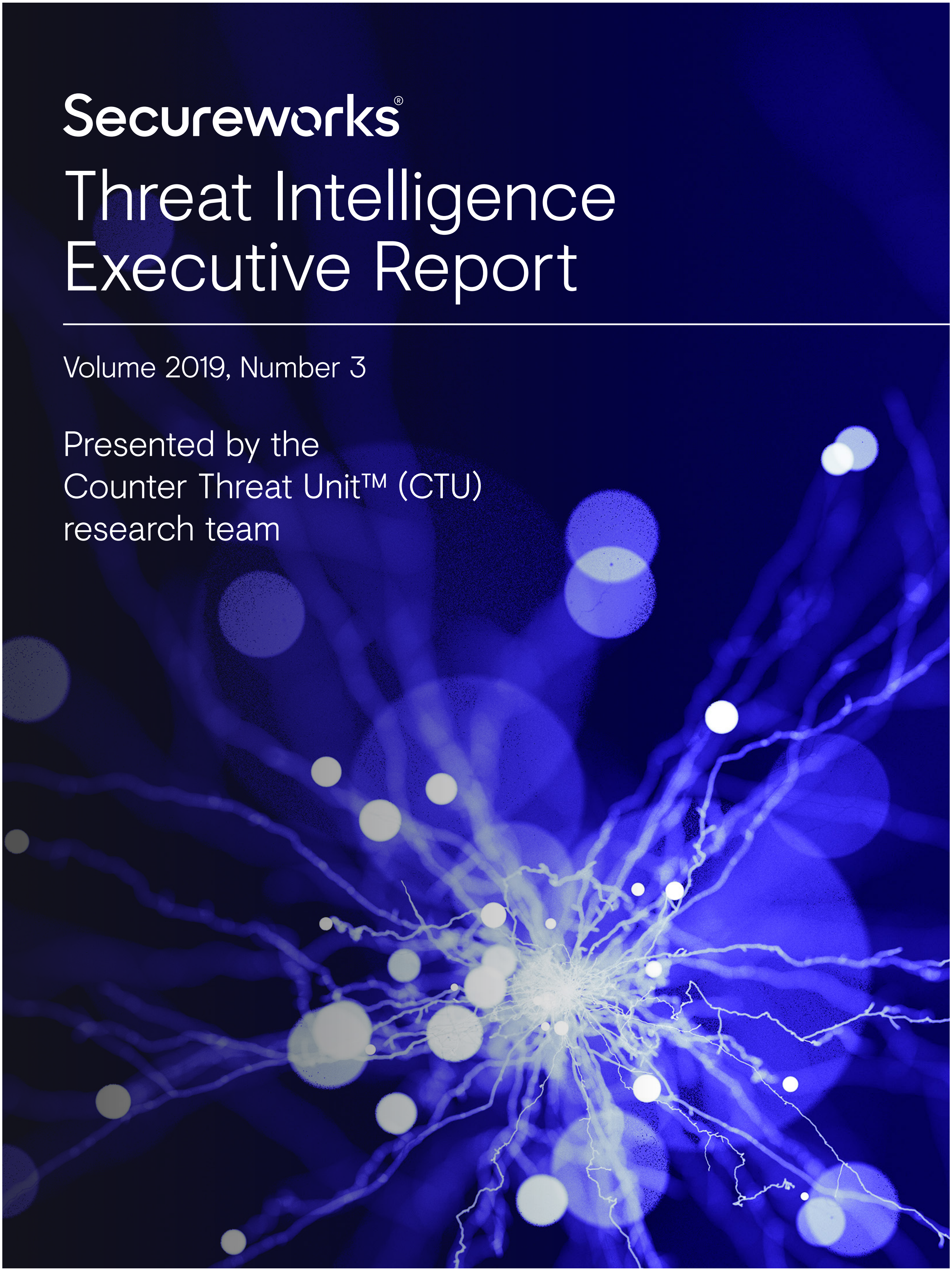
Secureworks®

Threat Intelligence Executive Report

Volume 2019, Number 3

Presented by the Counter Threat Unit™ (CTU) research team



Executive Summary

The Secureworks® Counter Threat Unit™ (CTU) research team analyzes security threats and helps organizations protect their systems. During March and April 2019, CTU™ researchers identified lessons learned and observed notable developments in threat behaviors, the global threat landscape, and security trends:

- LockerGoga attacks reinforced a trend of post-intrusion ransomware.
- Business email compromises increasingly affected organizations.
- Threat actors weaponized and exploited a SharePoint vulnerability soon after it was disclosed.

Post-intrusion ransomware trend continued with LockerGoga attacks

In March, Norway-based aluminum manufacturer Norsk Hydro was severely impacted by a LockerGoga ransomware attack. The malware encrypted and rendered unavailable many systems throughout Norsk's global operation, shutting down several manufacturing plants and requiring several weeks to fully restore operations. LockerGoga was also implicated in the January attack on French engineering consulting firm Altran and the March attacks on U.S.-based chemical manufacturers Hexion and Momentive.

Fundamental security practices can prevent threat actors from accessing a network and conducting post-intrusion ransomware attacks.

