MAY 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 clients protect their systems. The following events and trends were significant in April 2016:

1 MOBILE AND PC WEAKNESSES

Weaknesses in mobile and PC applications led to rogue updates, flawed update models, and the disclosure of sensitive data.

2 SECURITY UPDATES DELAYED

Delayed or unavailable security updates for hardware and software products caused vendors to rush to remove flawed code embedded in their products.

3 VERTICALS TARGETED

Analysts identified security issues plaguing the healthcare, education, and legal verticals.

4 MALWARE UPDATES

Malware experimented with novel exploits, delivery methods, evasion tactics, targets, and payment schemes.

5 SENSITIVE DATA STOLEN

Threat actors targeted various types of organizations to sell or dump stolen data.

6 CYBERSECURITY STRATEGIES

The U.S. and Australia released separate plans for a comprehensive cybersecurity strategy.

VULNERABILITIES

Mobile apps, traditional PC applications, and browser extensions contained flaws in their update and data exchange mechanisms, leading to unauthorized malicious updates, sensitive information disclosure, and discontinued apps that exposed abandoned data. Researchers and regulatory agencies focused on flawed update models that permit malvertising, trick victims into installing malware, and fail to warn users of end-of-life or unsupported software. When possible, clients should whitelist vetted software for users to install, regularly update apps and the underlying operating system, and uninstall discontinued software.

Several vendors announced delayed security updates or no updates, forcing vendors to quickly adapt. Adobe scrambled to remove Apple QuickTime for Windows code embedded in their products. Publicly disclosed vulnerabilities in some Moxa hardware may not be addressed until August, and some Quanta routers will not be patched. Clients should maintain a regular schedule of software and hardware upgrades well in advance of vendors' end-of-support announcements and consider alternate solutions for when major vulnerabilities or exploits make the primary solution risky to use.

Security analysts noted that the healthcare, education, and legal verticals increasingly became targets due to the data they possess and common security weaknesses. The use of Windows XP, Internet Explorer, and Flash were cited for poor security in the healthcare vertical, while a JBoss vulnerability in a popular library management system used by organizations in the education vertical was exploited by the SamSam ransomware. Legal firms were advised to improve data encryption, limit access to sensitive data, run background checks on new employees, and implement data access and exfiltration defenses.

MALWARE

Although ransomware received the most media attention for its rapid evolution and widespread damage, all malware types implemented significant upgrades and experimented with new functionality across a range of features. The changes included exploiting both legacy and zero-day vulnerabilities, targeting geographic regions relatively unaffected by malware, evading detection and circumventing defenses with fileless infections and overlays, and expanding ransom demands beyond bitcoins to include payment methods such as gift cards. Clients should implement best practices for defending against and mitigating malware, such as preventing the installation of unvetted software, making employees aware of suspicious situations and actions, deploying host-based and network-based countermeasures, and setting up an incident management team to isolate and restore compromised systems.

THREAT ACTORS AND METHODOLOGIES

The media followed developments with the Bangladesh Bank cyberattack that began in March. CTU™ researchers analyzed official statements, press reports, and potential malware that suggests a North Korean threat actor targeted the SWIFT (Society for Worldwide Interbank Financial Telecommunication) financial transaction software to monitor, manipulate, and delete fraudulent transfers. Clients should review the tools and techniques associated with this attack to evaluate and manage the potential risks to equivalent systems.

Multiple threat actors targeted hospital databases, government voting and citizenship databases, an offshore legal firm, university and corporate personnel data, and dating websites to sell and leak sensitive data online. The stolen data may be used for financial gain, additional attacks, or to embarrass victims. While users are typically forced to change account passwords after a breach, clients should educate users about the dangers of reusing login credentials. Clients should also protect sensitive information by collecting and storing only essential data, using encryption, implementing strong access controls such as two-factor authentication, and deleting obsolete or unnecessary data.

LAW ENFORCEMENT AND GOVERNMENT

U.S. president Barack Obama created the Commission on Enhancing National Cybersecurity to recommend what the government and private sector can do over the next decade to improve computer security. Australia appointed a special advisor on cybersecurity and published "Australia's Cyber Security Strategy," a comprehensive paper summarizing five aspects to "elevate cybersecurity as an issue of national importance." The recommendations and actions will likely have significant impact as governments and constituents debate regulation and standards. Clients should monitor developments and consider providing comments to legislators and advocates.

There were several notable arrests and prosecutions, with judgments ranging from light punishment to death

- The author of the Spyeye malware and a co-conspirator pleaded guilty and were sentenced to a total of 24 years in prison. The Blackhole exploit kit author, known as "Paunch," was sentenced to seven years in a Russian penal colony for stealing at least $2.3 million with the malware and enabling other criminals to grow botnets based on the Zeus and Citadel trojans. A UK minor pleaded guilty to selling booter software used for distributed denial of service attacks and received a suspended two-year sentence, restitution, and community service.
- Two unrelated couples involved in fraud against the U.S. Internal Revenue Service (IRS) were brought to justice. One couple pleaded guilty to filing fraudulent returns using data stolen from the IRS "Get Transcript" database, and the other couple was arrested for preparing inflated tax returns as IRS employees and pocketing the ill-gotten gains.
- A journalist convicted of providing an Anonymous hacktivist with login credentials to a Los Angeles Times newspaper website and retaliating against a former employer was sentenced to two years in prison, while his Anonymous accomplice in Scotland received a warning.

CONCLUSION

Events in April 2016 reinforced the importance of implementing and maintaining a robust, carefully vetted, and updated set of vendor-supported hardware and software, as malware took advantage of a panoply of legacy and zero-day vulnerabilities. Rapid reaction from properly prepared incident response teams when security incidents occur can help minimize the damage from a cyberattack and reduce the time and costs of restoring compromised systems.

www.secureworks.com

E16

SECUREWORKS COUNTER THREAT UNIT™ (CTU) 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 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.

A GLANCE AT THE CTU RESEARCH TEAM