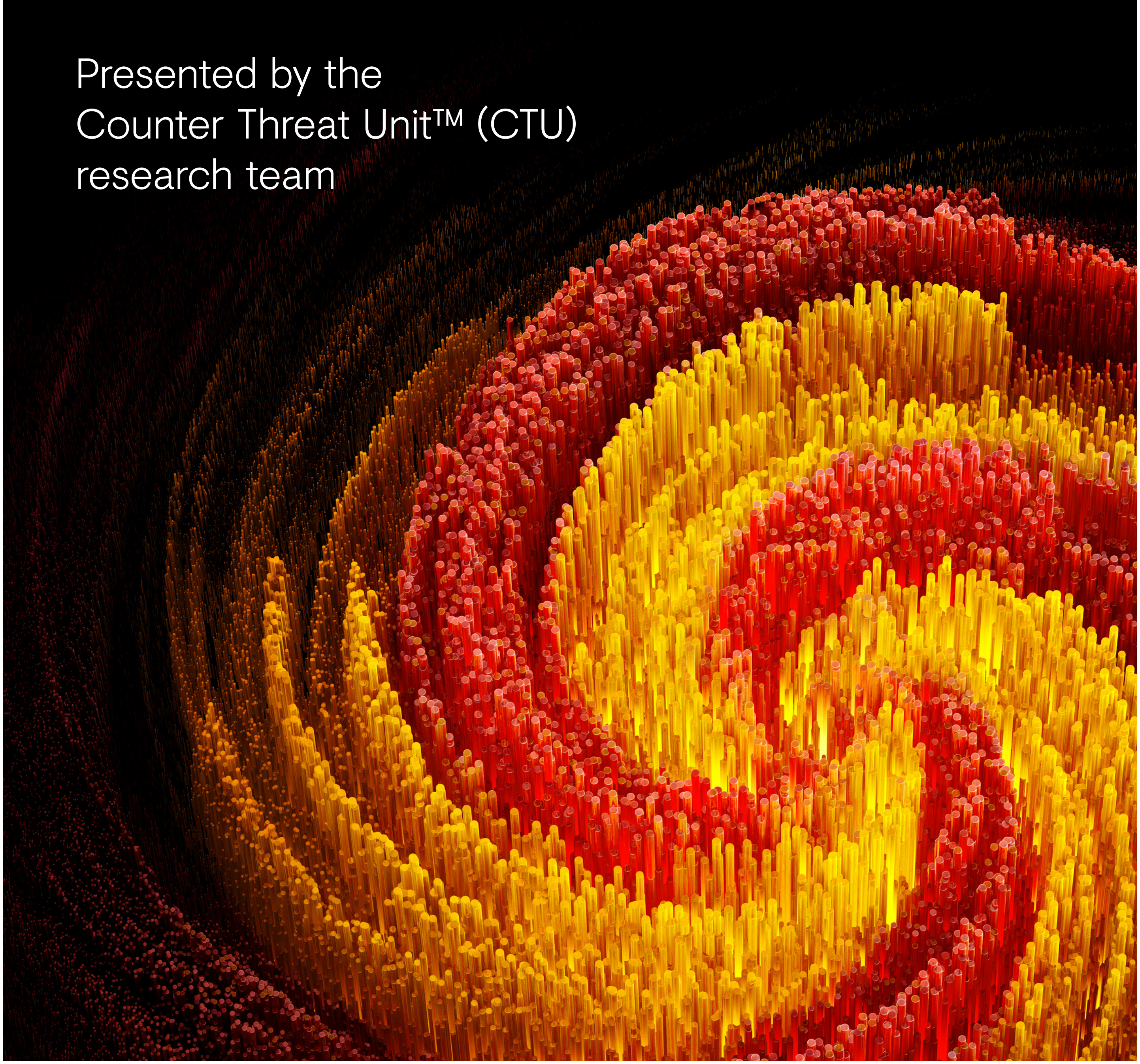
Secureworks®

Threat Intelligence Executive Report

Volume 2018, Number 2

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

- Interactive opportunistic ransomware intrusions continue.
- North Korean threat actors evolve financially motivated campaigns.
- Threat groups leverage newly exposed vulnerabilities when possible.

