Trinity Cyber

THREAT PREVENTION CASE STUDY

BlackCat Ransomware

BlackCat Ransomware

BlackCat ransomware, also known as ALPHV, is a far-reaching ransomware threat often used in Ransomware-as-a-Service (RaaS) attacks. BlackCat ransomware attacks have targeted organizations in multiple industries including energy, transportation, retail, utilities, telecommunications, and pharmaceuticals. However, all organizations, regardless of sector, are potential targets for BlackCat ransomware attacks.

The FBI recently issued FBI FLASH #CU-000167-MW on BlackCat ransomware noting that it is the first to use Rust, considered widely to be a more secure programming language. The use of Rust helps BlackCat evade detection from many commonly deployed security products. Ransomware groups employing BlackCat often begin the attack by encrypting and exfiltrating files, followed by a ransom demand to unlock the files. They then threaten to release the stolen files, sometimes adding the additional threat of a DDoS attack against the victim, unless the ransom is paid.

Trinity Cyber's **TC:Edge** *service, powered by the Trinity Cyber Engine, automatically prevents BlackCat and other ransomware attacks*

Blackcat Ransomware Attacks

A Unit 42 report notes that, because BlackCat is coded using the Rust programming language, the malware authors can easily compile it against various operating system architectures. Microsoft has already reported that it has observed successful BlackCat attacks against Windows and Linux devices as well as VMware instances.

BlackCat ransomware and other cyber attacks are successful because traditional network security products are failing in their mission to provide protection. Modern attackers constantly improve their tactics and find ways to penetrate their target's cyber defenses. For instance, adversaries often employ different techniques (such as obfuscation) which enable their cyber attacks to go undetected. All too often, organizations find that their traditional security products are simply inadequate; they do not and cannot examine Internet content deeply or accurately enough with the speed necessary to make a difference inline, nor do they have the preventive controls necessary to defeat and prevent modern threats. BlackCat and other threats are being missed, and organizations are vulnerable.

KEY TAKEAWAYS

- ***Prevents*** **BlackCat ransomware attacks on corporate networks**
- **Accurate detection and prevention enabled by full session protocol and file parsing within network traffic coupled with new automated preventive controls**
- **Dramatically reduces incident response workload and cuts false positives**

Stopping BlackCat Ransomware Cold

To solve the biggest challenges in cybersecurity, Trinity Cyber invented a breakthrough technology: the Trinity Cyber Engine. In less than a millisecond, it automatically deeply inspects and transforms full session Internet traffic in both directions to expose and mitigate actual threat content inline. *It dramatically reduces incident response workloads, cuts false positives, and delivers superior security against cyber attacks.*

The Trinity Cyber Engine powers the **TC:Edge** managed service line which detects, mitigates and prevents BlackCat ransomware and entire classes of other individual threats. **TC:Edge** provides security teams and organizations highly accurate network prevention against malware and exploit delivery,

Unlike others, the **TC:Edge** service prevents attacks by identifying and defeating attacker tactics, techniques and procedures (TTPs). This is critical to defeating and preventing entire classes of BlackCat ransomware (as well as other ransomware strains), actual malware, command and control (C2), remote code exploits (RCE), drive-by downloads, and in-the-wild malicious threats that are commonly missed by traditional detect-and-respond systems. The **TC:Edge** service automatically detects and removes BlackCat ransomware in *less than a millisecond, preventing it from fully executing.* **TC:Edge** dramatically reduces stretched security team's incident response workload with highly accurate and automated network threat prevention. Detailed threat intelligence, metadata and the actions taken by Trinity Cyber are immediately available to customers on their portal. BlackCat ransomware attacks are stopped cold, and users, data and infrastructure remain secure and protected.

Want to learn more? Contact us at info@trinitycyber.com for more information.

Gartner
COOL VENDOR 2020