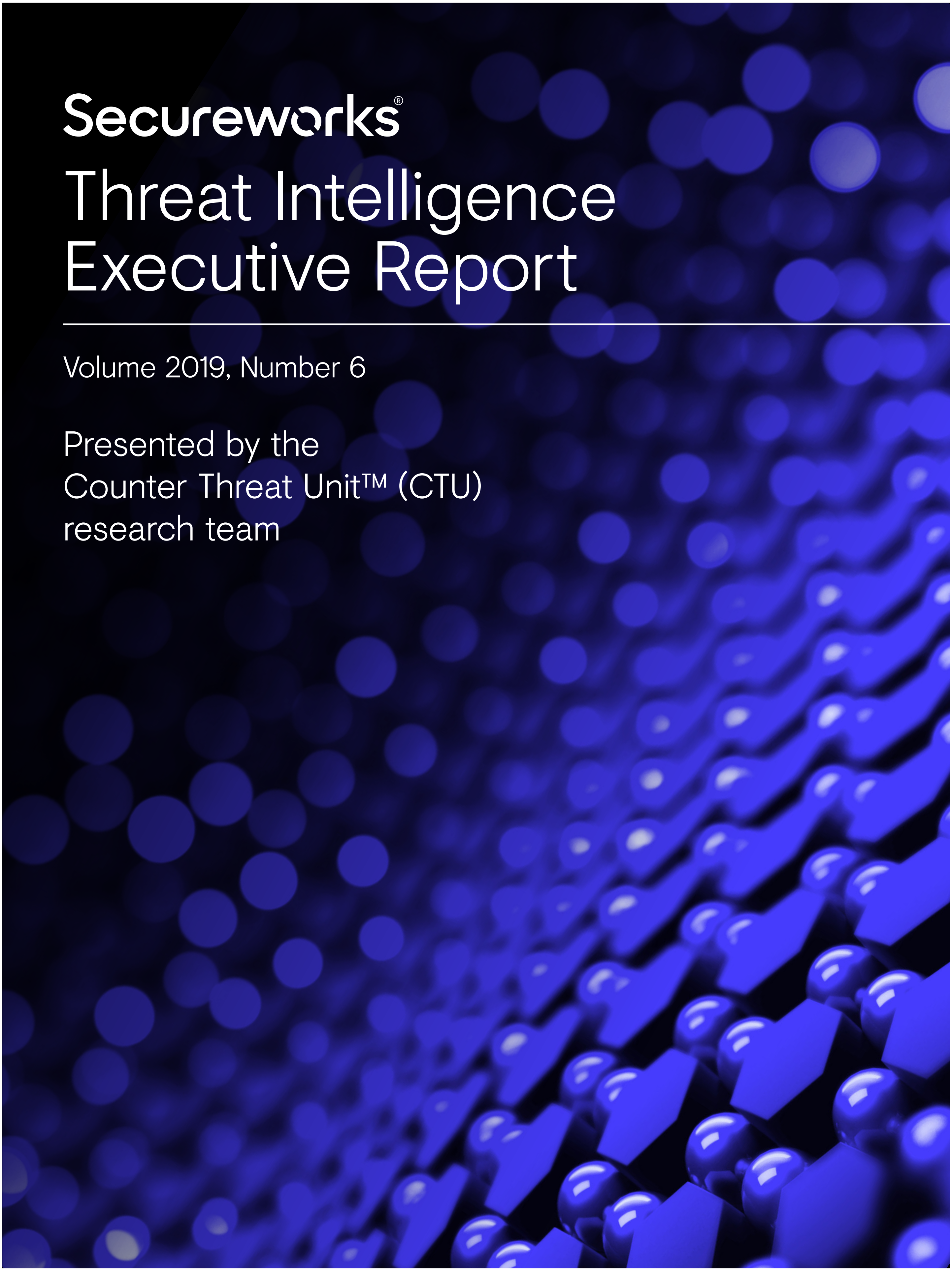

Secureworks®

Threat Intelligence Executive Report

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

- Malware and threat groups demonstrated persistence.
- Iranian threat actor activity continued in response to local geopolitical events.
- Post-intrusion ransomware leveraged existing infections after significant dwell times.

Putting the “P” in “APT” – Examples of persistent threats

Whether backed by a government or funded by a criminal enterprise, targeted threat actors (also known as advanced persistent threats (APTs)) invest significant time and effort to establish persistence. The persistence ensures continued success of their operations. These investments generally fall into two broad categories: fault tolerance and legal tolerance.

Some threat actors establish persistence that withstands operational failures and legal actions.

Fault tolerance is the ability to withstand operational failures without jeopardizing the mission. It includes techniques such as developing custom tools that evade existing detections, deploying multiple access vectors to victims’ networks during an intrusion, and building a robust network of compromised hosts (a “botnet”) through which malicious activity can be proxied and delegated.

