Secureworks®

THREAT INTELLIGENCE EXECUTIVE REPORT

Volume 2024, 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. Based on observations in September and October, CTU™ researchers identified the following noteworthy issues and changes in the global threat landscape:

- Novel social engineering ploys form basis of attacks
- Prompt patching is vital, especially on the network perimeter
- Securing the ICS attack surface reduces risk

Novel social engineering ploys form basis of attacks

Cybercriminals are using increasingly innovative and targeted social engineering techniques to dupe their victims.

Threat actors use social engineering techniques to trick victims into helping them to access systems, providing an alternative to technical methods such as exploiting vulnerabilities or stealing credentials. Phishing is a longstanding method of social engineering, but attackers continue to develop ingenious ploys.

In multiple incidents, threat actors presented fake human verification prompts to individuals searching for streaming videos. Visitors to the malicious websites were challenged to prove they were a human by entering a sequence of keyboard combinations that copied and executed malicious PowerShell to deliver infostealers.

In a CEO fraud example, the attacker conducted open-source research and obtained the victim's phone number. They then posed as a senior executive to contact the victim via WhatsApp about an urgent financial transaction before moving their communication to email. The threat actor adopted several personas while communicating with the victim to make their request more convincing, ultimately leading the victim to approve a payment to an attacker-controlled account.

In attacks that were likely intended to end in ransomware deployment, threat actors bombarded employees of the target organizations with large amounts of spam email. They then contacted the victims by phone or via Teams, offering technical support to resolve the spam problem. The "solution" involved downloading a remote management tool that gave the threat actors remote access to the victims' systems and corporate networks.

There have been several third-party reports of these spam attacks in recent months, which may indicate that ransomware operators are finding this technique effective. While the majority of cybercrime is opportunistic and exploits exposed vulnerabilities or stolen credentials, the social engineering aspect of these incidents suggests that the targets were preselected. The criteria or method used to identify potential targets is unknown.

Social engineering attacks are typically not detectable by endpoint solutions until malware is delivered. The use of artificial intelligence to create deep fakes will only increase the threat. Educating employees to recognize common and emerging social engineering techniques is important for protecting corporate assets.

What You Should Do Next
Stay abreast of innovative social engineering tactics to incorporate into security awareness training, and empower employees to question and report suspicious activity.

Prompt patching is vital, especially on the network perimeter

Quickly addressing vulnerabilities in internet-facing devices is an essential defense against ransomware attacks.

Analysis of an October network compromise that involved deployment of Black Basta ransomware indicated that the attackers likely exploited a SonicWall VPN vulnerability for initial access. SonicWall publicly disclosed and patched this vulnerability in August 2024 and then reminded users about patching in early September due to likely active exploitation. In early October, reports warned that Akira and Fog ransomware operators were exploiting the vulnerability.

This widely publicized vulnerability was assigned a critical severity in the Common Vulnerability Scoring System (a CVSS score of 9.8 out of 10). The severity score differs from risk, which is a calculation specific to each organization. Both measurements are affected by ease of access. A critical, easy to access vulnerability on an internet-facing device or system poses a much greater risk to the organization than a critical vulnerability on a system that is not externally accessible.

Implementing and adhering to a patching program that promptly and comprehensively addresses vulnerabilities can be difficult. Organizations almost always have to prioritize some patches over others regardless of how much publicity a vulnerability receives. Risk should be an essential consideration when calculating priority. One of the most important risk factors is whether the vulnerability affects an edge device. Threat actors often use easily accessible search tools to identify insecure implementations of internet-facing systems, either when a new vulnerability is publicly disclosed or to opportunistically discover organizations that have not hardened their perimeter defenses.

In addition to patching, organizations can harden their perimeter by ensuring that VPNs and other externally accessible devices are protected with multi-factor authentication.

What You Should Do Next
Audit your edge devices and remove internet access from those that do not need to be externally accessible.

Securing the ICS attack surface reduces risk

Minimizing the attack surface in industrial control system facilities reduces opportunities for threat actors to conduct disruptive attacks.

Industrial control system (ICS) facilities, which are often part of countries' critical national infrastructure, remain top targets for hacktivists. Although CTU researchers determined that there was lack of evidence to support pro-Russia hacktivist group Z-Pentest's boasts of responsibility for a September 2024 attack against a water treatment facility in Arkansas City, Kansas, the group may have attacked other ICS facilities in Taiwan, Poland, Romania, Belgium, and Italy since then. The claims spurred the U.S. Cybersecurity and Infrastructure Security Agency (CISA) to remind operators of ICS and operational technology (OT) devices in critical infrastructure sectors about the importance of cybersecurity and about CISA's May 2024 fact sheet containing mitigations to defend against attacks.

Critical national infrastructure also remains of considerable interest to state-sponsored threat actors from Russia, China, North Korea, and Iran for cyberespionage or disruptive attacks. Since the outbreak of the Israel-Hamas war, ICS systems with Israeli links have suffered attacks from personas that are likely affiliated with Iran, such as Cyber Av3ngers. In Ukraine, Russia has consistently attempted to disrupt or destroy Ukrainian ICS operations.

Hardening systems, selecting secure configuration settings, and reducing the attack surface remain essential defenses against state-sponsored threat actors and hacktivists. These approaches are vital for organizations in all sectors, not just ICS facilities, and it is particularly important to focus on systems on the network perimeter. CISA and equivalent agencies in other countries offer useful guides, and organizations should regularly check that they are following best practices.

✓ **What You Should Do Next**
Evaluate your attack surface to identify opportunities to reduce it.

Conclusion

Threat actors continue to develop new ways of compromising organizations. However, organizations can strengthen their cyber defenses by minimizing their attack surface, prioritizing and patching vulnerabilities in a timely manner, and conducting employee training. Keeping up to date on emerging threat actor tactics, techniques, and procedures and implementing guidance about best practices are important strategies for mitigating 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 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 thousands of 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