Secureworks®

Threat Intelligence Executive Report

Volume 2019, Number 5

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

- Criminal groups using fake WhatsApp profiles to extort money.
- Commodity malware updates suggest intent to bypass SMS authentication.
- Large-scale data breach illustrates complexity of securing cloud infrastructure.

Fake WhatsApp profiles used to extort money

Out-of-band verification is the best defense against sophisticated social engineering attacks.

Criminal groups have used social engineering to persuade victims to deposit billions of dollars into attacker-owned bank accounts. The threat actors continually develop new tactics to increase the success of these campaigns. In July, CTU researchers documented threat actors using WhatsApp messages to scam senior executives into transferring large amounts of money. The threat actors created profiles with a CEO's name and LinkedIn profile picture and then used these profiles to message senior executives within the CEO's company. The messages instructed the executives to contact a lawyer at an attacker-controlled phone number to discuss a large but secret corporate merger and sign a non-disclosure agreement (NDA). The lawyer's name and firm were legitimate, satisfying superficial checks by the executives. The threat actors then directed the victims to transfer up to $500,000 USD to complete the fake merger.

Leveraging applications such as WhatsApp provides an alternative to corporate email, reducing exposure to corporate security controls and increasing the intimacy of communication with the target. Although the examples observed by CTU researchers specifically targeted executives, all users must be wary of unexpected communications and must always verify requests out-of-band.

Malware updates provide potential to bypass SMS authentication

Stolen login credentials can allow attackers to intercept authentication codes.

In August, threat actors updated the TrickBot malware to steal customer login credentials for U.S.-based cell service providers Verizon Wireless, T-Mobile, and Sprint. These stolen credentials can enable phone porting and SIM swapping attacks, which transfer a victim's mobile phone number to an attacker-controlled handset and cause the victim's phone to effectively "go dead" on the network. The attacker can then receive the victim's phone calls and SMS messages and can intercept authentication codes for the victim's accounts.

Phone porting to intercept banking SMS two-factor codes has long been a problem in countries such as Australia. The relative ease of online porting encourages threat actors to use malware and phishing sites to steal the required information. TrickBot's expanded ability to steal the required information from U.S. providers suggests that phone porting attacks could target U.S.-based individuals in the near future if not already. While SMS-based authentication remains a more secure option than single-factor usernames and passwords, token-based authentication is the most secure.

Breach highlights risks of insecure cloud configurations

In late July 2019, United States federal prosecutors charged a woman with stealing personal information belonging to almost 110 million American and Canadian citizens. Researchers believe she exploited a Server Side Request Forgery (SSRF) vulnerability to gain access to a server and then used her knowledge of Amazon Web Services (AWS) roles to find credentials that could steal the data. SSRF vulnerabilities rely on a misconfiguration to exploit a cloud provider's identity and access management controls. The complexity of environments such as AWS can introduce security holes that threat actors can leverage. For example, AWS has over 2,500 individual permissions that can be assigned to users, and securely managing these permissions requires care and expertise.

Organizations must collaborate with cloud providers to implement appropriate security controls.

Migrating to the cloud requires that an organization adopt a model where the cloud provider becomes responsible for many of the security aspects. This change can result in better security, as many cloud providers dedicate significant resources and expertise to ensure their services are secure. However, it could increase the security model's complexity and introduce risks and vulnerabilities that organizations need to understand and address with compensatory controls. This breach illustrates the issues organizations can encounter when implementing cloud security models without a complete understanding of the cloud provider's security controls and the associated risks.

Conclusion

As the number of sophisticated attacks increases 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 other 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 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

