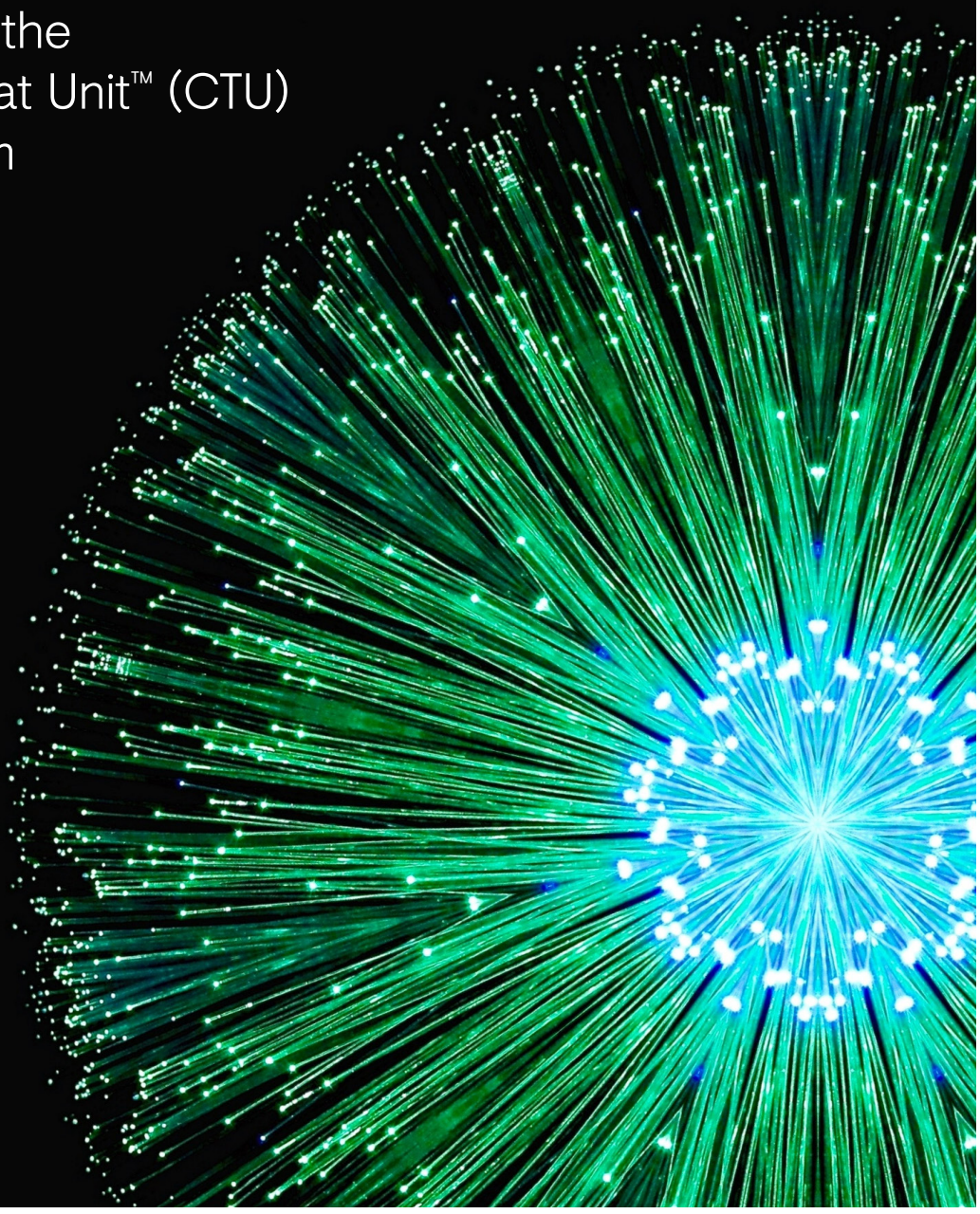
Secureworks®

Threat Intelligence Executive Report

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

- Self-propagating destructive malware is becoming more frequent.
- Threat actors are increasingly distributing malicious software updates via compromised vendors.
- A standard Microsoft Office feature has been used as a novel attack vector.
- Multiple espionage campaigns reflect increased interest in energy organizations.

Self-propagating destructive malware continues to emerge

In late October, CTU researchers observed the BadRabbit ransomware outbreak spreading through Russia, Ukraine, Japan, and Germany. Evidence indicates that multiple websites deliberately compromised as early as October 19 were used as the initial delivery vector. Some of these websites were previously compromised to deliver early variants of the NotPetya malware, which impacted organizations around the world in June 2017. BadRabbit and NotPetya also shared code and techniques for spreading. Although CTU researchers have not attributed BadRabbit to a threat actor as of this publication, these overlaps indicate that the BadRabbit authors had access to the NotPetya source code.

