Threat Intelligence Report

Trends in Threat Actor Behavior Post-Disruption

Law enforcement takedown operations, which include seizing threat actors' infrastructure, taking over their leak sites, issuing decryptors, and arresting cyber criminals, can significantly disrupt criminal operations, help victim organizations recover from incidents, and diminish threat groups' credibility in the cyber crime ecosystem. Following takedowns, however, threat actors often work quickly to resume their operations, establish new infrastructure, and even alter their tactics, techniques, and procedures to make future law enforcement disruption attempts less successful.

THREAT ACTIVITY

LOCKBIT

In February 2024, an international law enforcement team announced a coordinated operation against the LockBit ransomware gang. This operation involved arrests of alleged affiliates, the closure of thousands of threat actor accounts, and seizure of LockBit servers around the world. The operation also exposed Lockbit for not deleting victim data after payment, despite promising to do so.

Lockbit attempted to launch a new extortion site days later with new victim companies listed, but the new site did not feature any organizations targeted prior to the operation. Following the takedown, threat researchers identified a ransomware variant built using a LockBit 3 tool leaked in 2022. This tool was used to exploit critical vulnerabilities in remote access software and demonstrates the long-term impact of these groups, even if their present-day operations are disrupted.

BLACKCAT/ALPHV

In December 2023, the Federal Bureau of Investigation (FBI) announced a large-scale disruption of the BlackCat/ALPHV group, during which law enforcement released a decryption tool to more than 500 affected victims and seized several threat actor websites.

Following the disruption, BlackCat/ALPHV administrators launched a new dark web site, where they announced increased affiliate commissions and the removal of restrictions on potential victims, explicitly naming hospitals and nuclear power plants as fair game. In February 2024, the group claimed responsibility for a crippling attack on a U.S. healthcare company. In March 2024, the group's newest website featured an apparent seizure notice from international law enforcement, despite law enforcement denying involvement in the takedown. Experts speculate the group faked their own takedown to avoid making payments to affiliates, highlighting how threat actors may mimic large-scale operational disruptions for their own benefit.

THREAT ASSESSMENT

Short-Term Disruption vs. Long-Term Impact: Although takedowns can disrupt ransomware operations in the short-term, the long-term impact of these pauses may be limited. Ransomware groups often demonstrate resilience by re-forming under new names, with the same or similar members, thus quickly restoring their capabilities.

Fragmentation of Groups: The fragmentation of major ransomware groups post-takedown can lead to an increase in attacks. Smaller, autonomous cells may compete for resources or reputation, leading to a spike in ransomware activities as they attempt to establish dominance in the ransomware ecosystem.

Cashout Schemes: Following major disruptions to their operations, ransomware groups may pursue last-ditch efforts to make as much money as possible before taking their operation entirely offline. In these circumstances, the groups no longer care to preserve their reputation in the cyber criminal ecosystem, and may take aggressive action to maximize payout, often at the expense of their affiliates and victims.

RECOMMENDED ACTION

Organizations should not assume that the law enforcement takedown of a ransomware group means that the group no longer poses a threat. After significant ransomware group disruptions, organizations should continue to:

- Continuously monitor for threats and stay up-to-date on the latest cybersecurity risks and intelligence reports.
- Update devices regularly and apply any patches issued, especially for known vulnerabilities being exploited.
- Have a robust, routinely-tested incident response plan in place that includes the defined roles and expectations of involved parties.
- Confirm that critical assets are regularly backed up and stored on a separate network to ensure that access to significant resources is not restricted during a ransomware attack.

SOURCES

Sources include open-source information from public and private industry reporting.

- LockBit ransomware gang attempts to relaunch its services following takedown
- FBI posts takedown notice on AlphV ransomware group's website
- CISA Advisory: #StopRansomware: ALPHV Blackcat
- Change Healthcare confirms Blackcat/AlphV behind ransomware attack
- Europol, DOJ, NCA deny involvement in recent AlphV/BlackCat 'shutdown'

Why FTI Cybersecurity

Multidisciplinary Expertise

Intelligence-led, expert-driven, strategic approach to cybersecurity challenges

Core team from intelligence agencies, law enforcement, prosecuting offices, and global private sector institutions

Globally Positioned

Ability to respond anywhere in the world

Ability to staff the largest and most complex engagements and investigations

Relationships with the top global intelligence agencies, regulatory authorities, and private agencies

Integrated & Comprehensive

Comprehensive services include crisis communications, e-discovery, forensic investigations, and more

Seamless integration of FTI Consulting's expertise across service offerings

FTI Cybersecurity Global Offices

Americas

Atlanta
Boston
Chicago
Dallas
Houston
Irvine
Los Angeles
Mexico City
Miami
New York
Philadelphia
Roseland
San Francisco
Sao Paulo
Seattle
Toronto
Washington, DC
Wayne

EMEA

Berlin
Brussels
Cape Town
Dubai
Dublin
Dusseldorf
Frankfurt
Johannesburg
London
Madrid
Mumbai
Munich
Paris
Zurich

APAC

Brisbane
Hong Kong
Melbourne
Perth
Shanghai
Singapore
Sydney
Tokyo

CONTACT FTI CYBERSECURITY

Email: #fticybersecurity@fticonsulting.com

Phone: +1-844-CYBR-FTI (+1-844-292-7384)

FTI CONSULTING