
Secureworks®
THREAT INTELLIGENCE
EXECUTIVE REPORT
Volume 2024, Number 4
Presented by the
Counter Threat Unit™ (CTU)
research team

EXECUTIVE SUMMARY

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

- Despite law enforcement wins, some cybercriminals bounce back
- Multi-factor authentication can sometimes be bypassed, but proper implementation helps
- Unauthorized downloads may contain unwelcome content

DESPITE LAW ENFORCEMENT WINS, SOME CYBERCRIMINALS BOUNCE BACK

Law enforcement actions against cybercriminals are worthwhile. However, the effects can be short-lived, so organizations should not drop their guard.

In May, law enforcement agencies announced the results of two major operations intended to disrupt cybercriminal activity. The U.S. Federal Bureau of Investigation (FBI) and Department of Justice (DOJ) took down the June 2023 incarnation of the BreachForums criminal marketplace with assistance from international partners. Operation Endgame, which was coordinated by Europol and led by law enforcement agencies in France, Germany, and the Netherlands, took down or disrupted several cybercriminal operations that delivered precursor ransomware malware. Then in June, a UK citizen alleged to be a leader of the high-profile GOLD HARVEST cybercrime group (also known as Scattered Spider) was arrested in Spain.

In addition, Operation Cronos continued its disruption activity against the LockBit ransomware-as-a-service (RaaS) operators. The identity of the LockBit administrator was revealed as Russian Dimitry Yuryevich Khoroshev, and he was indicted and sanctioned for his alleged involvement in LockBit operations.

While these law enforcement efforts had an impact, some of the cybercriminal operations recovered quickly. For example, BreachForums re-emerged within two weeks of the disruption. At least one of the malware operations affected by Operation Endgame resumed activity within days of the announcement. Some LockBit affiliates continued to conduct attacks and post victim names to the leak site, although there were indications at the end of June that the operation had paused.

Other ransomware groups increased their attack tempo, likely because affiliates switched allegiances from LockBit and the ALPHV (also known as BlackCat) scheme that ceased operation earlier in the year. In addition, ransomware groups such as RansomHub expanded beyond Windows to include variants for Linux and ESXi, increasing the scope of potential damage.

These law enforcement operations appear to be impacting the confidence of threat actors in the cybercriminal ecosystem, especially when they live within reach of Western police. But these successes do not mean that organizations should relax cybersecurity defenses. Ransomware remains the biggest cyber risk for most organizations.

What you should do next:
Stay abreast of changes in the cybercrime landscape and align detection capabilities with the latest threat actor tactics and techniques.

MULTI-FACTOR AUTHENTICATION CAN SOMETIMES BE BYPASSED, BUT PROPER IMPLEMENTATION HELPS

Multi-factor authentication is not infallible. However, it remains a valuable defense if organizations choose the right solution, implement it correctly and comprehensively, and educate employees about how threat actors may try to bypass it.

Multi-factor authentication (MFA) can stop an attacker from using stolen credentials to access systems. An absence of MFA on some Snowflake cloud platform customer accounts may have enabled high-profile compromises reported in May and June.

While MFA is one of the most important protections an organization can implement, some threat actors are bypassing it. Secureworks incident responders have observed threat actors using adversary-in-the-middle techniques to hijack the authentication process, steal the MFA token, and authenticate to the system. Other attackers use social engineering techniques. In one incident, the threat actor called an organization's help desk and impersonated an employee to request that the user's account phone number be updated to their own. This change allowed them to respond to the MFA verification challenge and change the account password. The attacker then accessed the account, viewed email messages, and deleted messages associated with password resets and MFA verification requirements. Attackers may manipulate mobile-carrier support staff in SIM swap scams to bypass SMS-based MFA solutions. Threat actors can also bypass MFA controls by convincing victims to share their one-time password, or by repeatedly pushing authentication requests to the victim's device in MFA fatigue attacks.

These tactics are not reasons to stop using MFA. They do provide a strong argument for implementing phishing-resistant MFA. Organizations should apply and properly configure MFA on all accounts. Legacy systems that do not allow MFA implementation should not be accessible from the internet. Organizations should also ensure that configurations of other systems do not create loopholes that allow threat actors to bypass MFA.

What you should do next:
Review mitigations published by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) to limit the risk and impact of these types of attacks.

UNAUTHORIZED DOWNLOADS MAY CONTAIN UNWELCOME CONTENT

Implementation of an anti-cheat system in a game highlighted the risks posed by rootkits and other malware that can hide in unauthorized software on corporate devices.

At the beginning of May, Riot Games began deploying its Vanguard anti-cheat system in the League of Legends game on Windows devices. Ordinarily, that type of gaming announcement would not generate widespread corporate interest. However, Vanguard is a kernel rootkit that provides access to and potentially control over a device. Rootkits are widely used by a variety of threat actors.

There are no indications that U.S.-based Riot Games is allowing the rootkit to do anything other than prevent gamers from cheating. Nonetheless, Riot Games is owned by Chinese conglomerate Tencent, which is closely linked to the Chinese government. The Chinese government prioritizes information gathering, and Chinese organizations are obliged to share data with the Chinese government. This type of concern previously prompted TikTok bans on government devices.

Secureworks incident responders regularly investigate attacks that start with the download of unauthorized software to corporate systems. Other incidents result from bring your own device (BYOD) policies allowing devices with insufficient security controls to connect to corporate networks. Even if few corporate-owned laptops run League of Legends, some organizations may find that employees perform work functions on devices with game clients installed. Not all games include rootkit-like anti-cheat systems, but games downloaded from torrent or pirate sites often contain malware.

The risk to the corporate network can be considerably reduced by limiting employees to only downloading software from a centrally managed repository of allowed apps. Organizations should evaluate their BYOD policies to ensure they align with security requirements. They can also prevent users from accessing gaming and other non-authorized websites.

What you should do next:
Consider enabling endpoint monitoring and detection solutions on all endpoints that have access to the corporate network, whether they are owned by the organization or the employee[1].

[1]Consult with legal counsel to determine if monitoring personal devices is permitted under applicable laws.

CONCLUSION

Good cybersecurity is an ongoing process. Preventing threat actors from succeeding in their attacks is possible but requires constant vigilance. Reliance on law enforcement is not enough. Organizations must stay up to date with changes in the threat landscape, improving and fine-tuning their defenses as threat actors update their skills and tooling.

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 Secureworks Taegis XDR platform, managed solutions, and security consulting practices.

Secureworks®

Secureworks (NASDAQ: SCWX) is a global cybersecurity leader that secures human progress with Secureworks Taegis™, a SaaS-based, open XDR platform built on 20+ years of real-world detection data, security operations expertise, and threat intelligence and research. Taegis is embedded in the security operations of over 4,000 organizations around the world who use its advanced, AI-driven capabilities to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
www.secureworks.com

Asia Pacific

Australia
Building 3, 14 Aquatic Drive
Frenchs Forest, Sydney NSW
Australia 2086

Japan
Otemachi One Tower 17F, 2-1,
Otemachi 1-chome, Chiyoda-ku,
Tokyo 100-8159,
Japan
www.secureworks.jp

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom

1 Tanfield
Edinburgh EH3 5DA
United Kingdom

United Arab Emirates
Building 15, Dubai Internet City
Dubai, UAE PO Box 500111

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

+1-770-870-6343

