Secureworks®

THREAT INTELLIGENCE EXECUTIVE REPORT

Volume 2023, 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:

- Chinese threat group combines speed with stealth
- Cyber risk from the war in Ukraine remains focused on that region
- Initial access brokers contribute to the rise in ransomware attacks

CHINESE THREAT GROUP COMBINES SPEED WITH STEALTH

Chinese threat groups are known for rapid intrusions, but they increasingly focus on stealth and operational security too.

On May 24, 2023, cybersecurity agencies from the U.S., Australia, Canada, New Zealand, and the UK issued a joint cybersecurity advisory about hostile cyber activity it attributed to a People's Republic of China (PRC) state-sponsored threat group that CTU researchers track as BRONZE SILHOUETTE. The threat group has conducted cyberespionage operations against U.S. government and defense organizations since 2021.

One of the most noteworthy aspects of the group's intrusions is its abuse of native tools on victims' systems to achieve its objectives. This approach is known as 'living off the land.' The group hides its activities as much as possible. It also moves rapidly, spending just 90 minutes inside one compromised network before stealing the targeted database.

Secureworks incident responders have investigated several BRONZE SILHOUETTE intrusions since 2021. In addition, multiple other Chinese threat groups tracked by CTU researchers have used living-off-the-land techniques for years. As a result, Secureworks had existing detections for the types of activity described in the advisory.

Chinese cyberespionage efforts have been highlighted in a series of U.S. indictments against Chinese nationals and in publications by numerous organizations. The threat actors are likely under increased pressure from Chinese leadership to avoid public scrutiny, driving their focus on stealth.

What you should do next:
Review Secureworks reporting on these attacks and ensure that your monitoring can detect living-off-the-land techniques.

CYBER RISK FROM THE WAR IN UKRAINE REMAINS FOCUSED ON THAT REGION

Russian cyber hostilities continue to focus primarily on Ukrainian targets, but organizations with links to Ukraine should ensure they have protections in place.

Ukraine began its counteroffensive against Russia in June 2023. This effort focuses on regaining territory taken by Russia in 2022 and during Russia's invasion of Crimea in 2014. At the end of June, Ukraine's deputy defense minister described Ukrainian advances as slow. The West's support of Ukraine via supplies of weaponry, training, and intelligence will likely continue as the war persists.

Russia has conducted offensive cyber operations using state-sponsored threat groups and patriotic hacktivist groups. In mid-June, two self-described pro-Russia hacktivist groups, alongside someone claiming to represent a defunct ransomware group, promised to launch damaging cyberattacks against Western banking institutions. Little damage was reported.

Information from Ukraine's authorities and from intelligence agencies suggest that Russia continues to focus a large proportion of its cyber activities on targeting government entities, humanitarian relief organizations, non-governmental organizations (NGOs), and intergovernmental organizations (IGOs) located in or connected to Ukraine. Hostile activities include destructive wiper attacks, distributed denial of service (DDoS) attacks, and cyberespionage.

CTU researchers are not aware of cyberattacks conducted against Western organizations in direct response to the counteroffensive. However, CTU researchers continue to monitor for indications of Russian cyber activity. In 2022 and the first half of 2023, Secureworks incident responders assisted customers impacted by Russian cyberespionage activity. There is currently no end to the war in sight. As a result, organizations that operate in Ukraine or its neighboring countries, or that provide direct or overt support to Ukraine, will likely remain at risk.

What you should do next:
Assess your relationship to Ukraine or to efforts supporting Ukraine in the war. Maintain good cyber hygiene, consider DDoS mitigation services, and rehearse business continuity plans.

INITIAL ACCESS BROKERS CONTRIBUTE TO THE RISE IN RANSOMWARE ATTACKS

Ransomware attacks are on the rise again. Initial access brokers play an essential role in facilitating the spread of ransomware, so hampering their activities helps reduce the threat.

CTU analysis of the GOLD MELODY threat group revealed that it is likely a prolific initial access broker (IAB). IABs have an essential role in the ransomware ecosystem. They sell access to compromised organizations for other cybercriminals to exploit, often in ransomware attacks. CTU researchers discovered that GOLD MELODY frequently searched for vulnerabilities in unpatched internet-facing servers to exploit as an initial access vector.

Specialist search engines like Shodan make it very simple for IABs and other threat actors to identify vulnerable servers and unpatched internet-facing devices. For example, a major firewall vendor patched a vulnerability in its firewall operating system in mid-June. As of the end of June, barely 30 percent of vulnerable firewalls had been patched by the end of the month and Shodan identified the vulnerable devices.

After a brief reduction in activity in early 2022, ransomware attacks are again increasing. Leak site data suggests that the number of attacks per month could be at record levels. Dwell times remain low, with encryption sometimes happening in a matter of hours after initial access. As a result, network defenders have limited time for detection.

Perimeter and endpoint monitoring are essential for detecting unauthorized access attempts from IABs and for stopping malicious activity after a threat actor has compromised the network. However, it is just as important to address initial access vectors. For example, GOLD MELODY's reliance on exploiting vulnerabilities in unpatched internet-facing servers reinforces the importance of robust patch management.

What you should do next:
Patch and protect internet-facing devices, and implement multi-factor authentication.

CONCLUSION

The motivation for cyberattacks varies: espionage, financial gain, or destructive impact. Threat actors strive to hide their activities, at least until their goal has been achieved. Organizations must implement continuous and comprehensive monitoring for unusual activity such as threat actor tooling or suspicious use of system resources.

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