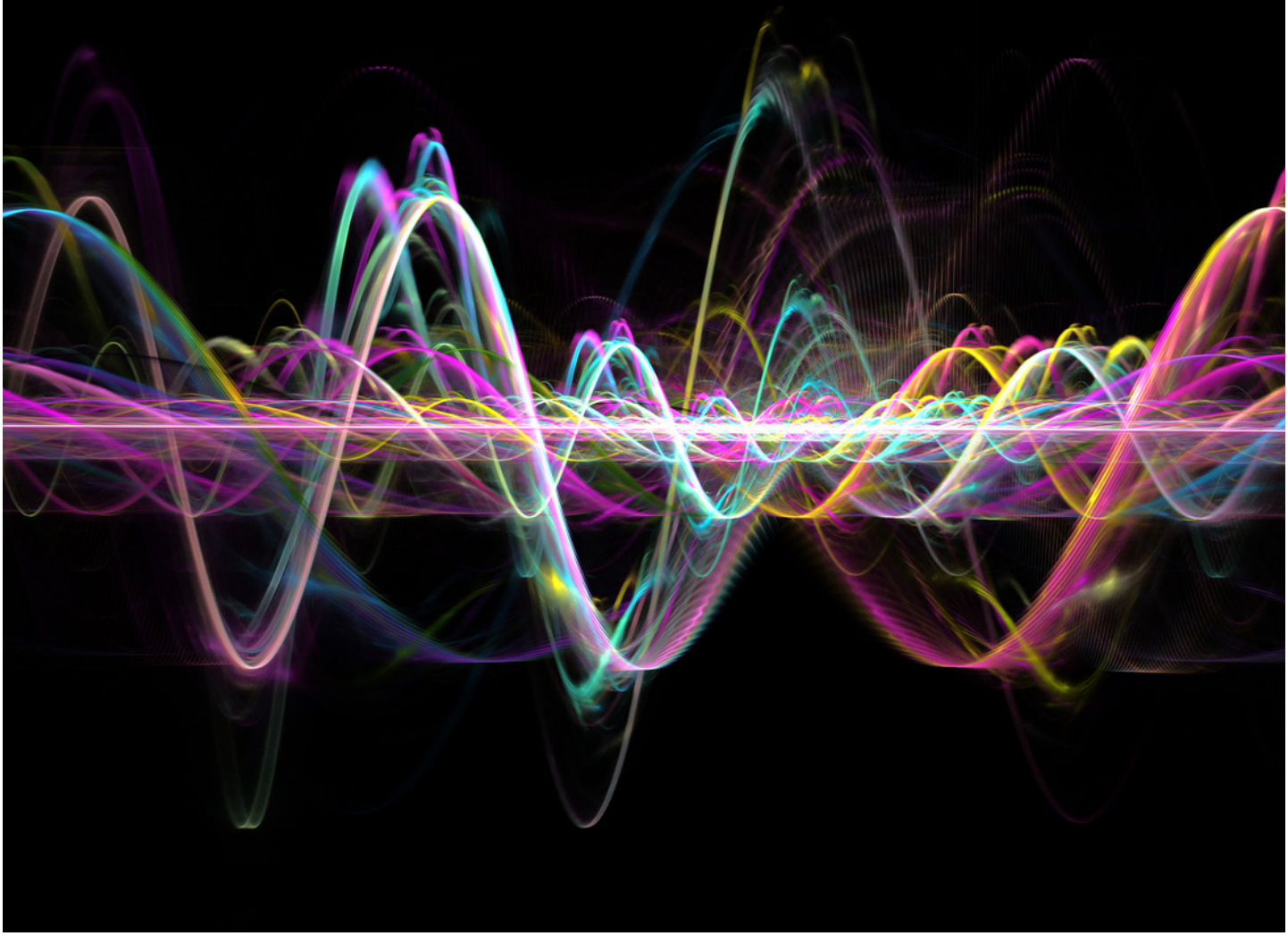
Secureworks®

Threat Intelligence Executive Report

Volume 2018, 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 2017, CTU™ researchers identified lessons learned and observed notable developments in threat behaviors, the global threat landscape, and security trends:

- Cryptocurrency miner abuse increased.
- Hardware vulnerabilities changed the scope of vulnerability management processes.
- Government-sponsored threat groups used tailored lures to compromise individuals.

