Secureworks®
a SOPHOS company

THREAT INTELLIGENCE EXECUTIVE REPORT

Volume 2025, Number 2

Presented by the
Counter Threat Unit™ (CTU)
Research Team

Executive Summary

The Counter Threat Unit™ (CTU) research team analyzes security threats to help organizations protect their systems. Based on observations in January and February, CTU™ researchers identified the following noteworthy issues and changes in the global threat landscape:

- The cyber arms race persists
- Underground monitoring reveals cybercriminal trends
- Arrests and takedowns hamper cybercriminals, for a while

The cyber arms race persists

Threat actors continue to evolve their tactics, updating existing campaigns and introducing new tools.

Cybersecurity is often described as an arms race between attackers and defenders. In this model, threat actors continually update their tactics, techniques, and procedures (TTPs) to stay one step ahead of organizational defenses. Organizations respond by tightening and updating their defenses, and the race goes on.

In early 2025, CTU researchers observed several examples of that escalation and responded by enhancing and updating countermeasures available to customers. In one example, North Korean state-sponsored threat actors adapted the Contagious Interview campaign that CTU researchers have monitored since early 2024. During these attacks, threat actors contact and interview job-seeking developers, convincing the candidates to download an interview task that contains malware. This malware provides access to the victims' corporate networks or enables data theft from the compromised devices. The TTP changes in January 2025 included using different malware and a new way of duping the victim into downloading it.

CTU researchers also continue to monitor the evolution of a social engineering technique known as ClickFix that uses fake human verification prompts such as CAPTCHAs. These attacks have evolved to using multistage prompts, directing victims to complete two verification challenges. The first challenge is basic or appears to fail. The second instructs the victim to paste disguised malicious code into a command prompt, leading to the download of malware.

In a third example, CTU analysis of COBALT ULSTER phishing infrastructure revealed an unprotected directory containing multiple tools and malware used by the threat group, including a previously unknown backdoor malware sample. This backdoor, dubbed Caveman, contains functionality to execute commands, download additional malware, and steal data.

It is important to remember that the arms race concept does not preclude threat actors' use of established TTPs. Organizations must continue to protect themselves against known attacks while ensuring that they are able to respond to new TTPs in a timely fashion.

What You Should Do Next
Apply the latest countermeasures across your networks, endpoints, and cloud resources.

Underground monitoring reveals cybercriminal trends

Keeping a close eye on underground forums gives CTU researchers key insights into cybercriminals' intentions.

In January, CTU researchers published private reporting to customers detailing their observations on a threat actor known as '0mid16b', who regularly claimed responsibility for data breaches and large data leaks. Although 0mid16b was arrested in February, he is just one of the many threat actors who reveal details about their compromises on the dark web. Comprehensively tracking cybercriminal activity on underground forums and Telegram channels helps CTU researchers protect customers.

One key insight from this monitoring is that credential theft via infostealer infections remains a prominent cybercriminal activity. Threat actors regularly announce updates to established infostealers and advertise new ones. For example, an update from the Vidar developer in February highlighted improvements in the theft of wallet data and the consistent collection of cookies, as well as the ability to correctly gather files from Telegram and Discord. Additionally, the LummaC2 developer emphasized improvements in performance, session management, anti-fraud mechanisms, security enhancements, and an optimized event system for future updates. Visibility of these changes allows CTU researchers to update customer protections.

The volume of stealer logs for sale on underground forums continues to increase. Between early January and early March 2025, the number of logs available from just the Russian Market forum rose 2% to nearly 11.2 million. Many of the logs contain stolen corporate credentials that offer buyers easy access to organizations that have not enabled multi-factor authentication (MFA). These credentials are particularly useful to initial access brokers who compromise networks and then sell the access to other threat actors, including ransomware affiliates. The initial access brokers often name the compromised organizations in their advertisements, allowing CTU researchers to alert impacted customers.

Other significant observations during the reporting period included a threat actor offering a tool that disables antivirus (AV) and endpoint detection and response (EDR) systems. Several ransomware-as-a-service operations emerged, including BlackLock and Anubis. Ransomware operators additionally promoted software updates, new features, and even refined encryption methods on their platforms.

What You Should Do Next
Implement phishing-resistant MFA across your systems to prevent threat actors from accessing systems via stolen credentials.

Arrests and takedowns hamper cybercriminals, for a while

Global law enforcement began 2025 with active operations targeting cybercrime. However, threat actors can recover and reemerge, making continuing vigilance as important as ever.

Law enforcement agencies across the world continue efforts to disrupt and prosecute cybercriminal activity. In February, Thai police arrested four Russian nationals as part of Operation PHOBOS AETOR. Two of these suspects were wanted by U.S. and Swiss authorities in connection with Phobos ransomware attacks by the 8Base threat group. A coordinated action by law enforcement agencies spanning numerous countries seized and took down 8Base's leak and negotiation sites.

Other actions during the reporting period targeted different operations. U.S. and Dutch law enforcement coordinated to seize a Pakistani network of online marketplaces that sold cybercrime tools. The U.S., UK, and Australia sanctioned a Russia-based bulletproof hosting services provider named Zservers for supplying essential attack infrastructure for the LockBit ransomware scheme. Singaporean and Thai law enforcement arrested the self-described hacktivist known as 0mid16b, whose data extortion attacks on dozens of organizations globally resulted in over 90 data leaks.

While law enforcement actions can stop some individuals' attacks and may cause threat groups to cease activity, the impact may not last. If one bulletproof hosting service or money laundering network is disrupted, threat actors will switch to another one. If a threat actor operates from Russia, U.S. sanctions and indictments may have little impact. Chat logs that were leaked in February revealed discussions between Black Basta and LockBit operators about how LockBit was still collecting ransom payments several months after the UK National Crime Agency and the U.S. Federal Bureau of Investigation (FBI) seized the LockBit leak site in February 2024. CTU researchers have observed LockBit attacks continuing into 2025. The chat logs also indicated that previous affiliates of the now-defunct Conti ransomware scheme were now working with Black Basta. When one group ceases operation, affiliates often shift to a different scheme or even start working on their own.

What You Should Do Next

Maintain your focus on basic cyber hygiene. Despite law enforcement successes, ransomware and other cybercrime remain major threats.

Conclusion

Threat actors continue to adapt their tools and behaviors in response to external pressures. These pressures could come from organizations improving network defenses, law enforcement takedowns, or even other threat actors' actions. Closely monitoring these adaptations helps CTU researchers protect customers against the latest threats.

A Glance at the CTU Research Team

CTU researchers frequently serve as expert resources for the media, publish technical analyses for the security community, and speak about emerging threats at security conferences. Leveraging Secureworks' advanced security technologies and a network of industry contacts, the CTU research team tracks threat actors and analyzes anomalous activity, uncovering new attack techniques and threats. This process enables CTU researchers to identify threats as they emerge and develop countermeasures that protect customers before damage can occur.

Research

Understanding the nature of threats customers face, and creating countermeasures to address and protect.

Intelligence

Providing information that extends the visibility of threats beyond the edges of a network.

Integration

Infusing CTU intelligence into the Taegis XDR platform, managed solutions, and security consulting practices.

Secureworks®
a **SOPHOS** company

Secureworks, a Sophos company, is a global cybersecurity leader that protects customer progress with Taegis™, an AI-native security analytics platform built on more than 20 years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

If you need immediate assistance, call our 24x7 **Global Incident Response Hotline:**

+1-770-870-6343

