Secureworks®

THREAT INTELLIGENCE EXECUTIVE REPORT

Volume 2023, Number 3

Presented by the
Counter Threat Unit™ (CTU)
research team

EXECUTIVE SUMMARY

The Secureworks® Counter Threat Unit™ (CTU) research team analyzes security threats to help organizations protect their systems. Based on observations in March and April, CTU™ researchers identified the following noteworthy issues and changes in the global threat landscape:

- Cascading supply chain attacks bring extra risk
- Infostealers are a gateway to ransomware attacks
- Avoid the cyber dangers that lurk outside your perimeter

CASCADING SUPPLY CHAIN ATTACKS BRING EXTRA RISK

The origin of the 3CX compromise reveals added complexity for organizations assessing the risk of supply chain attacks.

The SolarWinds supply chain compromise by a Russian state-sponsored threat group in 2020 remains one of the most significant example of attacks that originate from compromised vendor products. However, a supply chain attack discovered in March 2023 added a new dimension to the risk that organizations face.

During this attack, multiple versions of a 3CX softphone application were infected with malware. The incident is thought to be the first example of a 'double supply chain' attack. According to Mandiant, the compromise conducted by North Korean state-sponsored threat actors started when someone at 3CX downloaded an installer for the X_TRADER futures trading platform from Trading Technologies. This platform was infected in an earlier North Korean intrusion. As a result, the attackers gained access to 3CX software development systems and infected its products.

North Korea is known for financially motivated attacks and cyberespionage. The attack on Trading Technologies was likely financially motivated and affected users in the critical infrastructure and financial trading sectors. Its impact allowed the threat actors to build on the resulting opportunistic compromise of 3CX for more targeted espionage attacks.

In Volume 2023 Number 2 of the Secureworks Threat Intelligence Executive Report, we discussed how much of the onus for preventing software security incidents currently falls on users rather than vendors. Conducting due diligence on vendors' security practices is an essential part of mitigating and preventing compromises.

✓ **What you should do next:**
Understand where and how you use third-party applications so you can react quickly if a supply chain attack occurs. Only permit authorized software downloads required by your business and define baseline behavior for each application. Implement layered controls to detect any baseline deviations and potential post-exploitation activity.

INFOSTEALERS ARE A GATEWAY TO RANSOMWARE ATTACKS

Ransomware activity appears to continue unabated. Infostealer malware likely plays a significant role in the credential-harvesting activity that can lead to ransomware attacks.

One of the techniques threat actors use to obtain stolen credentials is infecting victims' systems with infostealer (also known as stealer) malware. Infostealers work very quickly on an infected system, often collecting and transmitting data to the threat actor within seconds.

Infostealers are advertised for sale or rent on underground markets for as low as $50 USD a month. There is a wide selection available that ranges in price, functionality, and level of support, making them accessible and usable by many threat actors. Infostealer malware can be installed on a computer or device via malicious software downloads or phishing attacks if users visit infected websites. Most of the popular infostealers can deliver additional malware. Kits are also available to help threat actors write their own infostealers.

The stolen credentials can be leveraged in further attacks or packaged as 'logs' and sold to other threat actors on underground marketplaces. The ransomware-as-a-service model makes information pilfered by infostealers valuable for ransomware affiliates seeking initial access to enterprises. Some marketplaces allow threat actors to parse logs to find data about specific organizations.

The number of stolen credentials advertised on underground forums keeps increasing. On a single day in February 2023, there were 5.3 million logs for sale on the Russian Market marketplace. Eight months earlier, that figure was 2.8 million.

This type of malware is a known precursor to ransomware attacks, and ransomware activity continues to pose a major threat. As a result, it is essential that organizations can detect and protect against infostealers.

✓ **What you should do next:**
Read the CTU analysis on the growing threat from infostealers for more information on how they operate.

AVOID THE CYBER DANGERS THAT LURK OUTSIDE YOUR PERIMETER

Sophisticated threat actors are increasingly approaching prospective victims via personal social media.

In March, CTU researchers publicly released details about COBALT ILLUSION's abuse of hijacked and fake social media accounts to contact potential espionage targets. Iranian state-sponsored threat actors have a history of this type of activity; the Mia Ash persona widely publicized in 2017 was the work of an Iranian threat group. Meta's Adversarial Threat Report for the first quarter of 2023 also described threat actors from multiple countries, including Iran, creating fake personas on Facebook and other Meta platforms for social engineering and other covert influence purposes.

China conducts similar campaigns. In a July 2022 joint address, the heads of the British Security Service (MI5) and the U.S. Federal Bureau of Investigation (FBI) warned about Chinese intelligence officers contacting a British aviation expert online who was then "wined and dined" before being tapped for technical information on military aircraft. A U.S. indictment unsealed in October 2018 indicated that Chinese intelligence operatives forged relationships with individuals in sensitive roles via email to steal intellectual property.

These reports serve as a reminder that threat actors, especially state-sponsored ones, often target individuals and organizations of interest via social media and other external platforms. They may build a relationship, sometimes over a long period of time, with the victim. This relationship can ultimately lead to a compromise that originated beyond the reach of organizational security controls. For example, COBALT ILLUSION's Twitter personas distributed phishing links via direct messages to steal victims' login credentials.

In general, user education should be a last line of defense rather than the first. In these incidents, warning employees to be wary of unsolicited contact on social media is essential. However, education should also be coupled with monitoring to identify suspicious login attempts.

What you should do next:
Understand your attack surface, especially any overlaps with resources that employees may access via both corporate and personal devices. Implement processes for employees to report suspicious contact or activity.

CONCLUSION

Threat actors are continually seeking ways to conduct attacks. Whether they hide behind Twitter personas, purchase credentials on underground forums, or add infected links to the supply chain, threat actors' malicious behavior leaves indicators that comprehensive implementation of extended detection and response (XDR) solutions can identify.

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 global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
www.secureworks.com

Asia Pacific

Australia
Building 3, 14 Aquatic Drive
Frenchs Forest, Sydney NSW
Australia 2086

Japan
Otemachi One Tower 17F, 2-1,
Otemachi 1-chome, Chiyoda-ku,
Tokyo 100-8159,
Japan
www.secureworks.jp

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom

1 Tanfield
Edinburgh EH3 5DA
United Kingdom

United Arab Emirates
Building 15, Dubai Internet City
Dubai, UAE PO Box 500111

If you need immediate assistance, call our 24x7 **Global Incident Response Hotline:**

+1-770-870-6343