Use of cryptocurrency mining software increased

Cryptocurrencies are high-profile news, as mainstream media regularly reports the rise and fall of the price of Bitcoin. As a result, threat actors leveraged their foothold on infected computers to mine cryptocurrencies. At the end of 2017 and continuing into 2018, CTU researchers observed a large increase in network intrusions involving the unauthorized installation of cryptocurrency mining software. Most of these incidents involved the publicly available XMRig mining software, which consumes computing resources to generate Monero cryptocurrency. CTU researchers observed threat actors installing XMRig by exploiting Oracle WebLogic and Ruby on Rails vulnerabilities and by leveraging existing network compromises. These efforts represent a subset of broader campaigns by financially motivated threat actors to deploy cryptocurrency mining software to large numbers of infected hosts. This type of activity is attractive to threat actors because of high cryptocurrency market valuation and the ability to outsource resource costs associated with mining.

Cryptocurrency mining will likely continue as long as it provides a return on investment for generating funds. While the potential impact may seem less significant than an information-stealing malware infection, organizations must consider the full range of risks associated with this threat. For example, threat actors could install additional malware or corrupt the system with faulty software. Affected organizations should launch a root cause analysis and address gaps in network security.

Hardware vulnerabilities widen vulnerability management scope

Hardware and software complexity make it increasingly challenging to assess an organization's exposure to vulnerabilities and weaknesses. Many vulnerability management processes focus on operating system and application security updates. Several hardware-based vulnerability disclosures encourage a comprehensive assessment that is not limited to software vulnerabilities:

- In October 2017, the Return of Coppersmiths Attack (ROCA) weakened the encryption-key generation capabilities of Infineon Technologies chips used in Fujitsu, HP, Google, Lenovo, and Microsoft systems. Researchers estimate this vulnerability could affect one-quarter of Trusted Platform Module (TPM) devices.
- In November, Intel announced multiple firmware-based Management Engine vulnerabilities that could run software without detection by other users or security controls, remotely infect systems with malware, or leak sensitive data from vulnerable systems.
- The SPECTRE and MELTDOWN vulnerabilities announced in January 2018 represent a new vulnerability class that affects most modern processors. A low-privilege user could exploit performance optimizations to read the protected memory of all processes on a system. This type of information leakage is significant for multi-tenant or cloud services that run multiple customers' services on one physical system. While proof-of-concept exploit code exists, CTU researchers are unaware of active exploitation as of this publication.

These vulnerabilities could be overlooked by a vulnerability management process that tracks only operating system and application updates. Organizations should catalog their hardware and prioritize firmware updates when appropriate. CTU researchers recommend a risk-based vulnerability management process, especially in multi-tenant environments. This process should include testing security updates prior to production deployment and applying compensating controls when reliable updates are not available. Organizations should also ensure their cloud vendors and other relevant third parties are patching appropriately.

Government-affiliated threat groups used customized lures

From referencing popular media stories like the Harvey Weinstein sexual assault scandal to crafting fake invoices, government-sponsored threat actors leverage a wide range of lures to target potential victims. CTU researchers detected a spearphishing campaign targeting senior-level individuals at legal, investment, and insurance organizations. The phishing emails, sent between September and December 2017, contained macro-enabled Microsoft Office document attachments that appeared to be customized to the target. CTU analysis suggests the campaign was conducted by the likely China-based BRONZE FIRESTONE threat group (also known as APT19). Based on similar BRONZE FIRESTONE campaigns, the threat actors may have deployed the publicly available Cobalt Strike Beacon penetration testing tool.

In November 2017, CTU researchers analyzed a Microsoft Word document that installed the Seduploader malware. Seduploader is used by the IRON TWILIGHT threat group (also known as APT 28 and Fancy Bear) to perform reconnaissance on an infected host. The delivery method is unknown, but phishing emails could have contained a hyperlink to a document hosted on an attacker-controlled domain. The document filename references the "Saber Guardian 2017" joint military exercise conducted by U.S. European Command and NATO member states in the Black Sea region, providing insight into which organizations were likely targeted in this campaign.

These campaigns illustrate the value of user education to mitigate phishing risks, particularly for employees in senior positions or with elevated access. The exploits provide justification for disabling macros and mitigating Dynamic Data Exchange (DDE) risks within corporate environments.

Conclusion

As sophisticated attacks increase 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
UK House, 180 Oxford St
London W1D 1NN
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

