BlackCat takes three-pronged approach to ransomware

What Cisco Talos knows about this threat, and how you can stay protected

BACKGROUND
BlackCat (aka ALPHV or Noberus) is a highly skilled ransomware-as-a-service (Raas) group. It emerged in late 2021 and quickly became one of the most active and impactful cybercrime groups, compromising dozens of organizations across the globe. BlackCat aims to attract highly skilled actors by actively recruiting on Russian-language forums and offering unusually lucrative payouts, allowing affiliates to keep up to 90 percent of the ransom. Cisco Talos assesses that some BlackCat affiliates formerly worked with the BlackMatter ransomware gang, as we observed the two groups using many similar tactics, techniques and procedures (TTPs).

CAPABILITIES
- BlackCat uses a triple-extortion tactic, whereby they steal data prior to encrypting devices, threaten to publish the data, and then indicate they’ll target the victim with follow-on distributed denial-of-service (DDoS) attacks if the ransom is not paid.
- BlackCat is uniquely recognized as the first group to commercialize ransomware based on the Rust coding language and use it in such public and lucrative cyber operations.
  - Rust is more user-friendly, secure, easy to debug, highly customizable, and able to quickly process large amounts of data.
- Once the malware gets a foothold into the target environment, the attackers can perform a variety of malicious actions, including encrypting victims’ files, maintaining persistence on the network and stealing sensitive information.
- Researchers from Talos have observed BlackCat activity, targeting companies predominantly located in the U.S. and Europe, across numerous industries.
- Talos is actively tracking BlackCat’s TTPs, compiling a broad list of the methods they use to establish persistence and propagate across a victim’s network, as well as elevating their privileges on the targeted machine.

RESPONSE
- Talos conducts regular open-source research on activity leveraging BlackCat.
- We use these findings to look for correlations with other threat actors or campaigns, as well as a starting point from which to pivot and conduct follow-on research.
- Our findings lead to new ClamAV, SNORT and Cisco Secure product coverage.
- Additionally, Talos has provided a full list of remediation recommendations victims can take should they be infected with BlackCat, along with precautionary tactics to prevent any ransomware attack.

COVERAGE
- Cisco Secure Endpoint deploys coverage into users’ environments, blocking BlackCat’s ability to dump user credentials and any attempts to disrupt critical processes.
- Cisco Talos Incident Response (CTIR) can assist customers in preparing for an attack and discovering any potential points of entry.
- There are ClamAV and Snort signatures that protect users from many of BlackCat’s malicious activities. We are continuing to create additional coverage as well.