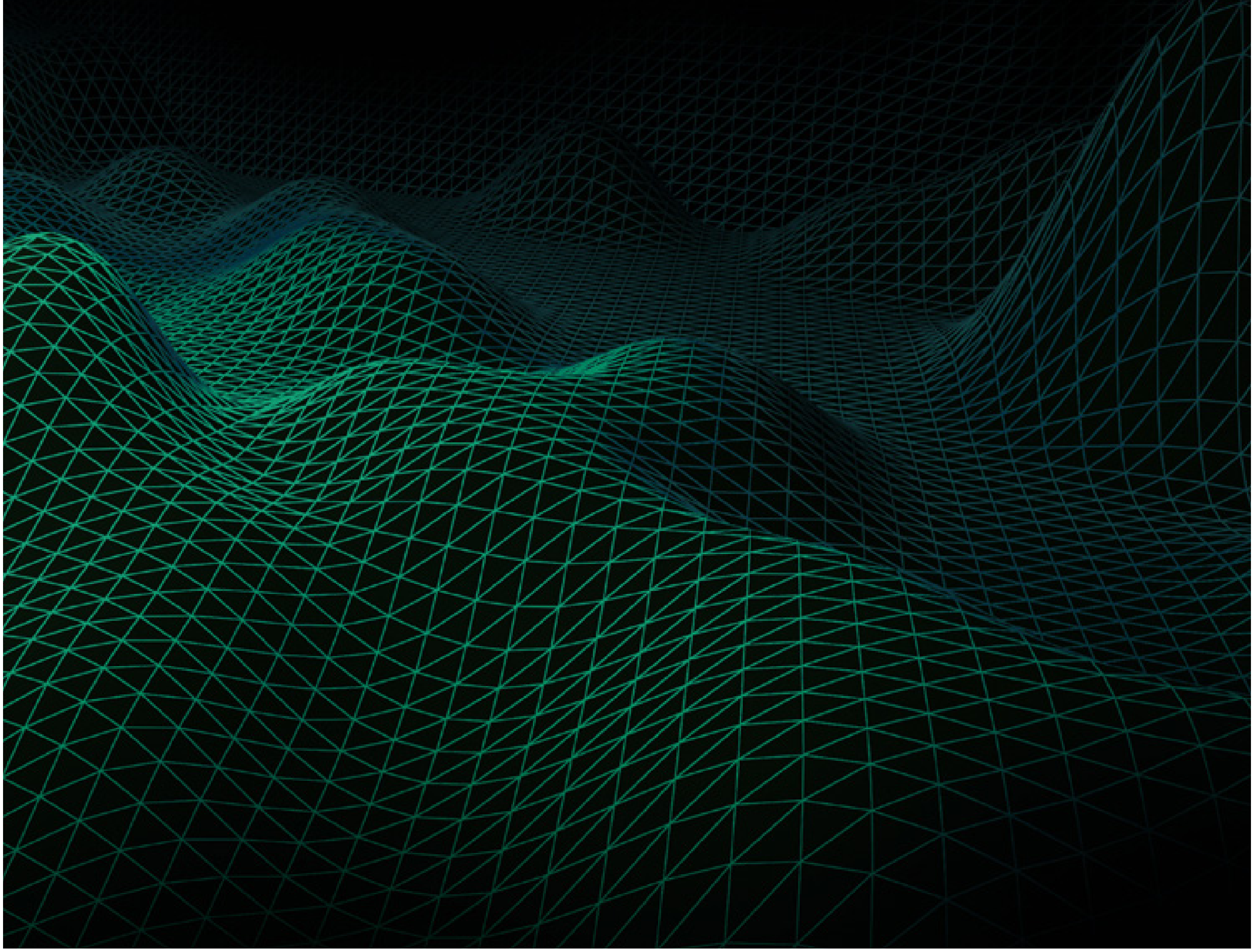
Secureworks®

Threat Intelligence Executive Report

Volume 2018, Number 3

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

- Geopolitical tension led to increased focus on Russian cyber activity.
- Business email compromise (BEC) attacks continued to be successful in stealing money.
- Cybercriminals shifted their focus to targeted attacks.

Increased vigilance against Russian cyber activity

A variety of events caused relations between Western allies and the Russian Federation to deteriorate:

- The March 2018 assassination attempt against former Russian spy Sergei Skripal and his daughter Yulia and the ensuing response from Western governments
- U.S. government sanctions against Russian citizens involved in cyber operations against the U.S. and its allies
- Russia's continuing military support of Bashar al-Assad's government in Syria

Amidst speculation that this strain could prompt the Russian government to conduct cyberattacks, US-CERT released intelligence regarding a Russian threat group that targets the energy sector. In April, the UK National Cyber Security Centre (NCSC), U.S. Federal Bureau of Investigation (FBI), and U.S. Department of Homeland Security (DHS) issued a joint technical alert (TA18-106A) discussing malicious cyber activity carried out by the Russian government. TA18-106A describes a long-term, persistent, and broad-ranging campaign by the Russian government to compromise the network infrastructure of U.S. and UK governments and private organizations, particularly those associated with critical infrastructure.

