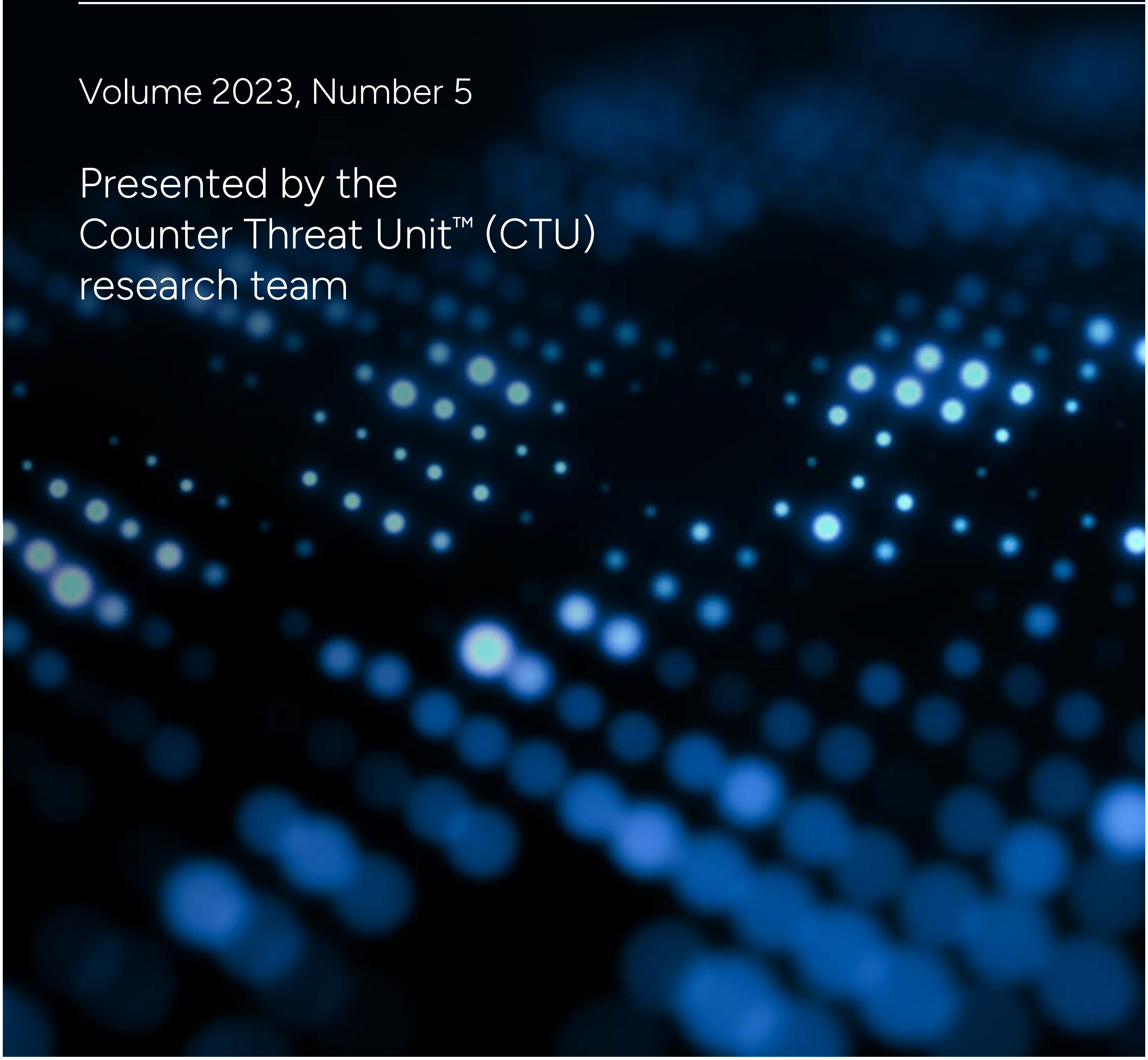
Secureworks®

THREAT INTELLIGENCE EXECUTIVE REPORT

Volume 2023, Number 5

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 July and August, CTU™ researchers identified the following noteworthy issues and changes in the global threat landscape:

- Botnet emulator shed early light on the Qakbot takedown
- Chinese cybercriminals share toolbox with state-sponsored threat actors
- Attackers used native encryption tool instead of ransomware

BOTNET EMULATOR SHED EARLY LIGHT ON THE QAKBOT TAKEDOWN

Emulating how botnets communicate with and control their victims helps us protect customers against malware that botnets distribute.

On August 29, 2023, U.S. law enforcement announced a takedown of the Qakbot criminal botnet (also known as Qbot) through Operation Duck Hunt. The financially motivated GOLD LAGOON threat group has operated the Qakbot botnet since 2007. Botnets are large networks of infected devices that threat actors use to conduct attacks for themselves or on behalf of other threat actors, including distributing malware that may lead to ransomware deployment. Devices may be recruited into a botnet without their owners' knowledge. As one of the biggest botnets, Qakbot represented a significant threat.

CTU researchers operate botnet emulators that provide unique, real-time insight into botnet activity. Valuable proprietary threat intelligence includes details about how botnets communicate with their victims. The Qakbot emulator allowed us to directly observe 10,000 infected devices across 153 countries connecting to a Qakbot server over a four-month period. From these observations, we were able to conclude that Qakbot could target victims in specific regions based on customers' requirements. We were even able to detect the early stages of individual ransomware campaigns.

The emulator and our ability to capture and understand the data also gave us early insight into the technical approach behind the takedown. The botnet emulation also provides up-to-date technical data that we use to protect Secureworks Taegis™ customers against the malware that botnets deliver.

There is no guarantee that the Qakbot takedown will hold. Botnets such as Emotet have reemerged after a short hiatus following law enforcement takedowns. If Qakbot remains shuttered, other botnets could fill the gap. Alternatively, threat actors may opt for more modern methods. Malware delivery networks like Gozi ISFB and Smoke Loader eschew old-style standing armies of traditional bots for more agile, ad hoc loader task forces formed for specific campaigns. Whatever transpires, the CTU botnet emulators will help us continue to monitor these types of activity and use the findings to protect customers.

What you should do next:
Configure your monitoring and detection solution to alert on the first signs of malware being delivered to endpoints. Detecting malware infections at an early stage and isolating infected hosts could stop threat actors from progressing to ransomware deployment.

CHINESE CYBERCRIMINALS SHARE TOOLBOX WITH STATE-SPONSORED THREAT ACTORS

Techniques used in Chinese ransomware attacks often have more in common with Chinese state-sponsored cyber activity than with techniques used by Russian ransomware actors.

Ransomware attacks are typically associated with cybercriminals in Russia and other former Soviet countries. However, CTU researchers have attributed multiple financially motivated compromises since 2021 to China-based threat groups, particularly GOLD FIESTA and GOLD BARONDALE. These attacks result in the deployment of ransomware such as Hello, Cring, and Rapture.

While Chinese state-sponsored threat groups such as BRONZE STARLIGHT may use ransomware attacks to hide cyberespionage and intellectual property theft, GOLD FIESTA and GOLD BARONDALE appear genuinely financially motivated. Despite different intent, the financially motivated groups' tactics, techniques, and procedures (TTPs) have more in common with Chinese state-sponsored groups than with Russian cybercriminals. These similarities may result from the preference shown by all types of Chinese threat actors for open-source tools and techniques developed by Chinese researchers. It is rare for Russian and Eastern European cybercriminals to use Chinese-language tools.

The Chinese government strongly supports security research, with the expectation that the results are first shared with them for state-sponsored activities. Only later does the wider Chinese cybersecurity community gain access. The use of these tools and techniques by cybercriminals does not necessarily indicate that they are tasked by the Chinese government. However, the overlap does confuse attribution.

What you should do next:
Ensure that you can detect and mitigate TTPs used by various Chinese threat groups, even if you do not consider your organization at risk of Chinese state-sponsored cyberattacks.

ATTACKERS USED NATIVE ENCRYPTION TOOL INSTEAD OF RANSOMWARE

Attackers can encrypt victims' files for financial gain without using ransomware. Awareness and proper configuration are essential for preventing an organization's own resources from being used against them.

In July, CTU researchers analyzed an incident involving threat actors using the victim's own technology for encryption. The NEWTON threat group used the native Windows BitLocker to encrypt the victim's files before demanding a ransom. This use of BitLocker is rare but not unique: CTU researchers observed the Iranian COBALT MIRAGE threat group use BitLocker in previous ransomware attacks.

Use of native tools poses an additional challenge for organizations, as it limits the ability of defensive monitoring solutions to detect the malicious activity. The previous Threat Intelligence Executive Report described how Chinese state-sponsored threat groups are increasingly using existing tools in their victims' IT environment because it helps them fly under the radar. While some security solutions may be able to block known ransomware prior to deployment, the threat actors' use of BitLocker eliminates that opportunity.

The key to detecting the abuse of native tools like BitLocker is to ensure that monitoring solutions alert on atypical use. Access to native tools should also be restricted to users with elevated privileges. To reinforce this restriction, organizations should apply the principle of least privilege, require strong passwords, and implement multi-factor authentication.

What you should do next:
Ensure that your BitLocker configuration balances organizational need with security and prevents it from being used against you.

CONCLUSION

Threat actors select the tooling and infrastructure that best suit their purpose at a given time. Some attackers may choose native system tools while others prefer tools developed in their own country. Events in the threat landscape, such as a major law enforcement takedown, can drive threat actors to replace their traditional approaches with newer methods. Applying up-to-date threat intelligence, both written analysis and countermeasures, is an essential aspect of protecting your organization against ever-changing 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 research and intelligence into Secureworks managed security services and security consulting practices.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 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.

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