one." Sensible affiliates will distance themselves from BlackCat, he added, despite the group's offer to decrease its take from extortion payments down to 10%.

BlackCat earlier offered affiliates a sliding scale of between 80% and 90% of the extortion money depending on the extortion amount, said cyberthreat intelligence firm Mandiant. The firm said it has already spotted actors affiliated with LockBit, another high-profile Russian-speaking ransomware-as-a-service group, apparently attempting to gain market share by appealing to BlackCat "affiliates and offering to post data from victims who were in the negotiation process with Alphv."

As of publication, the FBI has restored its seizure notice on the BlackCat leak site.