The activity detailed in the U.S. and UK government reports is not new, nor is there credible intelligence indicating an increase in Russian cyber activity. For years, the CTU research team has tracked multiple threat groups that are likely operated by the Russian government. CTU researchers assess that the Russian government would be wary of launching a significant disruptive cyber operation against the West due to fear of a significant response. Rather than indicating an elevated threat level, the timing of these reports likely reflects modified Western attitudes and risk appetite regarding known Russian activity in the strained political climate.

This assessment should not detract from the seriousness of the activity detailed in the reports. Once a threat actor has access to the devices that transmit network traffic, a number of scenarios may follow:

- The threat actor could read all unencrypted traffic and extract passwords and other information of intelligence value.
- The device configuration could be changed to copy or reroute all traffic to attacker-controlled infrastructure.
- Denial or degradation of service or even a destructive attack could be easily accomplished.

CTU researchers recommend that organizations evaluate their network devices for vulnerability to any of the described network attacks; avoid the use of insecure protocols such as Telnet, particularly across the Internet; and disable all legacy protocols wherever possible. The TA18-106A report details common attacks against network devices, and it contains simple mitigating advice and reference material for each attack.

Business email compromise attacks target payment instructions

Business email compromise (BEC) attacks continue to successfully steal large amounts of money from organizations in every vertical. The threat actors gain unauthorized access to a victim's email account; monitor email correspondence for weeks or months to understand employee roles, clients, and billing cycles; and then impersonate suppliers or partners to persuade the victim to make payments to attacker-controlled bank accounts. The social engineering tactics often involve intercepting and modifying legitimate invoices to include the attacker's bank account details. Businesses that transmit wire transfer details via email are especially susceptible to BEC.

One campaign involved GOLD GALLEON, a Nigerian hacking crew discovered by CTU researchers in April 2017 that exclusively targets the maritime shipping industry. The loose hacking collective consists of at least 20 members who plot to steal an estimated $6.7 million U.S. dollars per year. GOLD GALLEON's interest in maritime stems from its affiliation with the Buccaneers Confraternity, a pirate-infatuated fraternal organization. Some Nigerian confraternities are referred to as "campus cults" and have been observed engaging in gang-like activity.

GOLD GALLEON displays similar tactics to other West African BEC groups such as GOLD SKYLINE. The groups lack the technical expertise to produce their own tools and instead rely on inexpensive commodity malware. Evolving from their traditional campaigns as "Nigerian prince" 419 scammers, the groups have been observed crafting fraudulent documents, copying email footers, and impersonating victims by phone. What the group lacks in technical capacity is supplemented by social engineering, agility, and persistence.

CTU researchers recommend implementing two-factor authentication (2FA) for webmail to reduce the risk of an account compromise. Organizations should also enhance accounting controls to ensure that new or updated bank account details are verified out-of-band with the requesting party, and they should require multiple approvals for outbound wire transfer requests. Security-conscious organizations can still fall victim to BEC if they neglect to verify the other party in a business transaction.

Cybercrime actors trending towards targeted activity

While targeted activity is often associated with government-sponsored threats, CTU researchers have observed a shift toward targeted actions by cybercriminals. Criminal groups focus on maximizing profit, and a small number of successful targeted attacks can earn much more than a widespread non-targeted campaign. During the reporting period, the GOLD LOWELL threat group continued to compromise Internet-facing systems and services in an opportunistic manner, and then pivoted into the corporate environment using this access. Possibly spurred on by the success of GOLD LOWELL, additional threat actors are using similar methods to deploy ransomware.

CTU researchers have also observed threat actors using commodity malware in a more targeted fashion. Bugat v5 (also known as Dridex) is a banking trojan capable of stealing credentials, certificates, cookies, and other information from a compromised system, primarily to enable financial theft. While historically

Bugat v5 was a non-targeted commodity threat, threat actors have begun limiting the deployment to the most profitable organization types to maximize their return on investment. The targets include hosts associated with financial processing and organizations in the retail, hospitality, and finance verticals. Organizations that are alerted to the presence of this malware in their environment should investigate the compromised host for signs of lateral movement to other systems or evidence of threat actors actively running commands on a host.

Despite an increase in targeted activity, widespread non-targeted malware continues to pose a major threat to organizations in all industries. For the past year, the Emotet malware has been the most prevalent cybercrime threat CTU researchers have detected at organizations. Emotet is used to steal credentials and typically loads additional malware onto the compromised host, so organizations should investigate an infection to identify the full scope of the malicious activity. On May 4, 2018, the Necurs spam botnet started distributing IcedID, an emerging malware threat with credential theft and interactive capabilities that CTU researchers believe will gain in prevalence in the near future. As of this publication, Necurs continues to be the most active spam bot that CTU researchers are monitoring. These are examples of malware families that continue to evolve rapidly, highlighting the importance of continually applying threat intelligence and updated signatures to enable security tools to detect the latest threats.

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