Interactive opportunistic ransomware intrusions continue

While ransomware has been a major threat over the last few years, it has traditionally used automated malware delivery mechanisms such as spam emails. In 2017, manually driven ransomware campaigns became more prevalent. Unlike spam-driven ransomware attacks, these attacks involve a threat actor actively operating inside the victim's environment: interactively exploiting public-facing systems, using their system access to deploy ransomware, and then propagating the ransomware throughout the compromised network.

In January 2018, CTU researchers and Secureworks incident response (IR) analysts investigated multiple incidents associated with an interactive campaign leveraging the SamSam ransomware (also known as SamsamCrypt). Public reports highlighted that a U.S.-based health record provider was breached as part of this campaign. Since late 2015, SamSam ransomware intrusions have consistently involved threat actors opportunistically compromising Internet-facing systems, using this access to escalate privileges, and then spreading the ransomware to other internal systems. The threat actors often scan for open ports that they can use as entry points. They have also been observed returning to targeted organizations that did not pay the initial ransom demand.

In February 2018, CTU researchers published a public blog post detailing the tools and techniques used in these incidents. The consistent nature of these intrusions suggests that they were carried out by a defined group or a collection of closely affiliated threat actors nicknamed GOLD LOWELL by CTU researchers.

Applying security updates in a timely manner and regularly monitoring for anomalous behaviors on Internet-facing systems are effective defenses against GOLD LOWELL tactics. Organizations should also create and test response plans for ransomware incidents and use backup solutions that are resilient to corruption or encryption attempts.

North Korean threat actors evolve financially motivated campaigns

In 2017, North Korea became more financially isolated as a result of international sanctions placed on it, and cyber threat groups driven by the North Korean government continued to target organizations to steal money. Recent activity has targeted individuals and organizations involved with cryptocurrency, suggesting a strong interest in stealing Bitcoin wallets and other currency from multiple exchanges, particularly those based in South Korea.

CTU researchers observed one such group, NICKEL ACADEMY (also known as Lazarus), continuing phishing activity in January and February. This campaign targeted individuals by sending them emails referencing legitimate job postings. These emails included Dropbox links, which led to malicious documents that contained a custom NICKEL ACADEMY macro that downloads an executable file if macros are enabled.

Phishing activities against several Bitcoin exchanges in South Korea have been tentatively attributed to North Korea. CTU researchers suspect that the rise in Bitcoin prices reinforced North Korea's interest in cryptocurrency and that the North Korean threat against cryptocurrency will remain elevated for the foreseeable future.

Threat groups leverage newly exposed vulnerabilities

While advanced threats are often associated with previously unknown ‘zero-day’ vulnerabilities, the most common attacks leverage vulnerabilities that have been recently disclosed to the public. Exploiting these vulnerabilities imposes no cost on the threat actor, but it is often effective as organizations have not yet patched their systems.

In December 2017, CTU researchers observed BRONZE UNION using documents that exploited a Microsoft Equation Editor vulnerability that was publicly disclosed in November. BRONZE UNION is a targeted threat group of likely Chinese origin that has compromised data owned by government, manufacturing, and defense organizations. Another Chinese group, BRONZE MOHAWK, has also been observed leveraging this same vulnerability.

Using recent public vulnerabilities makes economic sense for sophisticated groups. Many organizations will take weeks or months to apply new patches, increasing the chances of successful exploitation without the need to obtain or reveal any valuable zero-day vulnerabilities.

Exploit code for new vulnerabilities is often published soon after vulnerabilities are disclosed, ready for use in commodity malware tools. The 2017 WannaCry (also known as WCry) ransomware campaign is a high-profile example of recently disclosed vulnerabilities being leveraged to rapidly propagate through target networks.

These tactics re-emphasize the importance of patching operating systems and applications in a timely manner. When vulnerabilities are disclosed, it is often a race between threat actors exploiting the vulnerability and defenders patching their systems. Threat intelligence on which vulnerabilities are being exploited in the wild is also useful to help organizations prioritize patches that are being actively exploited. In addition to protecting vulnerable systems, monitoring network traffic and endpoints for known exploits can help mitigate risk if signatures and countermeasures are updated in a timely manner.

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