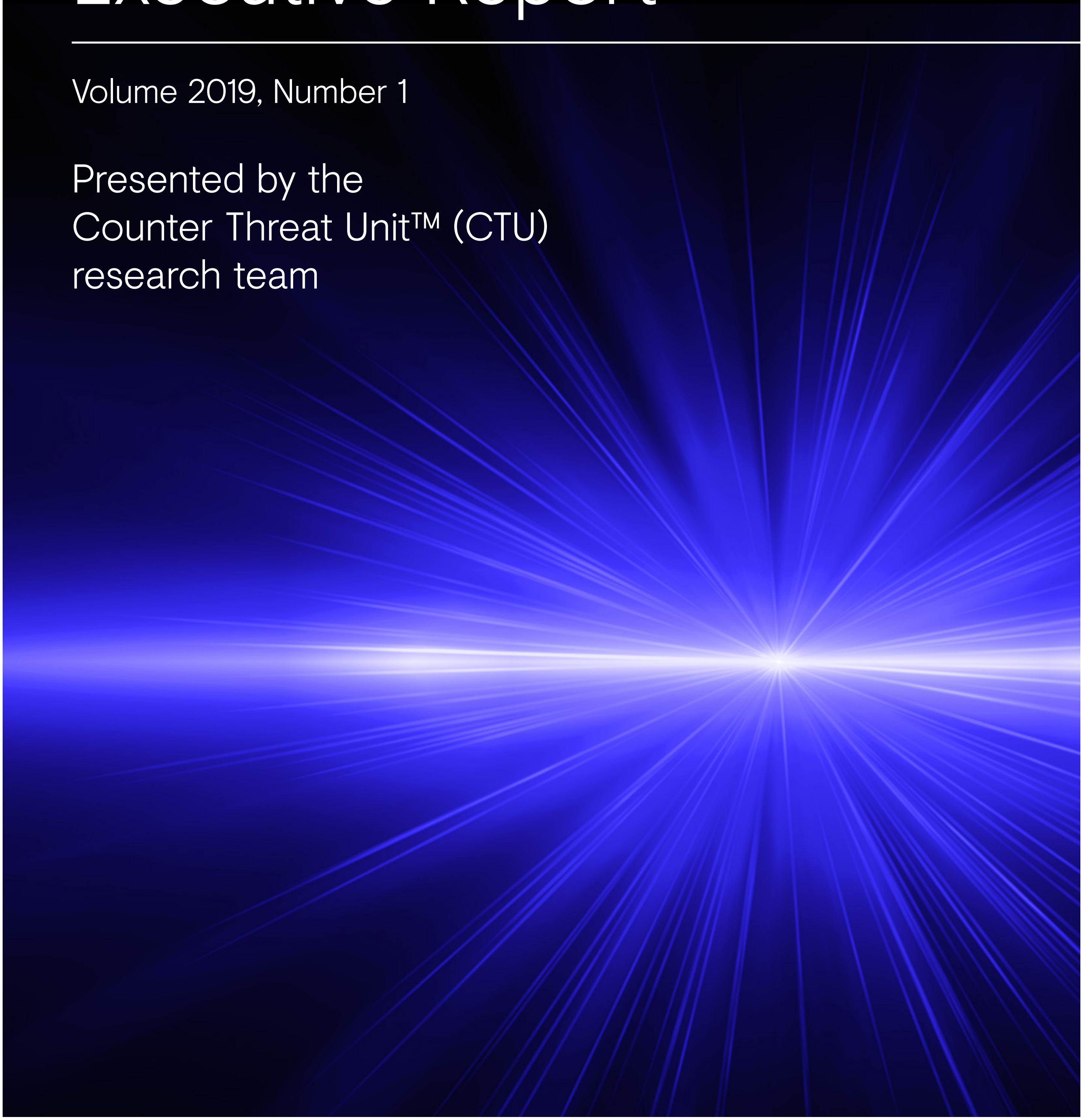
Secureworks®

# Threat Intelligence Executive Report

Volume 2019, 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 2018, CTU™ researchers identified lessons learned and observed notable developments in threat behaviors, the global threat landscape, and security trends:

- The Shamoon malware resurfaced for a third round of destructive attacks on oil companies with a Middle Eastern nexus.
- The U.S. Department of Justice continued to indict Chinese nationals for cyberespionage activity.
- Emotet continued to transform, and campaign characteristics suggest ties to ransomware and banking trojan operators.

