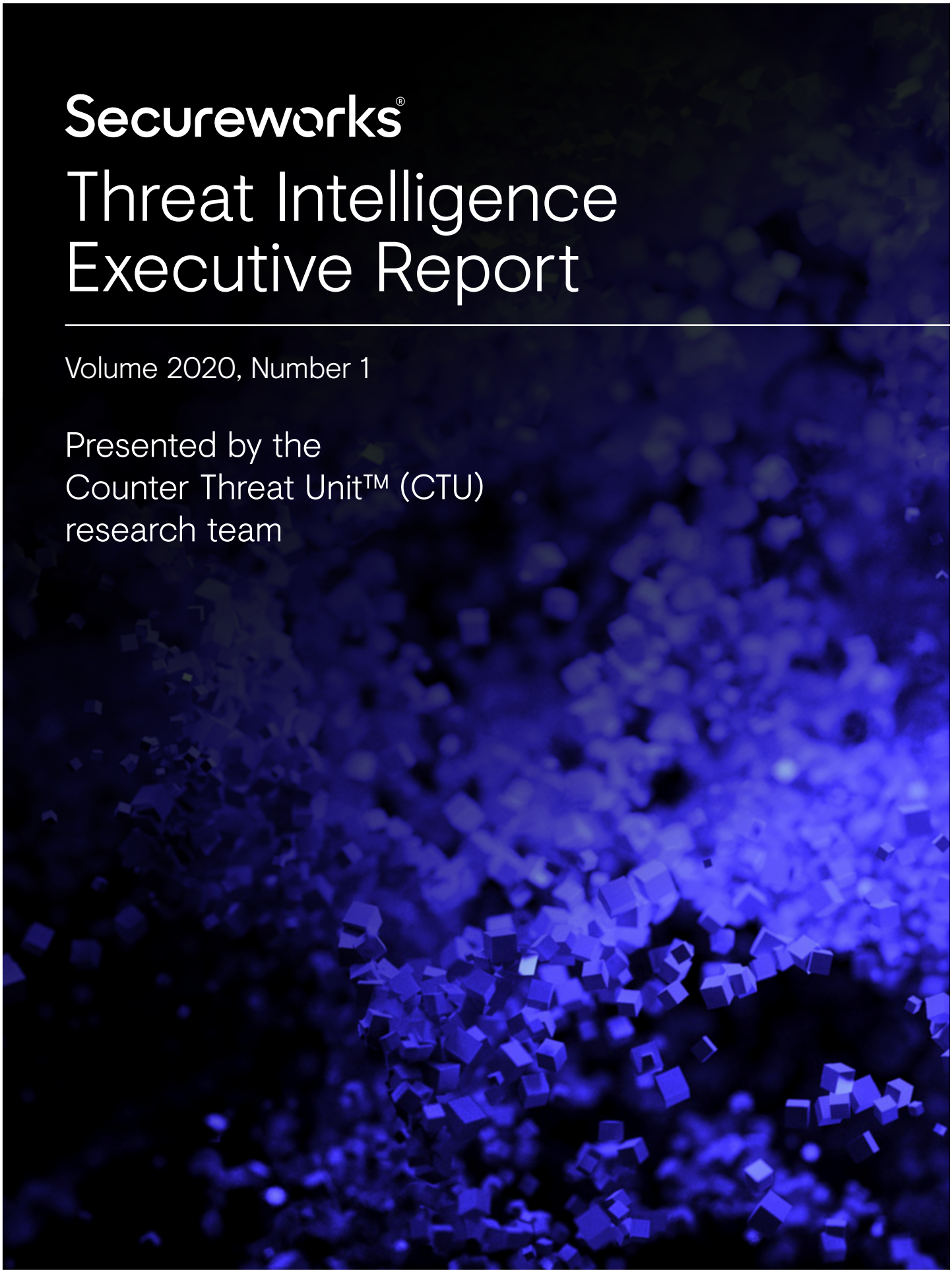
Secureworks®

Threat Intelligence Executive Report

Volume 2020, Number 1

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 November and December 2019, CTU™ researchers identified lessons learned and observed notable developments in threat behaviors, the global threat landscape, and security trends:

- Iranian espionage operations persist
- Customized Magecart attack steals customer data from high-profile retail website
- China-based threat group targets NGOs and Asian government networks

Iranian espionage operations persist

Repeated use of similar themes suggests that threat actors have had success with those tactics.

