Secureworks®

Threat Intelligence Executive Report

Volume 2020, 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 2020, CTU™ researchers observed notable developments in threat behaviors, the global threat landscape, and security trends, and identified lessons to be learned.

- Lesser-known government-sponsored threat groups put sensitive data at risk
- Citrix vulnerability disclosure causes spike in security incidents
- Ransomware operators leverage risk of GDPR fines as threat

Lesser-known government-sponsored threat groups put sensitive data at risk

Organizational visibility should extend beyond China, Russia, Iran, and North Korea.

CTU researchers have observed and documented numerous campaigns conducted by threat groups operating on behalf of the Chinese, Russian, Iranian, and North Korean governments. However, government-sponsored threat groups based in other countries, such as India and Vietnam, can also pose serious threats to targeted organizations and data.

In January 2020, CTU researchers observed Microsoft Word documents delivering version 4.0 of the YTY modular malware framework, which is associated with ZINC EMERSON. YTY steals documents, captures keystrokes, takes screenshots, and then sends stolen data to an attacker-controlled server.

CTU analysis suggests that ZINC EMERSON is likely sponsored by or affiliated with the Indian government. This threat actor has traditionally focused on political and military espionage, predominantly against Indian secessionist groups and targets in Pakistan and China.

ZINC EMERSON tends to use lure documents containing themes relevant to Pakistan and neighboring countries. The documents leverage object linking and embedding (OLE) to exploit a vulnerability in unpatched versions of Word and download an executable file. This executable file in turn downloads additional files to install the YTY malware on the victim's computer.

CTU researchers also observed ZINC EMERSON deploying Android malware in January. This behavior demonstrates the threat actors' attempts to compromise both mobile and desktop platforms to steal sensitive data.

Threat actors from other Asian countries were also active in 2019 and 2020. In early 2019, car manufacturer Toyota announced compromises of its Japanese and Australian offices. In December 2019, German media reported that BMW and Hyundai had been compromised. These compromises were likely conducted by the TIN WOODLAWN threat group (also known as APT32).

TIN WOODLAWN operates on behalf of the Vietnamese government. It focuses on persistent access to organizations and individuals of interest to the Vietnamese government. This threat group predominantly targets automotive manufacturers, media organizations, non-governmental organizations (NGOs), dissidents, social groups in Vietnam or overseas, and regional governments.

The threat actors develop custom Windows and macOS malware and use publicly available tools such as Cobalt Strike. The threat group's tools, behaviors, and targeting are consistent with well-resourced government-sponsored threat actors.

Key Takeaway

Although cyber activities from Russian, Chinese, Iranian, and North Korean threat groups monopolize media reports, there are many well-resourced and highly capable threat groups operating on behalf of dozens of other governments. Organizations should consider what information and resources they hold and ask which elements would be of interest to specific government-sponsored or criminal threat actors.

Citrix vulnerability disclosure causes spike in security incidents

A large percentage of Secureworks incident response engagements in January 2020 were due to network intrusions and malware deployment following the December 2019 public disclosure of exploit code for a Citrix vulnerability (CVE-2019-19781). An attacker could execute arbitrary code on Citrix Application Delivery Controllers (ADCs), Citrix SD-WAN WANOP, and Citrix Gateway (previously called Netscaler ADC and Netscaler Gateway). Following the disclosure, Citrix released mitigation steps that added a policy so the devices dropped certain badly formed network requests. Between January 19 and January 24, Citrix published a series of security updates to address this issue.

Organizations should implement mitigation advice as well as security updates.

Project Zero India released exploit code for this vulnerability on January 11. Other exploits quickly emerged on other platforms, including a Metasploit module on January 13 and a scan-and-exploit script on January 16. On January 15, there were approximately 10,000 vulnerable devices exposed to the Internet. The public availability of these exploits coupled with a broad attack surface led to a large number of compromises. Most of these compromises were opportunistic attacks that deployed cryptocurrency miners to generate revenue for the attackers, but some sophisticated threat groups exploited the vulnerability for targeted attacks.

Key Takeaway

Many organizations did not implement Citrix's mitigation steps before the vulnerability was widely exploited. It is likely that many vulnerability management processes missed the manual mitigation steps recommended by Citrix because they are designed to identify and deploy only vendor security updates. CTU researchers recommend that organizations ensure that their vulnerability management programs include mechanisms to review and implement all options to remediate vulnerabilities in a timely manner, even if no update has been released.

Ransomware operators leverage risk of GDPR fines as threat

Ransomware now threatens both confidentiality and availability.

In February, CTU researchers identified a REvil ransomware note that threatened to expose data stolen from a victim. The note included a warning about General Data Protection Regulation (GDPR) violations as an inducement to cooperate, signaling an evolution in the ransomware techniques used by criminal threat actors. Fines for violations of some provisions of the GDPR can exceed €20 million. Threat groups could be calculating that victims will decide to pay a significantly lower ransom amount rather than risk public embarrassment and large fines.

The trend since 2018 toward more precise targeting of victims, combined with post-intrusion ransomware deployment, allows threat actors to identify and exfiltrate personally identifiable data. Attackers can subsequently threaten to publish this data to extort the organization rather than simply demanding a ransom to decrypt the data.

In 2019, attackers increasingly followed through on threats to disclose data collected during post-intrusion ransomware attacks. In May 2019, a Twitter user claimed responsibility for the ransomware attack against the City of Baltimore and publicly released sensitive documents supposedly stolen during the incident. In November 2019, Maze ransomware operators released data purportedly stolen from Allied Universal's network. In early 2020, the DoppelPaymer and Nemty ransomware operators also started to employ this tactic. The collection and release of sensitive information ("doxing") and the threat of regulatory consequences increase the impact of ransomware attacks.

Key Takeaway

The best way to mitigate post-intrusion ransomware attacks and avoid extortion and regulatory fines is to detect and evict threat actors before they deploy ransomware. Paying the ransom does not guarantee that the attackers will refrain from disclosing data or that system availability can be restored. CTU researchers recommend that organizations apply security updates to Internet-facing systems, implement multi-factor authentication, deploy a layered defense, and develop and test incident response and recovery plans. This breadth of security measures guards against initial ransomware attacks and frustrates attackers attempting to spread malware throughout the network after an intrusion.

Conclusion

The threat landscape remains highly diverse. Government-sponsored threat groups from both large and small nations continue their activity. New vulnerabilities regularly appear, and attacker tactics and techniques mutate. Organizations should employ fundamental security hygiene practices:

- Maintain a broad awareness of geopolitical events that could generate targeted attacks.
- Update vulnerable systems in a timely fashion.
- Implement mitigation steps in addition to security updates.
- Frequently review and update defensive postures, governance processes, and security controls to protect systems against threat actor tactics and behaviors.

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

