SEPTEMBER 2016

SECUREWORKS® THREAT INTELLIGENCE EXECUTIVE MONTHLY REPORT

PRESENTED BY THE COUNTER THREAT UNIT™ (CTU) RESEARCH TEAM

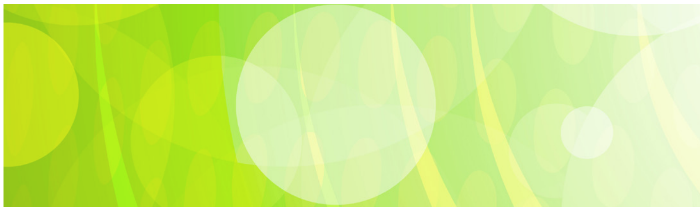
SecureWorks®

EXECUTIVE SUMMARY

The SecureWorks Counter Threat Unit (CTU) research team analyzes security threats and helps organizations protect their systems. The following events and trends were significant in August 2016:

1 FIREWALL VULNERABILITIES EXPOSED

Security vendors scrambled to address multiple vulnerabilities in firewalls after threat actors dumped exploits.



2 RIG POPULARITY INCREASED

The RIG exploit kit was one of the most versatile and popular tools to compromise targeted systems with multiple malware families.

3 RANSOMWARE DIVERSIFIED

The Locky, Cerber, CryptXXX, and TorrentLocker ransomware families diversified their infrastructure to expand into new regions and increase monetization.

4 POS SYSTEMS BREACHED

An organized crime threat group allegedly breached multiple point-of-sale (POS) systems for financial fraud.

5 THREAT GROUP OBJECTIVES VARIED

Government-sponsored threat groups used extortion, cyberespionage, and disruption for intelligence gathering, financial gain, and intimidation.

6 AGGRESSIVE POLICIES ENDORSED

Governments and law enforcement bodies endorsed aggressive policies to pursue suspected cybercriminals.

VULNERABILITIES

An unknown threat group compromised and released part of a code cache that contains exploits for multiple firewall products. Researchers and vendors continue to analyze the code, which purportedly belongs to the Shadow Brokers group (also known as Equation Group), and vendors have addressed several zero-day vulnerabilities. Organizations should prioritize installing security product updates, as threat actors have been quick to use the exploits to their advantage.

Several studies revealed poor security practices for both end users and computer-based technology. Organizations and individuals should monitor emerging threats for awareness and limit the attack surface by minimizing third-party apps on the corporate network that share sensitive data (for example, social network, chat, and file-trading software).

- Privacy may be compromised by software that uses address book, phone number, and even proximity data to create publicly available associations. Implications can include reportable violations in regulated fields such as healthcare and finance. Individuals should avoid accessing applications with a social media component from a corporate network, and avoid sharing private phone numbers or address books with third parties.
- In a study, 31% of employees clicked hyperlinks in a simulated phishing attack and 17% divulged sensitive information. In addition to positive education that rewards vigilant users, organizations should implement endpoint detection and protection controls to maximize trusted content presented to a user.
- Researchers reported on a study where individuals picked up 98% of USB drives dropped at a college campus, and monitored content was accessed on 45% of the drives. When possible, organizations should disable physical or logical access to USB adapters on hardware that contains sensitive data or can connect to corporate networks.
- Smartphone and mobile device users are vulnerable to multiple data leakage attack vectors via the recharging cable. In "video jacking," a malicious USB adapter can be configured to monitor the device's display. Individuals should always use their own recharger and avoid plugging the USB cable into an unknown system.

MALWARE

Malware distributors migrated from Neutrino to the RIG exploit kit to compromise systems with multiple malware families, striving to maximize monetization with coinfections. RIG developers aggressively tested new exploits to increase infections, and improved their command and control (C2) communications to evade detection. They also successfully recruited malware operators to use their service. CTU researchers recommend that organizations implement a patching process that addresses the vulnerabilities that exploit kits leverage, and to make employees aware of the many attack vectors available to spread malware.

Ransomware families such as Locky, Cerber, CryptXXX, and TorrentLocker diversified their infrastructure and expanded into traditionally less-affected geographic areas, such as the Asia-Pacific (AP) region. CTU™ researchers documented when ransomware incidents and variants were first reported to national computer security incident response teams (CSIRTs) in AP regions. While some malware families such as the Locky ransomware have rapid global distribution, typical time delays in expanding malware to other geographic regions can allow defenders to share threat intelligence and develop effective countermeasures prior to attacks. Organizations should implement security controls to minimize compromises from the most common attack vectors: exploit kits and spam email containing malicious attachments.