In early November 2019, CTU researchers discovered distinct phishing campaigns and a password-spraying operation likely performed by the Iran-based COBALT TRINITY threat group (also known as APT33 and Elfin). The two phishing campaigns had separate themes and targets, and they occurred at the same time as the broad password-spraying operation. For one of the campaigns, the threat actors created infrastructure that mimicked the targets' mail servers. The other campaign imitated a U.S. defense contractor job website to deliver the publicly available PoshC2 framework. Many of the COBALT TRINITY campaigns observed in 2018 and 2019 followed a playbook similar to the job-themed campaign. Specifically, a September campaign used a domain that mimicked a different U.S. defense contractor to deliver the PoshC2 and Koadic malware to infected hosts. The diverse and concurrent activity demonstrates the level of resources available to COBALT TRINITY. CTU researchers expect the threat group to continue job-themed campaigns, as use of this theme and technique for more than two years indicates it has been successful.

CTU analysis of COBALT TRINITY activity indicates that this group's main motivation is espionage for strategic gain, likely on behalf of the Iranian government. CTU researchers have identified numerous Iranian threat groups that have similar motivations. These types of business-as-usual espionage operations should not be conflated with retaliatory operations in response to the U.S. drone strike that killed Qasem Soleimani. As of this publication, CTU researchers have not observed Soleimani-related retaliation from Iran-based threat actors.

Customized Magecart attack steals customer data from high-profile retail website

Basic security practices can help retail organizations mitigate e-commerce website compromises.

In November and December 2019, CTU researchers investigated a Magecart website-skimming attack that impacted the Macy's department store website. In Magecart attacks, a threat actor inserts code into a website to steal personal details and payment information from website visitors. In a statement to affected users on November 14, Macy's stated that threat actors gained access to customers' address and payment information submitted on the macys.com checkout page and the My Account wallet page beginning sometime between October 7 and October 15. The skimmer was customized for Macy's online retail services, suggesting that the threat actors were technically sophisticated and specifically focused on this target.

Popular retail websites are common attack targets. The addition of malicious client-side scripts into e-commerce websites can damage organizations' reputations and affect operations. CTU researchers recommend that organizations running e-commerce websites apply appropriate security updates in a timely manner, review and minimize the number of third-party scripts, review network traffic for unusual activity, and enact processes to monitor websites for changes (e.g., change control, content management, and file integrity monitoring).

China-based threat group targets NGOs and Asian government networks

Monitoring for one threat group's known techniques could detect other activity that uses those tools and tactics.

In November 2019, CTU researchers observed the likely China-based BRONZE PRESIDENT targeted cyberespionage group distributing phishing emails with malicious Vietnamese-language attachments. The attachments included an information security professional's resume and a law enforcement training document. Opening the documents on a vulnerable system installed the publicly available Cobalt Strike penetration testing tool. In December 2019, CTU researchers publicly released an analysis of BRONZE PRESIDENT activity targeting non-governmental organizations (NGOs).

The group uses proprietary and publicly available tools to target South and East Asian law enforcement and political networks as well as global NGOs. China-based threat groups frequently share tools and use similar tactics, so CTU researchers encourage organizations that are likely to encounter China-based threats to review the techniques used by BRONZE PRESIDENT and apply this knowledge to assess defensive readiness.

Conclusion

As the number of sophisticated attacks increases and threat actors demonstrate greater adaptability, it is important to remember that most cybersecurity incidents leverage well-known malware and tools. CTU researchers recommend that organizations continuously review their defensive posture against these known threats to implement basic security controls on all systems. For example, using multi-factor authentication on Internet-facing systems could mitigate many attacks. Organizations should also maintain awareness of geopolitical events that could increase risk from advanced threat groups.

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

Germany
Main Airport Center, Unterschweinstiege 10
60549 Frankfurt am Main
Germany
069/9792-0

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

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

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

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

