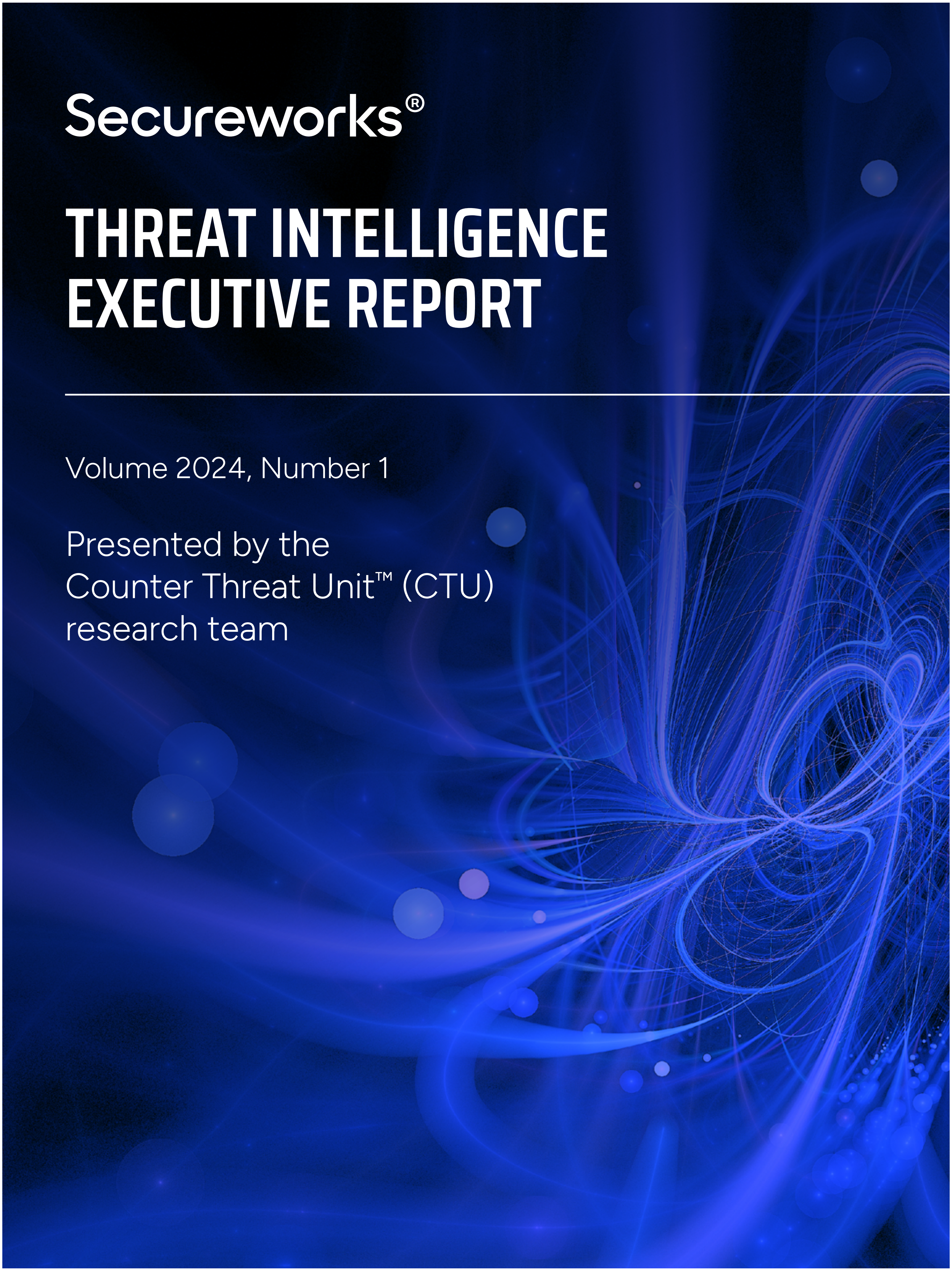
Secureworks®

THREAT INTELLIGENCE EXECUTIVE REPORT

Volume 2024, Number 1

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

- High-profile vulnerabilities continue to attract threat actors
- Unchanged default passwords open doors for attackers
- IRON FRONTIER used spearphishing against British politicians

HIGH-PROFILE VULNERABILITIES CONTINUE TO ATTRACT THREAT ACTORS

Patching a vulnerability promptly is best, but late is better than never.

In early November, CTU researchers warned customers that LockBit ransomware affiliates were exploiting a critical vulnerability affecting Citrix NetScaler appliances. The vulnerability, dubbed 'Citrix Bleed', provides an example of how exploitation of high-profile vulnerabilities can grow, increasing the level of risk to organizations.

Citrix disclosed Citrix Bleed in early October. A proof-of-concept exploit was released in late October. On October 31, Mandiant claimed to have detected exploitation as early as August. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added the vulnerability to its Known Exploited Vulnerabilities (KEV) catalog on October 18 and released patching guidance in early November. Ransomware and state-sponsored actors continued to exploit the vulnerability throughout November, prompting CISA to publish an advisory in late November.

The speed and order of the discover-warn-exploit cycle depends on factors such as who first discovers the vulnerability and how quickly (if ever) the vendor issues a fix. However, one aspect is relatively consistent: exploitation starts to happen days or even hours after threat actors find out about the vulnerability. The publication of a proof-of-concept exploit that explains how to abuse the vulnerability only hastens that step. Threat actors can use specialized search engines that help them identify unpatched instances of the vulnerable system.