The Cutwail spam botnet demonstrates success in fault tolerance. Since the Cutwail malware emerged in 2007, threat groups have used various versions to assemble spam email delivery botnets. The remaining Cutwail botnet has been continuously operated by the GOLD ESSEX threat group since 2012. In October, CTU researchers discovered the botnet targeting Japanese speakers, impersonating the Apple, Amazon, and Rakuten brands and referring to account loss, lockout, and fraud to convince recipients to divulge usernames and passwords. GOLD ESSEX’s ability to maintain its botnet despite multiple attempts by the security community to shutter all Cutwail botnets ranks it among the most persistent threats of the last decade.

Legal tolerance is the ability to avoid detainment and prosecution. It includes a wide range of technical and non-technical techniques, such as using bulletproof hosting providers, bribing authorities, and operating in regions where authorities either turn a blind eye or forgo prosecution. Cyber operations with optimal legal tolerance are conducted by or on behalf of a government.

In September, a phishing email purportedly received by individuals at the Ukraine Ministry of Foreign Affairs was uploaded to the VirusTotal public malware repository. The email contained a Microsoft Office document that dropped the Zebrocy downloader, which CTU researchers associate with the IRON TWILIGHT (also known as APT28, Fancy Bear, and Sofacy) threat group. CTU analysis indicates that IRON TWILIGHT is operated by the Russian GRU military intelligence service. The threat group's intrusions include the 2016 breaches of the Democratic National Committee (DNC) network and Hillary Clinton campaign staff's email accounts. The United States Department of Justice (DOJ) indicted 12 group members in July 2018. However, the September campaign and other reported activity demonstrate that IRON TWILIGHT possesses the persistence to withstand legal pressures on an international scale and the technical capabilities to ensure continued operations.

Iranian threat actor activity coincided with regional tensions

Provocative cyber and kinetic activity from Iran continued in September and October 2019 following a period of "tanker wars" and regionally focused cyber activity. CTU researchers discovered that the Iranian COBALT KATANA threat group compromised a Middle Eastern government organization's website to harvest credentials likely associated with the government's operations. Additionally, CTU researchers discovered an Iranian threat group associated with the TortoiseShell malware using the SysKit malware to target Saudi Internet service providers and the U.S. veteran community.

Political tensions can prompt cyber activity.

The intensity of likely Iranian government-sponsored cyber activity in the West remained consistent throughout September and October. CTU analysis of multiple 2019 campaigns suggest that Iran is interested in military, government, political, and financial matters. Observed activity aligns with the Iranian government's perceived strategic objective to establish regional dominance, particularly given the impact of U.S. sanctions on the Iranian economy and provocations in the Gulf of Oman and Persian Gulf.

Post-intrusion ransomware continues to be a major threat

CTU researchers observed an increase in post-intrusion ransomware activity during September and October, continuing the trend observed throughout 2019. Secureworks incident response engagements involving post-intrusion ransomware more than doubled between 2018 and 2019. There has also been an increase in the number of groups operating these schemes, and many have mature playbooks that have proven successful.

Remediating infections and patching vulnerabilities can reduce the risk of post-intrusion ransomware.

Threat groups primarily use two techniques to establish a foothold. The first method is to leverage existing commodity malware infections. For example, the Ryuk ransomware uses TrickBot infections, and BitPaymer uses Dridex infections. The initial malware is usually delivered by large-scale spam campaigns. The infection can exist for an extended time before the ransomware is deployed (see Figure 1).

Dwell Time (days)

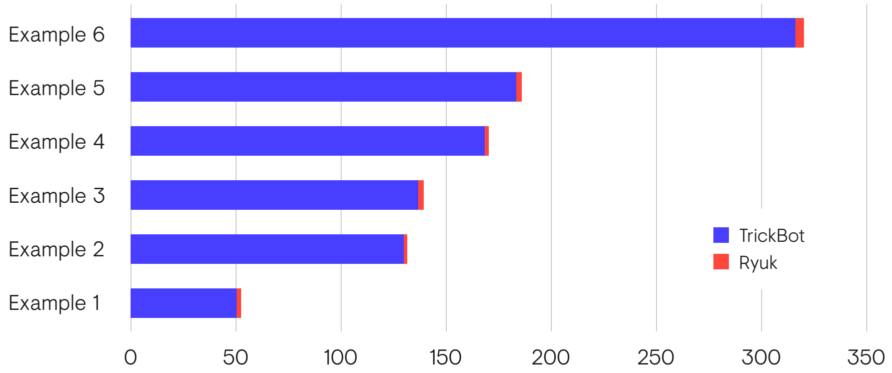

FIGURE 1: *There can be a large variance between the start of a TrickBot infection and the deployment of Ryuk. (Source: Secureworks)*

The second method for initial infection involves scanning for and compromising vulnerable Internet-facing servers. Threat groups typically use the Remote Desktop Protocol (RDP) to access the Internet-facing portion of the victim's network. They then compromise a system by exploiting a known vulnerability. The compromised system can be used as a foothold to access the rest of the network.

CTU researchers expect the post-intrusion ransomware threat to increase due to its profitability. Organizations can greatly reduce the risk by preventing the initial intrusion. If organizations identify an intrusion, it is important to thoroughly remove all malware and possible access vectors during remediation.

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