These incidents illustrate a continuing trend of post-intrusion ransomware attacks, which include previous U.S. campaigns such as the SamSam attacks that crippled the City of Atlanta's municipal services and Ryuk attacks that affected several media organizations. In these types of attacks, the ransomware deployment is the final stage of a long-running intrusion. Before the ransomware deployment, a threat actor must gain unauthorized access to the target environment by guessing or stealing credentials, exploiting vulnerable Internet-facing systems, or infecting a victim's system with malware. Only then can the threat actor attempt to gain privileged access to the network and use the access to deploy ransomware to as many systems as possible. A large number of systems can become unavailable within a very short period of time, causing significant impact to business operations. These attacks are financially motivated, but it is not clear how many compromised organizations pay the ransom rather than restoring from backups. The increase in these attacks suggests that the threat actors are making a profit, and CTU researchers expect this type of threat to increase.

In these incidents, the threat actor uses commercially available or native system tools and the malware is often relatively unsophisticated. As a result, organizations should implement fundamental security practices to protect against this type of threat:

- Apply multi-factor authentication for Internet-facing systems to prevent threat actors from successfully using stolen credentials.
- Update Internet-facing systems with security updates to address known vulnerabilities.
- Monitor endpoints for unusual user behavior.
- Store system backups in an offline but accessible location so data can be rapidly restored when needed.
- Develop and practice incident response procedures to mitigate the worst effects of a successful ransomware attack.

Business email compromise incidents continued to increase

Business email compromise (BEC) is one of the most lucrative and highest-grossing types of cybercrime, and CTU researchers continued to observe an increase in the number of BEC attacks. According to the FBI's Internet Crime Complaint Center (IC3) 2018 Internet Crime Report, losses from BEC doubled in a year to nearly $1.3 billion in 2018. The growing popularity can be attributed to the low overhead cost, as these attacks rely more heavily on social engineering than technical sophistication. An increasing number of traditional "Nigerian prince" 419 scammers are discovering the ease of BEC and are shifting their attention to business targets.

Organizations should verify requests to modify payment instructions.

Beginning in late 2018, CTU researchers observed an increase of payroll diversion fraud. Unlike conventional BEC attacks that impersonate CEOs or vendors to initiate wire transfers, payroll diversion attacks redirect an employee's pay to attacker-controlled bank accounts. This fraud typically targets employees through phishing emails to acquire login credentials. After obtaining the credentials, the threat actor uses the employee's email account to persuade human resource (HR) personnel to change the employee's bank account details to an attacker-controlled account. The employer then unknowingly begins sending the employee's salary to the threat actor. A variation of the payroll diversion fraud abuses compromised credentials to access self-service payroll systems and update direct deposit information.

Organizations should implement two-factor authentication to prevent unauthorized access to email accounts. Additionally, organizations should establish clear processes for their accounting, finance, HR, or payroll departments to verify requests to modify existing wire transfer instructions or direct deposit details using previously established channels such as a phone number.

Threat actors weaponized recently announced vulnerabilities

Threat actors continued to rapidly weaponize recently announced vulnerabilities, knowing that many organizations take time to patch systems. On February 12, Microsoft disclosed details of a critical SharePoint remote code execution vulnerability (CVE-2019-0604). A publicly available proof-of-concept exploit was published on March 22. In early April, CTU researchers observed threat actors exploiting this vulnerability on SharePoint 2016 servers at a wide range of organizations. The threat actors deployed the China Chopper web shell, which allows an attacker to execute commands on a compromised system and provides a foothold to compromise the wider network.

Delays in applying security updates can allow threat actors to exploit known vulnerabilities.

CTU analysis revealed that the web shell was not immediately used on many of the servers, suggesting that systems were opportunistically compromised. However, approximately three hours after one web shell deployment, the threat actor accessed it to perform reconnaissance on the compromised system. In a possibly unrelated campaign that exploited the same vulnerability, CTU researchers observed attempts to deploy a Cobalt Strike payload using a PowerShell loader. In another incident, a threat actor reportedly initially deployed the China Chopper web shell and then leveraged a PowerShell script to download a previously unobserved malware family.

The large-scale exploitation of CVE-2019-0604 by multiple threat actors shortly after exploit code was published highlights the importance of rapid and effective patching processes, especially for Internet-facing systems. In most cases where threat actors use scan-and-exploit activity to gain initial access to a target, a security update was available for the exploited vulnerability.

Conclusion

As the number of sophisticated attacks increases and threat actors demonstrate greater adaptability, CTU researchers encourage organizations to consider the lessons learned from these incidents when planning and prioritizing cybersecurity strategies and operations. Implementing security best practices could limit the likelihood and impact of many intrusions, and understanding and addressing threat behaviors could help organizations anticipate and disrupt breaches and security incidents.

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 leading global cybersecurity company that keeps organizations safe in a digitally connected world. By combining our visibility into threat behavior across customer environments with our expertise and a powerful processing platform, we help organizations anticipate emerging threats, detect malicious activity in real time, assess risk, and take appropriate action to avoid or mitigate risk of a security breach. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™ www.secureworks.com

Corporate Headquarters
1 Concourse Pkwy NE #500
Atlanta, GA 30328
1.877.838.7947
www.secureworks.com

Europe & Middle East France
8 avenue du Stade de France
93218 Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

Germany
Main Airport Center, Unterschweinstiege 10
60549 Frankfurt am Main
Germany
069/9792-0
www.dellsecureworks.de

United Kingdom
One Creechurch Place, 1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

United Arab Emirates
Building 15, Dubai Internet City
Dubai, UAE PO Box 500111
00971 4 420 7000

Asia Pacific Australia
Building 3, 14 Aquatic Drive
Frenchs Forest, Sydney NSW
Australia 2086
1800 737 817
www.secureworks.com.au

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp