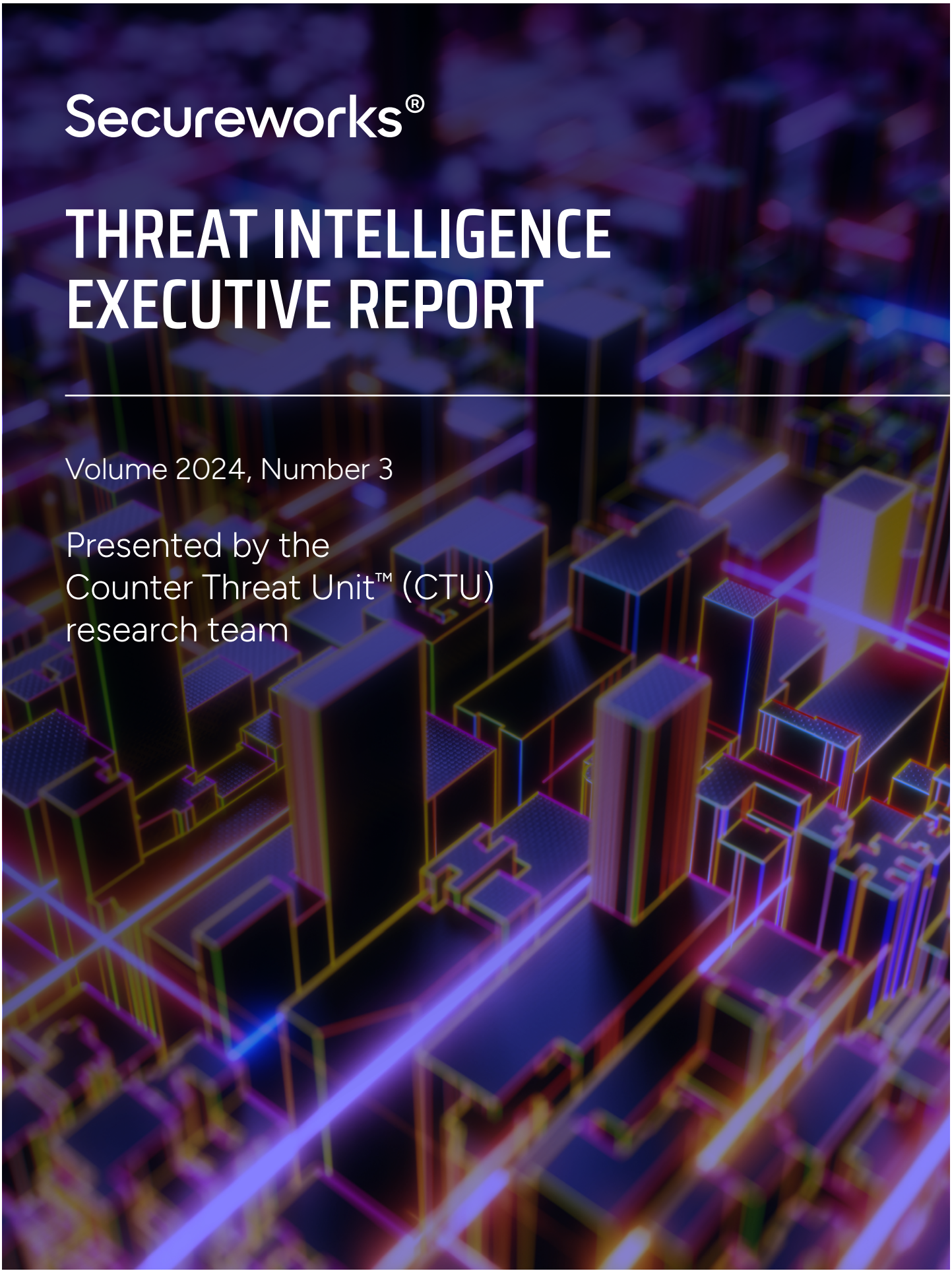
Secureworks®

THREAT INTELLIGENCE EXECUTIVE REPORT

Volume 2024, Number 3

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 March and April CTU™ researchers identified the following noteworthy issues and changes in the global threat landscape:

- Threat actors manipulate victims in social engineering attacks
- Open-source tampering compromises supply chain
- Threat actors are living on the edge

THREAT ACTORS MANIPULATE VICTIMS IN SOCIAL ENGINEERING ATTACKS

Flattery, the promise of employment, or the illusion of urgency can help threat actors turn employees and contractors into an organization's weakest link, tricking victims into providing access to corporate secrets.

In March, CTU researchers continued to investigate a North Korean campaign that targeted software developers for espionage purposes. The threat actors contacted developers via freelance job platforms, conducted interviews, and convinced the candidates to access a repository and download a task containing hidden malware. The intention was likely to either steal information from the compromised device or to leverage the compromise to access corporate networks.

The campaign has been widely tracked as 'Contagious Interview' and continues the employment-related theme used in the North Korean 'Dream Job' campaign that has been running since at least 2019. During the Dream Job campaign, North Korean threat actors attempted to infiltrate U.S. and Israeli defense contractors by conducting social engineering attacks via LinkedIn using fake job offers.

