Secureworks®

Threat Intelligence Executive Report

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

- U.S. indictments of government-sponsored attackers highlighted effective use of social media for targeting.
- Mergers and acquisitions exposed organizations to inherited risk.
- Publicly available and native system tools allowed threat actors to operate without malware, reinforcing the importance of focusing on security fundamentals.
- Chinese threat actors leveraged software supply chains to access targets.

U.S. indictment of Iranian threat actors highlighted use of social media in targeted attacks

Some threat actors use social media to establish trust relationships with targets.

According to a February 13 U.S. Department of Justice (DOJ) indictment, four Iranian nationals used information provided by a former U.S. counterintelligence officer to target members of the U.S. intelligence community in 2014 and 2015. In this Iranian government-sponsored cyberespionage activity, the suspects established relationships with the targets using fake Facebook accounts and then sent phishing emails containing malware. One of the Iranian nationals is associated with other high-profile activity as well, as he was indicted in 2018 for the 2017 Home Box Office (HBO) breach.

This activity bore striking similarities to activity that CTU researchers uncovered in 2017. The Iranian COBALT GYPSY threat group weaponized the stolen social media persona of an attractive young female to target mid-level male system administrators for the same purpose: to establish trust relationships and then convince victims to open a phishing email on corporate IT assets and install the attached malware payload.

Organizations should educate employees about the importance of limiting the information they share on social media and being mindful of the risks associated with establishing relationships with people they have never met in person. Organizations should also have processes in place for employees to report any unusual contact to internal security teams for further investigation.

Mergers and acquisitions exposed organizations to inherited risk and reinforced the need for security to play a role in business decisions

Due diligence during mergers and acquisitions could prevent costly incidents.

Mergers and acquisitions are common in the corporate world, but they introduce security risks for the companies involved. Pre-existing threats and vulnerabilities on an acquired organization's systems can expose the network of the acquiring organization to compromise. Some of the most serious incidents that Secureworks incident responders addressed in 2018 and 2019 occurred as a result of hidden threats inherited during an acquisition. These incidents damaged the integrity of data and systems and required a complex and costly remediation effort.

Organizations contemplating a merger or acquisition should involve security teams early in the process to determine potential issues. In addition, incorporating threat hunts prior to integrating networks can reveal security issues before they are introduced to the new environment. These types of proactive threat hunts almost always lead to identification of malicious activity and generation of recommendations that reduce the risk and cost associated with the acquisition.

Attackers preferred publicly available and native system tools, highlighting the importance of fundamental preventative and detective controls

Organizations should guard against compromises that leverage common tools.

There is a tendency within the cybersecurity community to focus on new or 'sexy' threats: zero-day exploits, never-before-seen malware, and novel techniques for bypassing security controls. This focus can lead to a fatalistic attitude that defending against advanced threats is impossible and a waste of time. Or, worse, vendors advertise shiny new tools to protect against 'the next generation of threat.'

In reality, CTU researchers regularly observe attackers preferring tools that are sold commercially, are available as free downloads from public code-sharing sites, or are native to Windows and other popular operating systems (also known as living off the land). By using effective, freely available tools, threat actors can avoid costs associated with developing and maintaining custom malware. Malicious activity that leverages these tools is also difficult to attribute to specific threat actors. In one intrusion during the timeframe covered by this report, CTU researchers observed attackers using a range of native Windows tools for discovery, defensive evasion, lateral movement, and data collection. The threat actors used the publicly available Mimikatz credential-theft tool and native procdump Windows Sysinternals tool to steal usernames and passwords from compromised systems.

Security teams should focus on addressing fundamental cyber hygiene to deny easy access to attackers. If a threat actor can gain remote network access by compromising Internet-facing services that require only a username and password and can then move laterally within the network using PowerShell and other native tools, there is no incentive for the attacker to spend additional money, time, and effort on more sophisticated malware. Implementing well-tested and pragmatic security controls that harden an organization's network against straightforward, low-cost attacks is a better investment than trying to anticipate novel malware or tactics an attacker might try.

Chinese threat actors exploited supply chain weaknesses

Insecure supply chains can provide access vectors for attacks.

In January, CTU researchers published an analysis of the BRONZE ATLAS threat group to clients. This group, which is likely based in the People's Republic of China and has been active since 2007, is one of the most active cyberespionage threat groups tracked by the CTU research team. It targets information held by a range of organizations in the engineering, pharmaceutical, manufacturing, technology, fossil fuel, and academic verticals.

This group has consistently targeted software supply chains using two methods to gain access to its final target. The first method involves compromising popular software updates so that they drop first-stage malware payloads. In the second method, the threat actors steal code-signing certificates from compromised software vendors. These certificates typically allow a user to trust that the signed code originated from a reputable source. BRONZE ATLAS signed its malware with the stolen certificates to evade security controls that use file reputation to indicate potential malicious activity.

Supply chain compromises are a particularly insidious form of attack because they exploit the trust relationships that organizations must establish with suppliers. Another China-based threat group known as BRONZE RIVERSIDE is notable for compromising managed IT service providers as a means of reaching targets. These increasingly common attacks are problematic because they circumvent perimeter controls and can reach an organization's internal network, frustrating intrusion prevention and detection tools and compromising sensitive business assets. Organizations should test the efficacy of existing security controls to prevent and detect these kinds of attacks.

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 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
One Creechurch Place, 1 Creechurch Ln
London EC3A 5AY
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

