FBI Shares Information on BlackCat Ransomware Attacks

By Ionut Arghire on April 21, 2022

The Federal Bureau of Investigation (FBI) this week published indicators of compromise (IOCs) associated with the BlackCat Ransomware-as-a-Service (RaaS).

Initially observed in November 2021 and also tracked as ALPHV and Noberus, BlackCat is the first ransomware family to be written in the Rust programming language.

As of March 2022, BlackCat had successfully compromised at least 60 organizations worldwide, the FBI said. The cybercriminals announced nine new victims in April – as of April 21.

Security researchers recently revealed an increased interest from BlackCat operators in targeting industrial organizations.

Security researchers have also connected BlackCat with the cybercrime group behind the Darkside/Blackmatter ransomware.

BlackCat affiliates often demand ransom payments of millions of dollars, but they have been observed accepting lower payments after negotiations with their victims.

For initial access, the FBI explains, BlackCat employs compromised user credentials. Next, Active Directory user and administrator accounts are compromised and malicious Group Policy Objects (GPOs) are used to deploy the ransomware, but not before victim data is exfiltrated.

As part of observed BlackCat attacks, PowerShell scripts, Cobalt Strike Beacon, and legitimate Windows tools and Sysinternals utilities have been used. The attackers were also seen disabling security features to move unhindered within the victim's network.

As usual, the FBI recommends not paying the ransom, as this would not guarantee the recovery of compromised data, and urges organizations to proactively deploy cybersecurity defenses that can help them prevent ransomware attacks.

Related: **FBI Warns of RagnarLocker Ransomware Attacks on Critical Infrastructure**

Related: **FBI Publishes IOCs for LockBit 2.0 Ransomware Attacks**

Related: **FBI Warns Organizations of Diavol Ransomware Attacks**

Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

Meta Offers Rewards for Flaws Allowing Attackers to Bypass Integrity Checks
Access Bypass, Data Overwrite Vulnerabilities Patched in Drupal
Cisco Patches Virtual Conference Software Vulnerability Reported by NSA
FBI Shares Information on BlackCat Ransomware Attacks
New BotenaGo Variant Infects Lilin Security Cameras With Mirai

Tags:

NEWS & INDUSTRY Virus & Threats Virus & Malware Malware Tracking & Law Enforcement Cybercrime