BadRabbit had significantly less impact than the NotPetya and WCry (also known as WannaCry) attacks in early 2017, but it was the third globally disruptive malware incident in six months. The combination of techniques that NotPetya and BadRabbit used to spread within an environment can be easily adopted by other threat actors. However, organizations can mitigate the impact of these techniques through a combination of security controls:

- Apply security updates to operating systems in a timely manner. WCry, NotPetya, and BadRabbit exploited a vulnerability addressed by Microsoft in March.
- Disable unnecessary protocols. When legacy systems require protocols such as SMBv1, or when hosts cannot be updated, restrict legacy protocols to networks that require the service and isolate them from other hosts on the network.
- Apply the principle of least privilege. Malware often requires enhanced privileges for operations such as credential theft, so limiting permissions minimizes the potential for damage.
- Ensure that security policies incorporate best practices for elements such as in-memory credential storage and securing Active Directory.
- Develop and regularly test robust offline backup and incident response strategies.

Malicious software updates present growing risk

In September, CTU researchers investigated the CCleaner registry and file removal tool. Between August 15 and September 12, millions of systems received a software update containing a malicious version of CCleaner that communicated with a command and control server. Third-party analysis of this server's data suggested that a small subset of the impacted systems were served a second-stage payload. Most of these systems appeared to belong to technology manufacturers in East Asia, suggesting a possible intent for the campaign. CTU researchers validated code overlap between the first-stage payload and the HiKit tool, which the China-based BRONZE KEYSTONE (also called APT17) threat group has historically used for targeted attacks.

Similar incidents in 2017, such as the NotPetya incident and the backdoor reported in the NetSarang software, suggest that capable threat actors increasingly leverage malicious software updates to compromise systems. Organizations should evaluate and manage the risks associated with automatic third-party software updates. The CCleaner incident also highlights the risks associated with 'shadow IT,' where organizations let unmanaged or unauthorized software update systems outside of corporate software provisioning and management processes.

Organizations should evaluate and manage the risks associated with automatic third-party software updates.

Malware campaigns abuse Microsoft Office feature

Abuse of Microsoft Office's Dynamic Data Exchange (DDE) protocol has emerged as a popular method for threat actors to execute code in malicious documents. This standard Microsoft Office feature allows data synchronization between documents but can be manipulated to execute arbitrary commands.

Weaponized Office documents have historically relied on macros to deliver malware. DDE allows an attacker to manipulate victims into granting permissions to execute an application on the system. This application could run any arbitrary command and download malware from an external server even if macros are disabled, and does not display security warnings to the victim.

CTU researchers observed an unknown threat actor leveraging this attack vector in an October phishing campaign that used a U.S. Securities and Exchange Commission (SEC) theme. Another campaign involved a purported North Atlantic Treaty Organization (NATO) document that abused the DDE protocol to deliver malware attributed to the IRON TWILIGHT threat group. CTU analysis indicates that IRON TWILIGHT is operated by or on behalf of a Russian intelligence agency. Microsoft acknowledged the use of DDE in attacks and provided guidance to disable this functionality. CTU researchers recommend that organizations review business requirements and risks for keeping DDE enabled.

Espionage campaigns targeted energy vertical

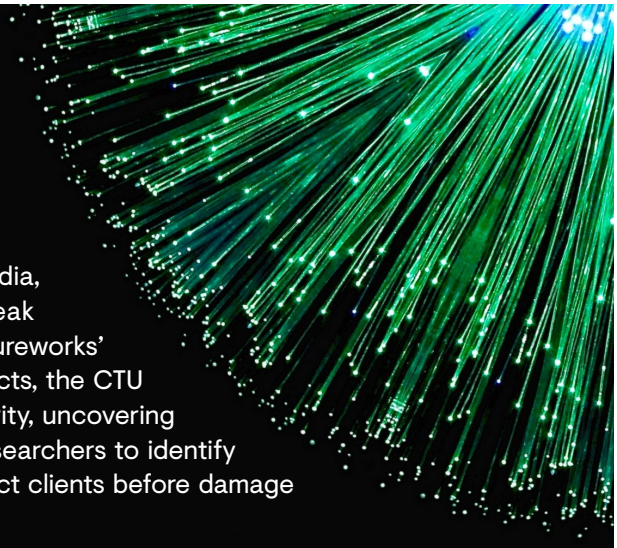
In September 2017, CTU researchers attributed multiple intrusions in the energy vertical to the IRON CASTLE threat group. The intrusions, likely directed by the Russian government, involved custom malware delivered by phishing and strategic web compromises. In 2017, CTU researchers saw an increased interest in the energy vertical by Russian, Iranian, and Chinese threat actors. All of those governments have strategic interests in energy initiatives. The Russian and Iranian economies rely heavily on oil and gas, and China continually places energy and mining (including fossil fuels, renewable technologies, and minerals) as one of its top economic priorities.

CTU researchers recommend that organizations associated with the energy vertical consider potential threats as part of their security risk management processes and employ a defense-in-depth approach to network security.

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

 © 2017 SecureWorks, Inc. All rights reserved.