Blackcat / ALPHV Ransomware

C-Suite level threat review by applicable business area addressing active threats.

In December, the FBI took control of Blackcat's website and released a decryption tool that allowed more than 500 victims the ability to restore their systems. In retaliation, Blackcat removed all but one restriction on the use of its ransomware. Affiliates can now target hospitals and nuclear power plants. The only exception is that affiliates cannot touch the Commonwealth of Independent States (areas from the former Soviet Union). Due to increased tensions between the FBI and Blackcat, organizations should be wary of heighted malicious activity from Blackcat and its affiliates.

Blackcat / ALPHV:

Blackcat is a Russian-based cybercrime group that operates under a ransomware-as-a-service (RaaS) model. This threat actor emerged in 2021 and is thought to be composed of members from several dissolved ransomware actors including Revil and BlackMatter / DarkSide. Affiliates primarily target the United States; 75% of victims are based in the United States. The top targeted industries by Blackcat ransomware are the finance, healthcare, manufacturing, legal and professional services industry.

Blackcat / ALPHV

Threat Level: High

Attack:

Blackcat affiliates tend to gain initial access into an organization using social engineering techniques and compromised credentials (MITRE T1598, T1566, and T1078). After obtaining initial access, affiliates may deploy remote access software such as AnyDesk and Splashtop (MITRE T1219) to establish command and control. Affiliates may also look for stored credentials and passwords to move laterally in the network and escalate privileges (MITRE T1059.001 and T1555). Affiliated threat actors may then modify Group Policy Objects (GPOs) to disable security controls and deploy the ransomware (MITRE T1484.001). Blackcat ransomware can encrypt VMware instances as well as Windows and Linux devices.

Remediation:

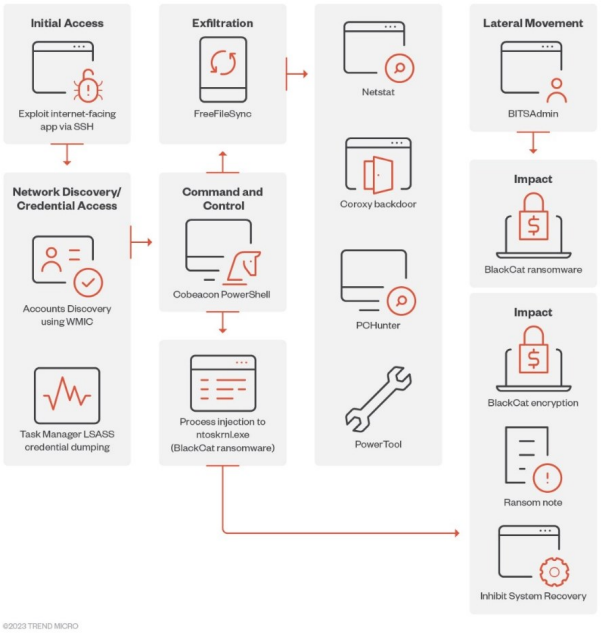
- Organizations should put in place software management controls. Users should not be able to install unauthorized remote access software or other software without prior approval.
- All users should be trained to recognize social engineering attacks. Particularly, organizations should ensure that their Help Desk is prepared to recognize advanced social engineering attacks. It is recommended for Help Desk personnel to receive training on this and to follow a formal process for user verification that requires two or more verification factors.
- Test and validate your organization's security controls against the MITRE ATT&CK techniques utilized by Blackcat affiliates.

Blackcat Ransomware:

- **Analysis Blackcat ransomware:** https://securityintelligence.com/x-force/blackcat-ransomware-levels-up-stealth-speed-exfiltration/
- **Cybersecurity advisory on Blackcat ransomware:** https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a

How K logix Can Help

- Technology Advisory
  - Email Security
  - Endpoint Detection and Protection (EDR)
  - Identity and Access Management (IAM)
  - Managed Security Service Provider (MSSP)
  - Security Information and Event Management (SIEM)
  - Cloud Security Posture Management (CSPM)
  - SaaS Security Posture Management (SaaS)
- Programmatic Advisory
  - Advanced Risk Assessment (i.e., HIPAA, NIST, PCI, etc.)
  - Cloud Security Maturity
  - Identity and Access Management Program Maturity
- Threat Intelligence
  - Notification to customers of threats
  - On-demand briefings
  - Threat exposure workshops
  - User awareness training seminars
  - Monthly and quarterly threat intelligence reports



Attack chain using Blackcat ransomware

Source: https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackcat