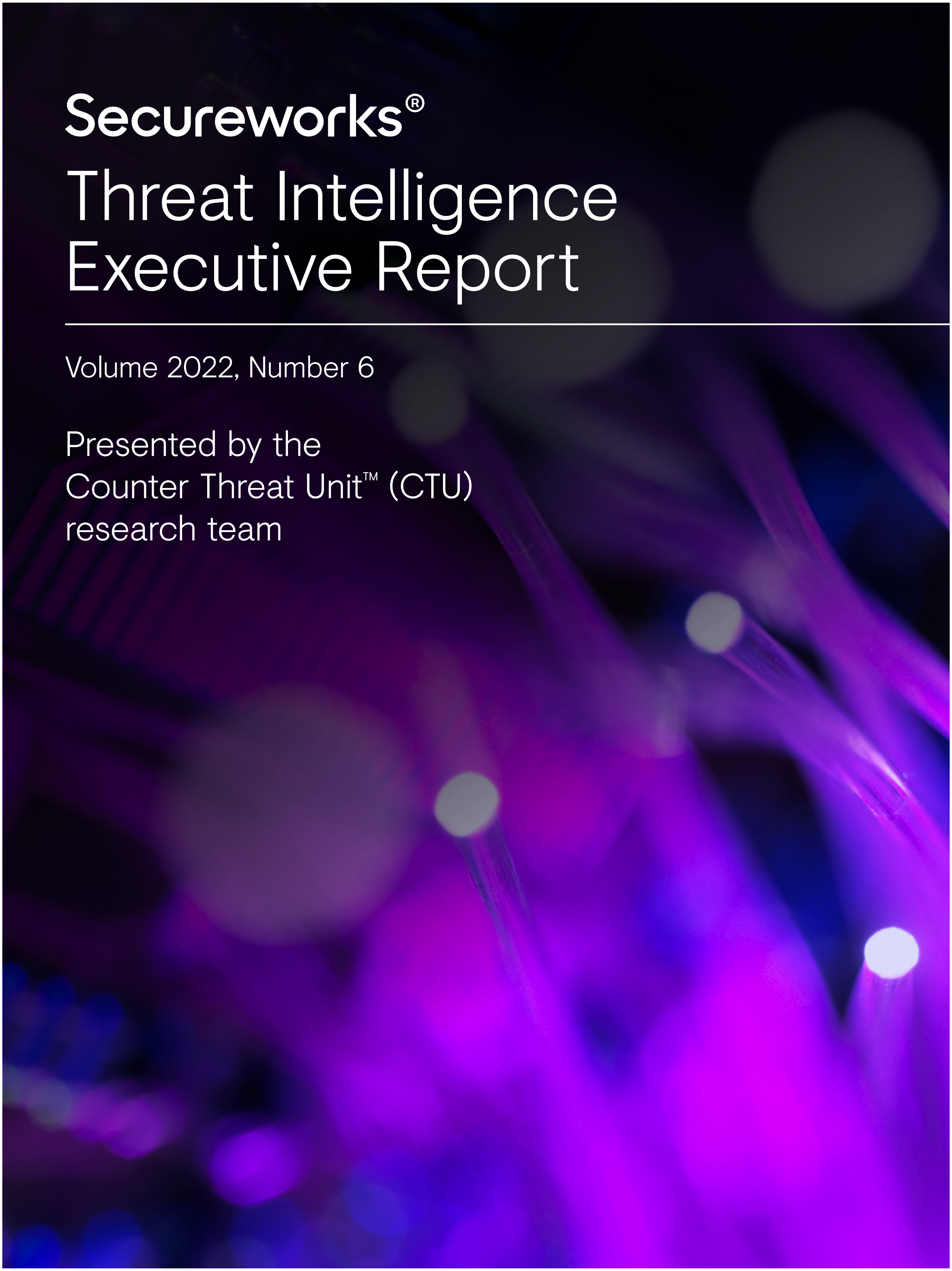

Secureworks®

Threat Intelligence Executive Report

Volume 2022, Number 6

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. During September and October, CTU™ researchers identified the following noteworthy issues and changes in the global threat landscape:

- Attackers switch to lesser-known adversary emulation tools to evade detection
- Denial of service attacks: Prepare but don't panic
- Threat actors target home users for corporate credential theft

Attackers switch to lesser-known adversary emulation tools to evade detection

Detecting both widely available and newer offensive frameworks is an essential element of cyber defense.

In October, CTU researchers discovered attackers using the Brute Ratel C4 (BRc4) adversary simulation framework against Secureworks customers.

Cybersecurity red teams use adversary simulation frameworks to probe, discover, and highlight gaps in organizations' defenses. But as highlighted in the Cobalt Strike section of the Secureworks 2021 State of the Threat report, many threat actors use these frameworks too, especially ransomware operators and Chinese government-sponsored threat groups. It's not hard to understand why: these tools are specifically designed to slip past security controls. Cracked and unlicensed versions are freely available, there is no development or maintenance burden, and developers compete to make the frameworks as feature-rich and effective as possible.

Their widespread availability to threat actors has had a damaging effect on the threat landscape. This proliferation is one of the key 'future threat challenges' that the UK National Cyber Security Centre (NCSC) identified in its 2022 annual report. Frameworks consistently favored by threat actors include Cobalt Strike and PowerShell Empire. As defenders increasingly implement controls to identify use of these tools, savvy threat actors seek lesser-known alternatives that victims may not detect.

In fact, these new frameworks often offer advanced defensive evasion capabilities. BRc4 is a prominent example. Released in December 2020, it gained popularity in early 2022 and is promoted as being able to detect and evade endpoint detection and response (EDR) tools. In July 2022, BRc4 made headlines after Palo Alto Networks found possible evidence that it was used by a threat group controlled by one of Russia's intelligence services. A cracked version was leaked in September 2022, making BRc4 even more available to a range of threat actors.

Other adversary simulation frameworks include Sliver and Core Impact, increasing the number of potentially malicious tools organizations must detect. Threat actors aren't going to suddenly stop using Cobalt Strike and PowerShell Empire, but organizations must stay up to date with new frameworks and be able to detect them too.

What you should do next:
Conduct regular tests to ensure your security controls can detect and alert on both established and newer frameworks.

Denial of service attacks: Prepare but don't panic

Distributed denial of service (DDoS) attacks from hacktivists and other threat actors rarely cause long-term business damage, but they are aggravating and stressful. It's often too late to act when they are under way, so planning, preparation, and prevention are essential.

DDoS attacks featured prominently in the media in September and October thanks to their use by hacktivists on both sides of the conflict in Ukraine. The pro-Russia group KillNet launched attacks on October 10 against several U.S. airport websites, briefly impacting site availability but causing no disruption to airport operations.

KillNet has also attacked Japanese, Romanian, Italian, and other European organizations over the course of the conflict. According to the U.S. Federal Bureau of Investigation (FBI), the impact of these attacks has been short term and limited. KillNet targets entities it views as sympathetic to Ukraine, but like other hacktivists its targeting can be unsophisticated and unpredictable.

However, hacktivists aren't the only threat actors to use or threaten DDoS attacks. Russian government-sponsored threat actors have used them against Ukrainian targets, and cybercriminals use DDoS attacks for extortion purposes. In one incident, the GOLD MYSTIC threat group threatened to launch DDoS attacks to pressure its victims during LockBit ransom negotiations. Ironically, GOLD MYSTIC experienced a DDoS attack against its leak site earlier in 2022. The GOLD FLANDERS cybercrime group uses surprise DDoS attacks coupled with the threat of additional, bigger attacks to extort payments.

Guidance from the U.S. Cybersecurity and Infrastructure Security Agency (CISA) discusses the importance of preparation in advance of denial of service attacks. Engaging mitigation services during an attack can be expensive.

What you should do next:
Proactively protect your organization by implementing a DDoS mitigation service or a dedicated mitigation device to detect and block attacks. Creating and testing a DDoS incident response plan before an incident happens aids response and recovery.

Threat actors target home users for corporate credential theft

Remote working greatly expands an organization's threat surface, especially if home-based employees use weakly protected personal devices for work purposes. This scenario can offer threat actors an easy way into corporate systems.

In October, CTU researchers discovered an underground forum post advertising access to a Fortune 500 company's network obtained from an employee's personal computer. The researchers promptly alerted the company, even though it wasn't a customer. The data stolen from the personal computer included credentials that provided access to the employee's corporate Outlook account and an internal corporate system. From those entry points, an attacker could easily reach deeper into the corporate network to deploy ransomware. The theft likely resulted from an infostealer malware infection.

Thanks in large part to the COVID-19 pandemic, remote working has become more common. Remote workers use many tools, including personal devices, to move data and stay updated on the job. Some employees use their personal devices to perform their job duties. Flexibility in how remote workers access resources makes life easier for employees and can reduce costs for employers, but it hugely increases risk.

Some organizations, especially smaller ones, may not have considered the effect on their attack surface when rushing to adapt to remote working. Their ability to monitor and protect personal devices is limited. Employees may not understand the need for strong security controls and behaviors on personal equipment. As a result, they may adopt lax security practices such as storing corporate credentials in weakly protected web browsers.

CTU researchers expect an increase in the amount of corporate credentials stolen from compromised personal devices. These credentials provide an easy initial access vector for ransomware operators and other threat actors. Limiting how employees access company resources from personally owned devices greatly reduces the organization's risk from infostealers and other forms of malware.

✓ **What you should do next:**
Enforce phishing-resistant multi-factor authentication on all corporate systems to reduce the value of stolen credentials to threat actors. Mandate secure credential management, including password managers, even on personal devices.

Conclusion

A proactive mindset about cybersecurity is one of the most important first steps toward reducing business risk. Proactive steps include detecting commonly used and newer offensive tools, protecting against DDoS attacks, and ensuring that stolen credentials are never sufficient for a threat actor to breach your systems.

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 leading global cybersecurity company that protects organizations in the digitally connected world. We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

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