BlackCat plays dirty with malvertising mouse traps • The Register

theregister.com/2023/11/16/blackcat_ransomware_luring_corporate_targets/

Connor Jones

Updated Affiliates of the ALPHV/BlackCat ransomware-as-a-service operation are turning to malvertising campaigns to establish an initial foothold in their victims' systems.

Paid adverts for popular business software such as Slack and Cisco AnyConnect are being used to lure corporate victims into downloading malware that in turn leads to ransomware deployment.

Rather than downloading the legitimate software, victims are instead infected with Nitrogen malware – an initial access payload that can be used to launch second-stage attacks, akin to the the deployment of ransomware.

eSentire's Threat Response Unit (TRU) says it was engaged after affiliates of the ransomware group targeted its customers on multiple occasions.

The Nitrogen malware campaign was first observed in June, but the tactic of malvertising associated with Nitrogen is new.

"Nitrogen is initial-access malware that leverages Python libraries for stealth," says Keegan Keplinger, senior threat intelligence researcher with TRU in its report. "This foothold provides intruders with an initial entry into the target organization's IT environment.

"Once the hackers have that initial foothold, they can then infect the target with the malware of their choosing. In the case with this attack campaign, the target victims are being infected with the ALPHV/BlackCat ransomware."

Using Python libraries allows attackers to more easily blend into an organization's normal traffic patterns since they are so ubiquitous. Added obfuscation techniques further delay defenders from spotting malicious activity.

eSentire says it stopped the BlackCat ransomware attack before it unfolded, but the company has a special resentment for the group owing to its previous, "despicable" methods.

Not only is the group known for its willingness to target victims in the healthcare sector, activity that's considered off-limits even for some criminals, in July it also tried to extort one healthcare network by posting topless images of breast cancer patients. The same tactic was repeated recently by the Hunters International group.

Among its other major scalps claimed this year are social media giant Reddit, Seiko Group, and Barts Health NHS Trust – the latter another example of healthcare attacks.

The group has also shown its continued ambition to evolve and strengthen over time. It recently broke its rule on partnering with English-speaking cybercriminals after welcoming Octo Tempest into its affiliate program.

Octo Tempest's expertise in SIM swapping, SMS phishing, and advanced English-speaking social engineering campaigns was enough to seduce BlackCat, supposedly with a view to opening up its pool of potential targets.

Malvertising scourge

Malvertising has grown in popularity among cybercriminals in the past few years, with Google often addressing the issue reactively rather than proactively.

Security researcher Will Dormann posted a lengthy thread to X earlier this year criticizing Google's apparent lack of action in preventing malicious ads from appearing in Search results.

It followed a widely publicized case of a cryptocurrency influencer downloading what they thought was a copy of the OBS streaming software. The link turned out to be malware and they then had their NFT (remember those?) wallet raided.

Among the many criticisms was the suggestion that Google didn't run links through the VirusTotal platform, which it owns, before approving them for display.

Ransomware crooks SIM swap medical research biz exec, threaten to leak stolen data

READ MORE

In a number of examples listed by Dormann, searches displayed links that led to known malicious payloads detected by various security vendors.

Numerous malware campaigns used malvertising for attacks throughout the year. HP Wolf Security's report from January found a notable increase in malvertising activity, especially toward the end of 2022.

It found a variety of campaigns making use of search engine ads to promote their payloads, including IcedID, BatLoader, and Rhadamanthys Stealer. Weeks later, SentinelOne alerted the community to .NET malware loaders using the same method.

Recently, in its Digital Defense Report, Microsoft identified Magniber deployments from the Russian cybercrime group that it tracks as Storm-0381 through its heavy use of malvertising. ®

Updated on November 17 to add:

A Google spokesperson told *The Register*: "We don't allow ads on our platform that contain malicious software. We've reviewed the report in question and taken action where appropriate. We continue to see bad actors operate with more sophistication and at a greater scale, using a variety of tactics to evade our detection.

"We invest heavily in our ads safety efforts and have a team of thousands working around the clock to enforce our policies at scale."

More about

- Cisco
- Cybercrime
- eSentire

×

More about

Narrower topics

Broader topics

Security

More about

1 COMMENTS

More about

- Cisco
- Cybercrime
- eSentire

×

More about

- Cisco
- Cybercrime
- eSentire
- Ransomware
- Slack

Narrower topics

- Kenna Security
- NCSC
- REvil
- Wannacry
- Webex

Broader topics

Security

TIP US OFF

Send us news