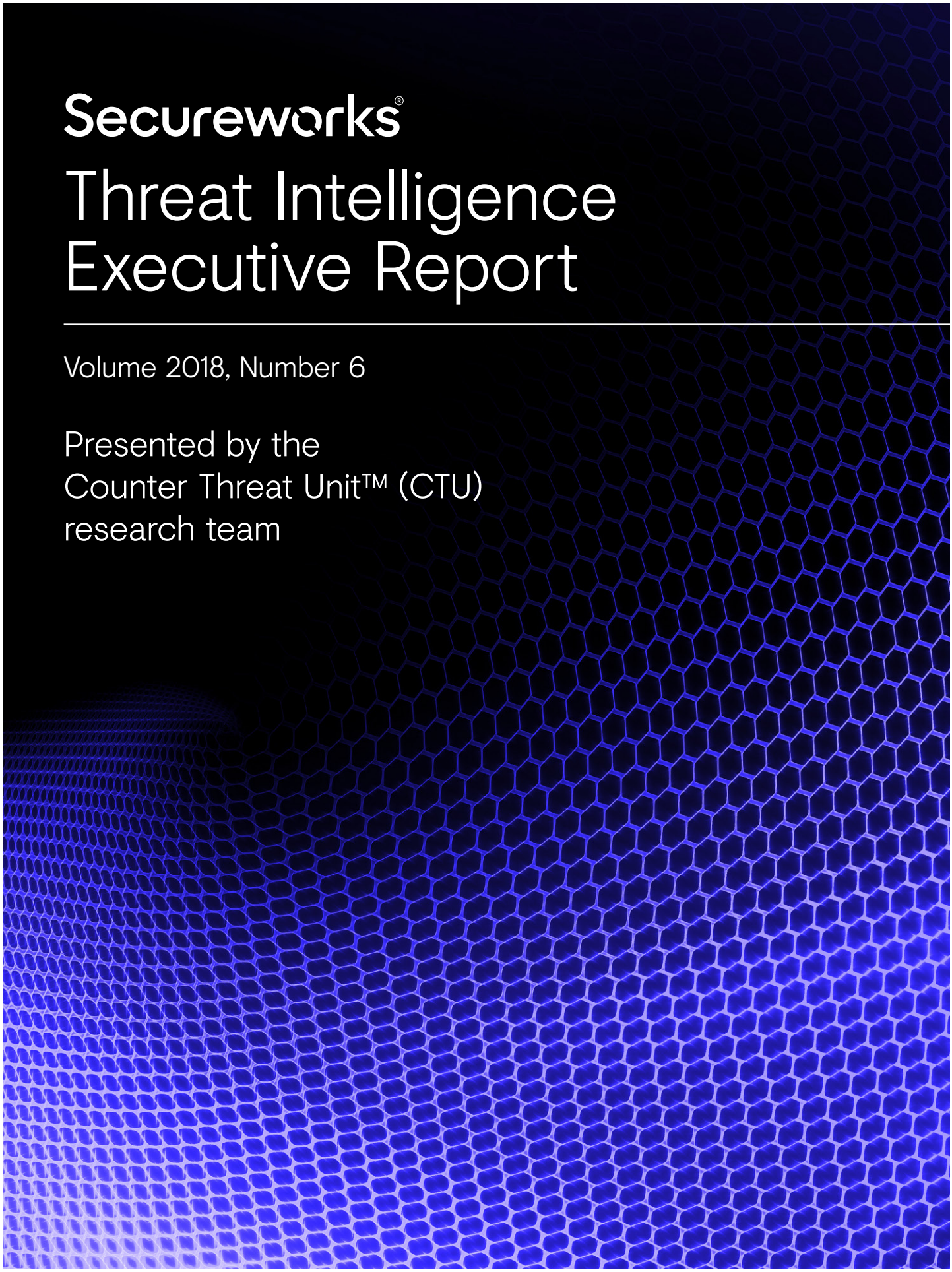
Secureworks®

Threat Intelligence Executive Report

Volume 2018, Number 6

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 September and October 2018, CTU™ researchers identified lessons learned and observed notable developments in threat behaviors, the global threat landscape, and security trends:

- Cybercrime groups used banking trojans to deliver ransomware.
- Chinese intelligence operative indictments highlighted risks of intrusions that leverage both insider and remote access.
- Digital skimmers increased risks to payment card data on retail websites.
- Following an uptick in SamsamCrypt ransomware activity, threat actors were indicted in late 2018.

Banking trojans delivered ransomware

In September and October 2018, CTU researchers tracked multiple cybercrime groups using commodity banking trojans to compromise systems and manually deploy ransomware payloads. This targeted approach to delivering ransomware is difficult to prevent and has caused significant damage to affected organizations.

Securing privileged access and applying two-factor authentication can limit malicious activity.

