Secureworks®

THREAT INTELLIGENCE EXECUTIVE REPORT

Volume 2024, Number 5

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

- Chinese government wants first access to zero days
- North Korean workers infiltrate organizations
- The risk from ransomware remains high

Chinese Government Wants First Access to Zero Days

China requires its security researchers to report vulnerability discoveries to the government, giving Chinese threat groups a head start with zero-day exploits.

Microsoft's August 2024 Patch Tuesday release featured a critical Windows vulnerability (CVE-2024-38063) that was described as wormable and zero-click. Those two qualities mean that it could infect a system and spread to other systems without interaction from the victim, which resulted in it being assigned a near-maximum severity rating. The issue was discovered by China-based security researcher XiaoWei, who ranks second on Microsoft's most 100 Most Valuable Researchers (MVRs) list for 2024. Chinese security researchers regularly report vulnerabilities to companies such as Microsoft. However, vendors are not the only recipients of these notifications.

Chinese researchers are legally obligated to disclose security vulnerabilities to the Chinese government within two days of discovery. This early insight could allow the government to task state-sponsored threat groups with exploiting the issues before vendors issue patches. Chinese state-sponsored threat groups were reportedly the most prolific exploiters of zero-day vulnerabilities in 2023. These groups have continued to exploit zero-day vulnerabilities through 2024, often targeting internet-facing perimeter devices.

This rapid and prolific exploitation highlights the importance of prompt patching and additional layers of defense. Defenses include implementing comprehensive monitoring and detection coverage across endpoints, the network, and cloud.

What You Should Do Next

Ensure that your organization's patching program considers all relevant risk factors, including implications related to who discovered the vulnerability.

North Korean Workers Infiltrate Organizations

Organizations are unknowingly hiring fraudulent North Korean IT workers as remote employees.

Revenue generation is a prime objective for North Korean threat actors who have stolen billions of dollars in cryptocurrency and have conducted numerous ransomware attacks. In another scheme, skilled North Korean IT workers, often living in China and Russia, have fraudulently obtained remote employment with Western companies.

In late July, U.S. organization KnowBe4 revealed how a newly recruited remote working software engineer attempted to upload malware immediately after receiving their corporate laptop. An investigation into the suspicious activity revealed that the company had inadvertently employed a North Korean threat actor. Other companies have had similar experiences. In May 2024, the U.S. Department of Justice (DOJ) unsealed court documents detailing how thousands of North Korean IT workers allegedly posed as U.S. citizens and residents to defraud over 300 companies and generate at least $6.8 million USD of revenue for North Korea, evading U.S. sanctions.

On August 8, a Tennessee man was charged with helping North Korea generate revenue for its weapons program. The indictment revealed that the individual operated a laptop farm running remote desktop applications that made North Korean workers in China appear to be located in the U.S. North Koreans may also use stolen identities, artificial intelligence and deep fake technology, and cloned resumes to fool recruiters. Candidates may provide references for each other and share phone numbers.

Organizations that employ North Korean IT workers risk being defrauded by these employees. Companies that operate in the cryptocurrency sector may experience significant losses. Compromised organizations could also face charges of sanction breaking.

What You Should Do Next

Incorporate the U.S. Federal Bureau of Investigation (FBI) guidance about recognizing North Korean IT workers into your recruitment practices to detect fraudulent applicants and mitigate this risk. Verify that external recruitment services are aware of the risk.

The Risk From Ransomware Remains High

Industry research shows no signs that the danger from ransomware is dropping, despite law enforcement wins.

Recent ransomware trends reports suggest that while law enforcement efforts have disrupted ransomware operations and fragmented the ransomware ecosystem, there is little evidence that attacks have significantly slowed. The overall level of business risk from ransomware is either steady or rising.

A Chainalysis investigation of cryptocurrency payments to blockchain wallets controlled by ransomware actors revealed an increase of approximately two percent in the first half of 2024 compared to the same period in 2023. While that

percentage appears minor, it is likely that Chainalysis does not have full visibility of wallet transactions and the actual increase is higher.

The size of ransom payments could be a factor in this shift. The median payment for what Chainalysis calls "the most severe ransomware strains" rose from just under $200,000 USD in early 2023 to $1.5 million in mid-June 2024. Zscaler reported that one organization allegedly paid a ransom of $75 million to the Dark Angels ransomware group in early 2024.

Research indicates that overall breach costs have risen. According to IBM, the global average cost of a breach is $4.88 million in 2024, up ten percent from the previous year. Remediation costs are often higher than ransom demands. IBM's research found that victims saved an average of $1 million, excluding ransom costs, by involving law enforcement after the attack.

Interestingly, Coveware discovered that over ten percent of ransomware attacks they investigated in the second quarter of 2024 did not appear to be affiliated with a known ransomware operation. Ransomware actors typically reveal their affiliation via a branded encryptor, ransom note, or Tor leak site. While some affiliates displaced by law enforcement actions switched to other ransomware schemes, a lack of affiliation indicators in attacks could imply that others have decided that life is simpler without any clear associations with specific ransomware brands.

What You Should Do Next
Review your ransomware incident response plans and store them in a location that would be accessible after a ransomware attack.

Conclusion

Threat actors continue to take advantage of every opportunity to maximize their chances of success. These opportunities could include early access to zero-day vulnerabilities, revenue-earning activities that defraud employers, and new ways of operating in the ransomware landscape. Organizations should use multiple layers of defense to strengthen their processes and protect their endpoints, networks, cloud resources, and identity implementations.

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