## Shamoon malware was resurrected for a third round of destruction

Shamoon, the malware that destroyed major companies' networks between 2012 and 2017, reemerged at the end of 2018. In early December 2018, CTU researchers discovered destructive malware samples uploaded to a public sandbox. Analysis revealed that these samples were the Shamoon malware that affected Middle Eastern organizations in 2012, 2016, and 2017. The samples discovered in December were similar to older versions, including the use of the same EldoS RawDisk driver from previous campaigns. To ensure its execution, Shamoon resets the compromised system's clock to August 11, 2012 as a part of the installation routine. The time change is required because the malware uses a 2012 trial license for the EldoS RawDisk driver.

***Threat actors continue to use Shamoon to wreak havoc on networks.***

Italian oil company Saipem acknowledged a Shamoon incident on its network in December that impacted servers in Saudi Arabia and United Arab Emirates. It did not publicly disclose the delivery method used by this third wave of Shamoon attacks. Past incidents involving Shamoon have been widely attributed to the Iranian government. Iranian threat groups remained active throughout 2018, focusing on victims of likely interest to the Iranian government.

## U.S. indictment reinforced BRONZE RIVERSIDE's links to Chinese intelligence

***BRONZE RIVERSIDE will likely persist despite indictment.***

On December 20, 2018, the U.S. Department of Justice (DOJ) indicted two Chinese nationals for their involvement in Chinese government-sponsored cyberespionage between 2006 and 2018. The indictment claimed that the individuals, who worked for the Huaying Haitai Science and Technology

Development Company in Tianjin, collaborated with the Tianjin bureau of the Chinese Ministry of State Security (MSS) to conduct campaigns aimed at stealing intellectual property and other sensitive data. The MSS is the Chinese government agency responsible for counterintelligence, foreign intelligence, and political security.

The CTU research team associates the activity cited in the indictment with the BRONZE RIVERSIDE threat group (also known as APT10, Stone Panda, POTASSIUM, Red Apollo, and CVNX). CTU researchers investigated several intrusions perpetrated by the group and determined that it targeted intellectual property aligned to China's strategic interests, including defense technologies, agriculture, energy, mining, telecommunication, finance, construction, and manufacturing. The threat actors leveraged compromised managed service providers (MSPs) to access target networks and exfiltrate stolen data.

Previous indictments have not deterred Chinese government-sponsored cyberespionage operations, so CTU researchers expect BRONZE RIVERSIDE activities to continue. However, this indictment further illuminated the nature of the relationships between Chinese intelligence agencies and third-party organizations, and how these organizations are tasked to fulfill China's espionage operations.

## Emotet campaigns continued to evolve; coordination among operators likely

As network defenders employ more detection rules to stop Emotet, the malware authors have adapted their techniques to evade security controls. During November and December 2018, CTU researchers continued to observe prolific and widespread phishing campaigns delivering the Emotet malware to organizations across numerous verticals and geographic regions. Researchers observed two distinct phishing campaigns employed by the threat actors. The first campaign heavily targeted the U.S. Thanksgiving and Christmas holidays, often enticing users with gift cards and vouchers. The second type targeted specific organizations, often referencing the organization's name or projects in the lure documents to increase the click-through rate.

***Phishing education can limit the success of Emotet campaigns.***

During the latter half of 2018, Emotet began utilizing a PowerShell framework that CTU researchers refer to as PowerSplit to start the execution of code. PowerSplit provides rudimentary obfuscation of PowerShell command-line arguments and also hinders extraction by defenders who monitor Emotet staging domains. Subtle changes to the macro code used in the lure documents increased infection rates and evaded defensive controls. At the end of October 2018, the threat actors deployed a new Emotet module to aggressively harvest and exfiltrate email content from compromised systems, significantly increasing the risk to organizations. CTU researchers believe this trend of evolving tactics, techniques, and procedures (TTPs) will continue.

There were indications that malware developers collaborated on shared code and functions across multiple distinct malware families. Researchers identified strong links in the code used by the Emotet malware, BitPaymer ransomware, Gozi ISFB (also known as Ursnif) trojan, and Bugat v5 (also known as Dridex) banking trojan. Emotet was also linked to the Ryuk ransomware, as Emotet delivery of the TrickBot malware led to Ryuk infections. These connections could indicate that threat actors are sharing resources to increase efficacy. Network defenders must increase indicator sharing and collaboration within the information security community to counter these threats.

CTU researchers assess that Emotet will continue to be a pervasive and high-risk threat to all verticals in 2019. Organizations should train personnel to recognize and report suspicious email content.

# 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