CTU researchers regularly urge organizations to apply appropriate patches or mitigations as soon as they are available. 'Scan-and-exploit' is one of the top ways that ransomware actors gain initial access to systems, making timely patching of internet-facing systems essential. We understand that patching is a complex and costly process and can pose difficulties, so we also advise organizations to prioritize patching according to their business risk profile. That prioritization requires assessing the amount of threat a vulnerability poses to the organization. Considerations should include factors such as whether the vulnerability affects an internet-facing system, if authentication is required to access the system, and if exploit code is publicly available.

This assessment cannot be based on a one-time static calculation. The level of threat that a specific vulnerability poses can quickly change dramatically, and patching prioritization must adapt accordingly. A low-severity vulnerability that initially appeared to be a minor threat can suddenly become far more dangerous. For example, threat actors could 'chain' two low-severity Microsoft Windows vulnerabilities disclosed in 2023 to conduct a covert attack without needing to trick the victim into clicking a malicious link.

In addition, threat actors continue to search for unpatched vulnerabilities years after they are disclosed. Every year, CISA publishes a list of 'top routinely exploited vulnerabilities' for the previous year. Vulnerabilities from 2019 and earlier regularly rank high on the list.

Evaluating and addressing the threats an organization faces is not a one-time exercise. Citrix Bleed is just one example of why regular and timely patching is essential.

✓ **What you should do next:**
Use CISA's KEV catalog and 'top routinely exploited vulnerabilities' list to inform your vulnerability and patch management processes.

UNCHANGED DEFAULT PASSWORDS OPEN DOORS FOR ATTACKERS

Keeping the manufacturer's default password leaves systems open to attack.

In November, CISA warned that Iranian threat actors were actively exploiting Unitronics programmable logic controllers (PLCs) used in the water and wastewater systems sector. The supposed hacktivists (a probable front for Iranian state-sponsored threat actors) targeted users of the Israeli-made equipment in multiple countries. One of CISA's recommendations was to change all default passwords on the controllers.

It is common for internet of things (IoT) and operational technology (OT) systems to ship with default credentials that customers are expected to change before deployment. However, as CISA stated in guidance aimed at manufacturers of these systems, "Years of evidence have demonstrated that relying upon thousands of customers to change their passwords is insufficient…" Some default passwords are hard-coded and cannot be changed. In addition, lists of default passwords are easy to find on the internet. It is too early to tell if or when manufacturers will respond to this guidance. However, threat actors, whether hacktivists, state-sponsored groups, or cybercriminals, will continue to target IoT and OT systems users.

Default passwords make it easier for threat actors to compromise systems. Organizations should replace default passwords with strong passwords as soon as they can. They should also further protect their systems with additional controls such as multi-factor authentication (MFA).

✓ **What you should do next:**
Establish and enforce an organizational policy to identify and change default passwords.

IRON FRONTIER USED SPEARPHISHING AGAINST BRITISH POLITICIANS

The Russian threat group conducts cyberespionage attacks to support Russia's political and military activities. The UK is just one of its targets.

Each of Russia's three intelligence agencies operates or works with threat groups that conduct cyberattacks against Russia's enemies. In December, the UK, U.S., and allies tied the IRON FRONTIER threat group (also known as Star Blizzard) to Russia's Federal Security Service (FSB) Center 18. IRON FRONTIER focuses on gathering foreign intelligence and has been linked to spearphishing attacks against military and government organizations, journalists, and think tanks in Europe, the U.S., and Russia's near abroad. It steals credentials to gain access to sensitive email communications and documents.

According to the UK government, the group was behind a sustained effort to target the UK democratic process, including cyberattacks on UK civil servants, Members of Parliament, journalists, and non-governmental organizations. Some attacks targeted email accounts belonging to British politicians and high-profile Brexit campaigners. Previous U.S. targets included staff at three national laboratories: Argonne National Laboratory, Brookhaven National Laboratory, and Lawrence Livermore National Laboratory. IRON FRONTIER's attacks continued through 2023.

Spearphishing is used by both cybercriminals and state-sponsored threat actors. It often involves research to ensure that the initial outreach is tailored to avoid suspicion and be as convincing as possible. IRON FRONTIER is known to create email accounts impersonating targets' contacts to boost the appearance of legitimacy. The threat actors may also create fake social media profiles.

User education for all employees, including senior executives, is essential to protect organizations against spearphishing from IRON FRONTIER and other threat groups. However, organizations cannot depend solely on users for their defense. Awareness must be part of a broader set of defenses that include MFA and comprehensive monitoring.

What you should do next:
Review the joint publication tying IRON FRONTIER to the FSB for further details about the threat group's tactics and how to combat them.

CONCLUSION

Whether cyberattacks are opportunistic as in most cybercrime, or targeted for political or military purposes, many threat actors conduct exhaustive preparatory research. This research can involve scanning for unpatched servers, combing through leaks of stolen or default credentials, or investigating potential victims to fine-tune spearphishing attacks. Effective cyber defense strategies are multilayered and include prompt patching, MFA, comprehensive monitoring, and user education to stop threat actors from successfully leveraging their findings.

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