Social engineering is used by both state-sponsored and financially motivated threat groups. For example, Iranian state-sponsored threat groups have a long history of leveraging fake social media personas to target a broad range of individuals and organizations to satisfy intelligence-gathering objectives. Unsolicited outreach can be flattering or intriguing, especially if it is complimentary, appears to come from an attractive individual, or offers tangible or intangible benefits, such as the chance to share knowledge in an area of expertise. Threat actors can use these tactics to obtain credentials for additional phishing activity and to collect bulk data that can help inform intelligence requirements.

Members of the GOLD HARVEST cybercriminal group have called corporate help desks and claimed to be employees who urgently need their credentials reset. The threat actors then attempted to leverage the network access in ransomware attacks. GOLD HARVEST is not the only group to use phone-based social engineering attacks. However, unlike groups that are located in Russia and Commonwealth of Independent States (CIS) countries, GOLD HARVEST appears to include several native English-speaking members. Their telephone-based social engineering is more credible and effective for targeting Western organizations.

The most effective defense against these attacks is training all employees to recognize online and phone-based social engineering. Organizations should also implement procedures for employees to promptly report attempts to internal security teams.

What you should do next:
Train help desk staff to verify employees' identities before updating accounts, and empower them to refuse suspicious unverifiable requests.

OPEN-SOURCE TAMPERING COMPROMISES SUPPLY CHAIN

Software can contain components from a wide range of sources. Some of those components may have been tampered with to leave backdoors that threat actors can later use to conduct attacks.

On March 29, Red Hat released an advisory warning that malicious code with backdoor functionality had been discovered within the open-source XZ (xz-utils) data compression utility project. Investigations revealed that earlier in the year, a contributor to the open-source project had committed malicious files in the guise of test cases to verify the library's functionality, as well as a build script containing malicious commands. These malicious components were then included in the next update, functioning as a passive backdoor. The threat actor behind this activity had used several personas to lobby for acceptance as a contributor to the project and for the malicious update to be included in Linux distributions.

This example illustrates risks of the open-source system. Open-source projects are frequently incorporated into other software. Many of these projects are managed by volunteers who may welcome contributions by industry participants. If a project becomes dormant due to lack of volunteer resources, the temptation to accept offers of help, especially when active lobbying occurs, must be considerable. However, if components are compromised, it creates considerable potential for downstream supply chain risk.

In April, the OpenJS Foundation revealed that it too was targeted by individuals seeking privileged access to its project. Their blog post about the attempt includes a helpful checklist of suspicious behaviors that project maintainers should be wary of, including manipulative social engineering techniques.

Although attribution is unclear, the XZ tampering reinforces the amount of effort threat actors are putting into developing code-based supply chain attacks. It is important for organizations to understand the components in the software deployed in their environments. The emphasis placed by the Biden-Harris Administration on encouraging the use of software bills of materials (SBOMs) will help.

What you should do next:
Enhance your visibility of your organization's attack surface by identifying software and platforms use open-source components and then document with SBOMs.

THREAT ACTORS ARE LIVING ON THE EDGE

Organizations should always base patch priorities on business risk. But internet-accessible edge devices on the organization's network perimeter should automatically be prioritized, especially when exploit code is available.

Vulnerable internet-facing edge devices continue to act as magnets for threat actors, sometimes even before the vulnerabilities are disclosed. On April 12, Palo Alto Networks published mitigation guidance for a critical, zero-day vulnerability impacting PAN-OS firewall software (CVE-2024-3400). The vulnerability was already under limited exploitation by a likely state-sponsored threat actor who targeted specific victims with precision and efficiency. Palo Alto initially released limited information about the vulnerability to delay wider exploitation while it developed patches, but researchers' publication of a proof-of-concept exploit on April 16 led to wider exploration and exploitation of the vulnerability.

On April 24, British, Australian, and Canadian security agencies warned that a threat actor was targeting virtual private network (VPN) services used by government and critical national infrastructure networks globally. The impacted products were primarily Cisco ASA devices vulnerable to CVE-2024-20353 and CVE-2024-20359. This campaign, which Cisco Talos dubbed ArcaneDoor, is thought to be the work of a Chinese state-sponsored threat actor.

There is no evidence that the same threat group was responsible for both campaigns. However, both campaigns involved targeted attacks on perimeter devices followed by public disclosure of the vulnerability and then wider exploitation. CTU researchers regularly observe threat actors on underground forums actively discussing topical vulnerabilities and how to exploit them, as well as sharing advice and exploit code. Threat actors also advertise credentials for edge devices, which enable attackers to compromise networks without exploiting a vulnerability.

It is essential for organizations to patch and mitigate vulnerabilities in internet-facing devices in a timely manner to limit the risk and impact of exploitation. Organizations should also plan for rapid remediation, even if they do not consider themselves a target of the initial exploitation campaign. It is also important to monitor the situation, as vendors' mitigation advice can change as more information about exploitation comes available. For example, initial advice about temporarily disabling device telemetry as a workaround for CVE-2024-3400 was rescinded a few days later for being ineffective. Organizations should also monitor, log, and analyze traffic on both sides of perimeter devices to identify signs of actual or attempted compromise.

What you should do next:
Assume that unpatched systems have been breached, and respond accordingly.

CONCLUSION

Threat actors focus on security weaknesses to attack organizations. These weaknesses can be employees who are eager to please, in a hurry, in need of help, or simply happy to talk. Other times, threat actors target edge devices on the network perimeter that are unpatched against a vulnerability for which exploit code is available. A successful defense strategy is multi-pronged but always includes detecting and stopping threat actors in the early stages of a compromise.

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 over 4,000 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

