LOGPOINT

Dec 08, 2022 07:00 CET

Hunting BlackCat: A ransomware family on the rise

- **Logpoint research reveals that BlackCat has the fourth-highest number of victims in the last six months.**
- **BlackCat uses its public leak site to intimidate victims, where anyone can easily search and access the leaked victim information.**

COPENHAGEN, Denmark & BOSTON, December 8, 2022 – Intimidation is the name of the game with BlackCat ransomware. Victim information is made easily accessible on the BlackCat website, ransom demands increase, and encryption keys are deleted. The intimidation seems to be working. The ransomware group had the fourth highest number of victims from May to

November 2022, Logpoint research reveals, and the highest ransom demanded so far is 14 million dollars.

Logpoint's Security Analyst team has analyzed multiple variants of the BlackCat ransomware to understand its Tactics, Techniques, and Procedures (TTPs). The analysis reveals that the ransomware mainly achieved initial access via spearphishing, tricking victims into downloading macro-enabled documents. The ransomware supports multiple encryption modes along with intermittent encryption, providing speed and defense evasion capabilities. In addition, BlackCat uses the data destruction method to destroy essential data or render it useless, maximizing the impact on the victim.

"BlackCat operates under the Ransomware-as-a-Service (RaaS) model and uses both double and triple extortion techniques. Now that it's spreading, organizations need to be extra cautious," says Doron Davidson, VP Logpoint Global Services. "Each second wasted equals lost data, so organizations must implement preventive measures that enable detection, apply automation for enrichment and response, and keep contingency plans up their sleeve."

To safeguard your organization against BlackCat, Logpoint recommends:

- Monitor carefully for suspicious activity that shows the possibility of BlackCat infection, such as suspicious processes spawned by various Microsoft Office utilities
- Simulate the worst-case scenarios regularly and make sure the incident response, playbooks, and disaster recovery plan are in place for working and continuity of business
- Use segmentation or other methods to design the network in such a way as to maximize the reduction of impact from BlackCat

Read Logpoint's blog post about hunting and remediating BlackCat ransomware here. It contains an in-depth technical analysis of execution and persistence, lateral movement, impact, and more. It also provides tangible means of detecting, investigating, and responding to BlackCat.

About Logpoint
Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of

evolving threats. By combining sophisticated technology and a profound understanding of customer challenges, LogPoint bolsters security teams' capabilities while helping them combat current and future threats. Logpoint offers SIEM, UEBA, SOAR and BCS technologies converged into a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more. Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company. For more information, visit http://www.logpoint.com

Contacts

Maimouna Corr Fonsbøl
Press Contact
Head of PR
PR & Communications
mcf@logpoint.com
+45 25 66 82 98