Secureworks®

Threat Intelligence Executive Report

Volume 2019, Number 4

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

- Iranian cyber activity continued as political tensions increased.
- Post-intrusion ransomware continued to be a major threat.
- Emotet continued evolving but then went quiet.

Iranian cyber activity continued in the wake of rising global tensions

Political tensions could provoke disruptive or destructive attacks.

Tensions between the U.S. and Iran have increased since the U.S. announced its departure from the Joint Comprehensive Plan of Action (JCPOA) on May 8, 2018 and implemented financial sanctions. Rhetoric between the two countries escalated in June and July 2019 following conflicts such as the destruction of drones in the Strait of Hormuz. On June 22, the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) issued a statement regarding the cyber threat from Iran, specifically noting an increase in observed activity against U.S. industries and government agencies. The statement indicates that in addition to gathering information, Iranian threat actors have disruptive and destructive capabilities.

CTU researchers have observed consistent activity from threat actors likely associated with the Iranian government since tensions began to increase. For example, COBALT TRINITY (also known as APT33 and Elfin) launched a campaign in June with a characteristic playbook: job-themed spearphishing emails initiated a multi-stage PowerShell-based infection chain to deploy the POWERTON PowerShell-based remote access trojan (RAT). This campaign centered around two politically themed domains and could deliver additional disruptive or destructive wiper attacks. These threat actors previously targeted aerospace, defense, and oil/energy organizations with business ties to the Middle East.

CTU researchers also identified targeted activity in the Middle East from previously unobserved threat groups. On May 21, several employees at a Middle Eastern organization received a phishing message from a previously compromised internal resource. The message contained a macro-laden Excel attachment that dropped a malware payload that CTU researchers named DanBot. DanBot downloads and uploads files, updates itself, and executes commands on the compromised host. It can also create files containing static commands to

execute at a later time. Once installed, the DanBot malware communicates with a command and control (C2) server using either the HTTP or DNS protocols. Further analysis revealed links to a malware family that CTU researchers named GooglUPDT, which could be a previous version of DanBot.

CTU researchers observed multiple Iranian intrusions begin with the collection of valid credentials in the victim's environment. The threat actors' tactics to obtain these credentials included social engineering, phishing, password spraying, brute-force attacks, and the exploitation of publicly available systems. Organizations should protect user credentials within their environment through periodic user awareness training, implementation of a robust password policy, and multi-factor authentication.

Post-intrusion ransomware continued to impact organizations

Throughout 2019, ransomware has been a major challenge for organizations as threat actors deliberately held victims to ransom.

"Commodity" malware can lead to a major incident.

In May, CTU researchers analyzed the previously unobserved RobbinHood ransomware family. RobbinHood was implicated in at least two high-profile incidents affecting U.S. government organizations, but the initial access vector (IAV) is unknown. RobbinHood iterates through a list of 179 service names associated with antivirus, security, backup, and database software and attempts to stop each service. The ransomware then encrypts files on the system that match a list of file extensions. These extensions are associated with a broad range of multimedia, productivity, and software development applications. The RobbinHood samples analyzed by CTU researchers demand either 7 or 13 Bitcoin to decrypt all infected systems, or 3 Bitcoin to decrypt individual systems.

Organizations continued to experience Ryuk ransomware incidents. This ransomware is often the result of an Emotet and TrickBot malware infection. Victims typically perceive Emotet as a low-threat commodity malware downloader. However, a single Emotet infection could compromise many more systems and could subsequently install Ryuk, creating a major organization-wide incident. The IAV is often a user opening a malicious email attachment. These incidents highlight the importance of responding quickly to routine "commodity" malware infections, before they have the chance to escalate.

Threat actors invest time and effort to deliver these attacks, reaping a significant return on investment. CTU researchers recommend that organizations search out and address the weaknesses in their networks that may allow such an attack to occur.

Emotet took a holiday

Emotet has consistently been one of the top malware threats during 2018 and 2019. It evolved from a financially motivated banking trojan to a malware distribution mechanism. The highly organized Emotet operators develop and maintain the malware and its command and control (C2) infrastructure. Through April and May, CTU researchers observed several Emotet updates that included anti-analysis techniques, obfuscation, and PowerShell download commands. However, Emotet spam activity declined on June 1, and its C2 infrastructure stopped providing updates to infected hosts as of June 7.

Lulls in malware activity do not necessarily indicate elimination of a threat.

Emotet has been known to dip in activity around holiday times in the past, including taking a lengthy (Northern hemisphere) summer break. CTU researchers expect the activity to eventually resume. Organizations should remain vigilant and use this lull to review technical controls and refresh user education regarding email threats.

Conclusion

As the number of sophisticated attacks increases and threat actors demonstrate greater adaptability, it is important to remember that most cybersecurity incidents leverage well-known malware and tools. CTU researchers recommend that organizations continuously review their defensive posture against these known threats to implement basic security controls on all systems. For example, using multi-factor authentication (MFA) on Internet-facing systems could mitigate many attacks. Organizations should also maintain awareness of geopolitical events that could increase risk from advanced threat groups.

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