THREAT ACTORS AND METHODOLOGIES

A threat actor breached six point-of-sale (POS) systems for financial fraud and gained access to payment card data stored on more than one million POS systems. Media reports and some researchers attribute the breach to a Russian threat group named the Carbanak Gang, which reportedly has stolen millions of dollars from financial firms. Organizations using POS and other embedded systems should evaluate their exposure to these threats and minimize exposure where necessary. Remedies should include changing passwords on computers connected to networks that access payment systems.

Government-sponsored threat groups widened their scope of attacks, methods of compromise, and motives to fulfill their objectives. Groups linked to Russia, China, and Iran primarily engaged in cyberespionage to collect intelligence data, and secondarily pursued goals to disrupt systems. CTU researchers determined that North Korean threat actors are unique in attempts to acquire currency via bold cyberextortion techniques. Organizations should monitor world events to assess their degree of exposure, as government-sponsored threat actors frequently attack assets that may have links to the primary target. Organizations should also maintain vigilance to protect financial or personally identifiable information from unauthorized intrusion and disclosure.

LAW ENFORCEMENT AND GOVERNMENT

Several national governments and law enforcement bodies lobbied for aggressive policies to pursue cybercriminals. Organizations should monitor these developments for business impact and consider providing feedback on the legislation at an early stage.

- In the United States, the Department of Homeland Security (DHS) considered designating the U.S. election system as critical infrastructure, which would set security requirements and influence long-term cybersecurity investments.
- The Royal Canadian Mounted Police (RCMP) wanted a law that allows police officers to force suspects to reveal passwords for computing devices and online accounts.
- In the United Kingdom, police started a pilot project that hired private law firms to pursue criminals and seize assets in civil courts in an attempt to prosecute fraud. Critics are concerned that the lower burden of proof in civil courts versus criminal courts, as well as the profit motive, could impair the fairness and impartiality of the legal process.
- Pakistan passed a cybersecurity law that allows regulators to block private information deemed illegal, using vague language that could curtail free speech and lead to excessive prosecutions.

Arrests, indictments, prosecutions, and convictions in August included political activists, identity thieves, drug lords, insiders, and opportunists:

- International police arrested a Nigerian man known as "Mike," who managed 40 criminals across four countries to steal $60 million via payment diversion fraud and business email compromise (BEC). SecureWorks detailed the operations and provided recommendations that organizations can use to protect themselves against these attacks.
- A Danish man and a Sri Lankan teenager were arrested in two separate incidents for attacks on government websites. A Minnesota man using the handle "IcyEagle" was arrested for allegedly stealing bank passwords and selling them to the highest bidder. Three suspects in Finland associated with the now-defunct Silk Road cybercrime marketplace were arrested for drug smuggling.
- Gary Davis, who is known as "Libertas" and was linked to the Silk Road marketplace, was extradited from Ireland to the U.S. on hacking charges. A Ukrainian national suspected in the 2008 attack against RBS WorldPay was extradited to the U.S. for fraud.
- A New Hampshire man pleaded guilty to extorting victims and compromising social media accounts, and an FBI agent pleaded guilty to being a Chinese spy and selling classified technology.
- Roman Valerevich Seleznev, also known as "Track2," was found guilty of compromising POS computers to steal and sell credit card numbers.
- A Florida man received 70 months in jail for stealing $905,000 across five states in an ATM skimmer scheme, an Arizona man was sentenced to nine years for insider theft of $571,000, and an Australian teenager convicted of distributed denial of service (DDoS) attacks avoided jail but may pay restitution.

CONCLUSION

Trends and activities in August highlight the continued need for organizations to evaluate and apply security updates across vetted and approved software, especially as unpatched zero-day vulnerabilities hoarded by threat actors become public and are then exploited by many others. Monitoring world affairs may also allow organizations to anticipate and mitigate direct and collateral threats. Organizations must implement layers of security controls, such as ongoing employee education, endpoint threat detection, and a responsive incident reporting mechanism, to mitigate security incidents.

www.secureworks.com

I16

SECUREWORKS COUNTER THREAT UNIT THREAT INTELLIGENCE

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. Our IT security experts also provide Information Security Awareness Training solutions specific to your organizational needs. Leveraging our advanced security technologies and a network of industry contacts, the CTU research team tracks leading hackers 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 our customers 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.

A GLANCE AT THE CTU RESEARCH TEAM