Secureworks®

THREAT INTELLIGENCE EXECUTIVE REPORT

Volume 2023, Number 2

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

- Shifting the liability for software security bugs?
- China is rated a higher-priority threat than cybercrime
- "Ignorance is no defense" principle underpins U.S. cyber sanctions

SHIFTING THE LIABILITY FOR SOFTWARE SECURITY BUGS?

Making software vendors legally liable for software vulnerabilities could go a long way toward improving security for customers, but it may prove difficult to implement.

One striking aspect of the U.S. National Cybersecurity Strategy that was under development during the reporting period and announced by the Biden administration at the beginning of March 2023 is the intent to shift the liability for insecure software development onto the vendor. Currently, software users bear the cost when major software vulnerabilities are identified and exploited through no fault of their own. The strategy describes how the U.S. government will work with Congress to develop legislation that holds software vendors responsible for failures in their duty of care toward software users. The strategy also encourages coordinated vulnerability disclosure and promotes the development of software bills of materials (SBOMs). SBOMs provide a formal record of the details and supply chain relationships of various components used in building software. SBOMs also contribute toward identifying and mitigating risk in unsupported software, and they encourage investment in secure software development resources.

Organizations will undoubtedly welcome improvements in the security of software that they purchase and run within their environments. Too often, threat actors rapidly weaponize newly discovered vulnerabilities and compromise hundreds or even thousands of corporate and personal systems. In 2022, one third of Secureworks incident response engagements revealed exploitation of vulnerabilities in internet-facing devices as the initial access vector. It makes logical sense that the responsibility for writing secure code should belong to the software vendor rather than expecting end-users to bear the burden of compensating controls.

The strategy acknowledges that one potential unintended side effect could be to constrain innovation. Presumably guidelines will have to be established for which flaws a software vendor could reasonably be expected to proactively identify and fix. Increased code inspection adds time and cost. Vendors will almost certainly pass this cost to their customers, and the inspections will likely not completely prevent code from being shipped with security flaws. In addition, software vendors may lobby to challenge measures that increase their operating costs, encourage more public scrutiny of their intellectual property, and put them at a disadvantage compared to software vendors that are not subject to U.S. legislation. However, the inclusion of similar goals in the draft of the European Union's proposed Cyber Resilience Act may reduce the impact of some of these objections.

The impact to vendors depends on how the strategy is implemented. If executed as currently described, the strategy could force a seismic shift in software development practices and the security of the information technology ecosystem. However, there is a long way to go before new legislation is introduced, leaving plenty of opportunity for these measures to become more palatable for major software vendors and their advocates.

What you should do next:
Understand the core components of the U.S. National Cybersecurity Strategy and their implications for your security program.

CHINA IS RATED A HIGHER-PRIORITY THREAT THAN CYBERCRIME

Chinese cyber activity must not be viewed in isolation from the country's political and economic goals. Monitoring and understanding these goals helps organizations mitigate risk from Chinese cyber activity and ensures that cyber defense strategies are appropriate and current.

The Annual Threat Assessment of the U.S. Intelligence Community published in February emphasizes the magnitude of the cyber threat posed by China. The same conclusion is present in the U.S. National Cybersecurity Strategy, which calls China the "broadest, most active, and most persistent" threat to the U.S. government and private sector, even worse than cybercrime. Secureworks observations support these assessments: in 2022, Chinese threat actors were responsible for over 90% of the state-sponsored activity investigated by incident responders.

Chinese cyberespionage activities aimed at non-domestic targets have two primary focuses: gathering political and military intelligence and supporting China's economic development objectives. Intellectual property theft is a major part of the second focus. Depending on the Chinese leadership's prevailing goals, the balance and geographic focus of economic and political espionage may shift for individual threat groups or for Chinese threat activity as a whole. For example, the Chinese state-sponsored BRONZE PRESIDENT threat group largely focused on Southeast Asian targets between 2019 and 2021. In 2022, it turned its attention to cyberespionage against European targets, likely to gather intelligence related to the war in Ukraine. The worsening of China's bilateral relationships with the U.S. and its allies has likely also influenced tasking. However, China still conducts a considerable amount of hostile cyber activity toward neighboring countries, as well as continued monitoring of countries involved in its Belt and Road Initiative soft power strategy.

Chinese cyberespionage also focuses on areas of specific economic concern to the country. Although the Chinese economy grew 3% in 2022, it was one of the slowest rates of growth in the past 30 years and significantly missed its target of 5.5%. The target for 2023 is 5%. This potentially ambitious target amid worsening trade relationships with the West will likely increase the pressure on economic espionage operations.

Chinese threat groups predominantly compromise networks by exploiting known vulnerabilities in internet-facing devices. CTU researchers are also observing an increasing shift toward Chinese threat actors using plausibly deniable tactics and ambiguous infrastructure to complicate attribution, including the use of ransomware attacks to mask cyberespionage activity.

What you should do next:
Understand the strategic priorities of countries such as China and consider whether your intellectual property and other data might be of interest. Know where that information is located on your network and ensure it is adequately protected with up-to-date cyber defenses.

"IGNORANCE IS NO DEFENSE" PRINCIPLE UNDERPINS U.S. CYBER SANCTIONS

The U.S. government expects organizations with U.S. interests to understand and respect the demands of OFAC sanctions and associated regulations when ransomware crises occur.

On February 9, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), in coordination with UK government agencies, announced sanctions against seven current and former members of the Russia-based GOLD BLACKBURN cybercrime group that operates the TrickBot malware. The sanctions require freezing bank accounts, cryptocurrency wallets, funds, and other economic assets associated with the designated individuals.

TrickBot (formerly the Dyre banking trojan) was modular malware that ran on a network of infected systems (a 'botnet') and delivered additional malware used in ransomware attacks. GOLD BLACKBURN abandoned the TrickBot malware and botnet in March 2022 following data leaks and competition from other crimeware. Although the sanctioned individuals may no longer be operating TrickBot, they are likely still involved in cybercrime.

OFAC sanctions prohibit transactions with the designated individuals "by U.S. persons [(a much broader legal category than U.S. citizens)] or within the United States." Persons who ignore these sanctions and foreign financial institutions that knowingly facilitate transactions could be sanctioned. As a result, sanctions against ransomware groups can impact victims of ransomware attacks as well as organizations that facilitate payments on their behalf, such as financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response.

These sanctions name individuals but not specific ransomware operations. In theory, this distinction could reduce the risk of breaching sanctions because it is almost impossible to know which individuals receive a ransom payment. However, OFAC regulations operate on the basis that "ignorance is no defense," so organizations considering paying a ransom may be expected to demonstrate that they attempted to verify that sanctioned individuals were not involved in the attack.

Whether an organization chooses to pay a ransom is an individual business calculation. This calculation should include monitoring OFAC sanction designations and regulations, as well as performing due diligence for any intended payment. As the National Cybersecurity Strategy increasingly focuses on "more sustained and effective disruption of adversaries," the U.S. will likely continue to leverage sanctions to achieve this goal and expect the same actions from its allies.

What you should do next:
Review your incident response plan and verify that it considers regulatory imperatives such as sanctions. Checking in advance will save valuable time during a cyber incident.

CONCLUSION

The new U.S. National Cybersecurity Strategy provides essential insight into the biggest cyber threats that affected organizations in early 2023. These threats will continue to have widespread impact. For CISOs and other senior executives not just in the U.S. but also around the world, the strategy provides valuable guidance for driving effective and impactful cybersecurity strategies.

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