In one example, an organization's systems were compromised by the TrickBot banking trojan. The attacker was able to use TrickBot's capabilities to steal credentials, move laterally within the environment, and compromise the victim's domain controllers. The attacker then staged and delivered the commercially available Ryuk ransomware to a number of servers within the environment. Delivering ransomware using a domain controller allows threat actors to target critical assets efficiently, because they can communicate with any system in the environment that uses the domain controller for authentication.

During another intrusion, the BitPaymer ransomware payload was delivered to systems using initial access provided by the Bugat v5 (also known as Dridex) banking trojan. The targeted nature of these 'post-intrusion' ransomware attacks is a significant development in the cybercrime threat landscape and increases the potential disruptive risk associated with opportunistic infections such as Bugat v5 and TrickBot. Organizations should follow best practice around privileged access and apply two-factor authentication for all remote access routes. These actions will significantly limit opportunities for threat actors to gain access to and subsequently move laterally in an environment.

The cybercrime threat impacts all organizations. The Secureworks 2018 State of Cybercrime report provides insights into key developments in the cybercrime threat landscape.

Indictments highlighted blended intrusion risks

On October 25, a U.S. grand jury indicted ten individuals associated with China's Ministry of State Security (MSS) for espionage activities that targeted European and U.S. technology firms between 2010 and 2015. The indictment described an MSS operative instructing two China-based employees of a European aerospace firm to install malware via a removable media device. One of the employees was the organization's IT infrastructure and security manager in the region. This employee provided the MSS contact with details of the company's internal investigation into the intrusion. The indictment reinforces the significant role that the MSS plays in commercially motivated espionage, as well as the human and technical resources at the MSS's disposal.

Organizations should evaluate their risk to this type of activity, review their insider risk policies, and implement controls such as staff vetting, network segregation (between high risk and core business units), and role-based privilege management.

While these kinds of 'blended' techniques are likely reserved for the MSS's high-priority targets, the risk of intrusions is amplified when business units operate in countries that engage in corporate espionage. Organizations should evaluate their risk to this type of activity, review their insider risk policies, and implement controls such as staff vetting, network segregation (between high risk and core business units), and role-based privilege management.

CTU analysis suggests that threat groups of likely Chinese origin pose the most active and sophisticated targeted economic espionage threats to organizations globally. Since 2015, CTU researchers have observed China-based espionage groups targeting a wide range of organizations involved in defense technologies, education, financial services, heavy industry, investment, IT managed service providers, legal, manufacturing, pharmaceuticals, space technologies, and software production.

Digital skimmers increased risks to payment card data

In 2018, CTU researchers tracked multiple incidents of threat actors using 'digital skimmer' scripts to steal payment card data on compromised retail websites. In most cases involving digital skimmers, threat actors exploited known unpatched vulnerabilities on ecommerce platforms such as Magento, Powerfront, and OpenCart. In September, digital skimmers deployed on the British Airways website stole approximately 380,000 credit card details. The threat actors reportedly modified a JavaScript library on the company's website, adding a malicious script that collected payment data and relayed it to a spoofed British Airways website set up by the threat actors.

Limiting third-party scripts and monitoring for unusual and unauthorized activity can help protect ecommerce websites.

These campaigns demonstrate the risks of malicious client-side scripts added to retail websites, particularly when the sites rely on unpatched third-party ecommerce platforms. CTU researchers recommend that organizations running ecommerce websites apply security updates, review and minimize third-party scripts, review network traffic on existing pages for unusual activity, and enact processes to monitor websites for unauthorized changes.

SamsamCrypt ransomware activity increased prior to indictments

Between August and September 2018, CTU researchers tracked an increase in SamsamCrypt ransomware incidents at U.S.-based and European organizations. SamsamCrypt ransomware is linked to the GOLD LOWELL threat group. GOLD LOWELL typically compromises organizations via weak remote access protocols (chiefly RDP) to deploy SamsamCrypt. After the initial compromise, the threat actors perform reconnaissance in the environment by fully enumerating the network, establishing credentialed access to reachable systems, and attempting to destroy or encrypt system backups present on the network. The threat group then deploys SamsamCrypt ransomware to targeted systems using custom scripts and tools.

CTU researchers recommend that organizations consult with legal counsel regarding any decision to pay a ransom request.

In November, the U.S. Department of Justice (DOJ) announced the indictment of two Iranian nationals for their involvement in the SamsamCrypt ransomware attacks. The U.S. Department of Treasury announced action against two additional Iranian nationals accused of helping to process SamsamCrypt ransom payments. None of these individuals have been apprehended as of this publication and are able to continue operating from Iran. However, the indictments may introduce legal implications for victims who choose to submit ransom payments.

CTU researchers discourage victims from paying ransom requests, but in some cases payment may be necessary. CTU researchers recommend that organizations consult with legal counsel regarding any decision to pay a ransom request. As of this publication, it is unclear how the indictments will impact future GOLD LOWELL operations. However, numerous criminal and government-sponsored threat groups have not changed their tactics after indictments.

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 clients before damage can occur.

Research

Understanding the nature of threats clients 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 client 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 clients 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

