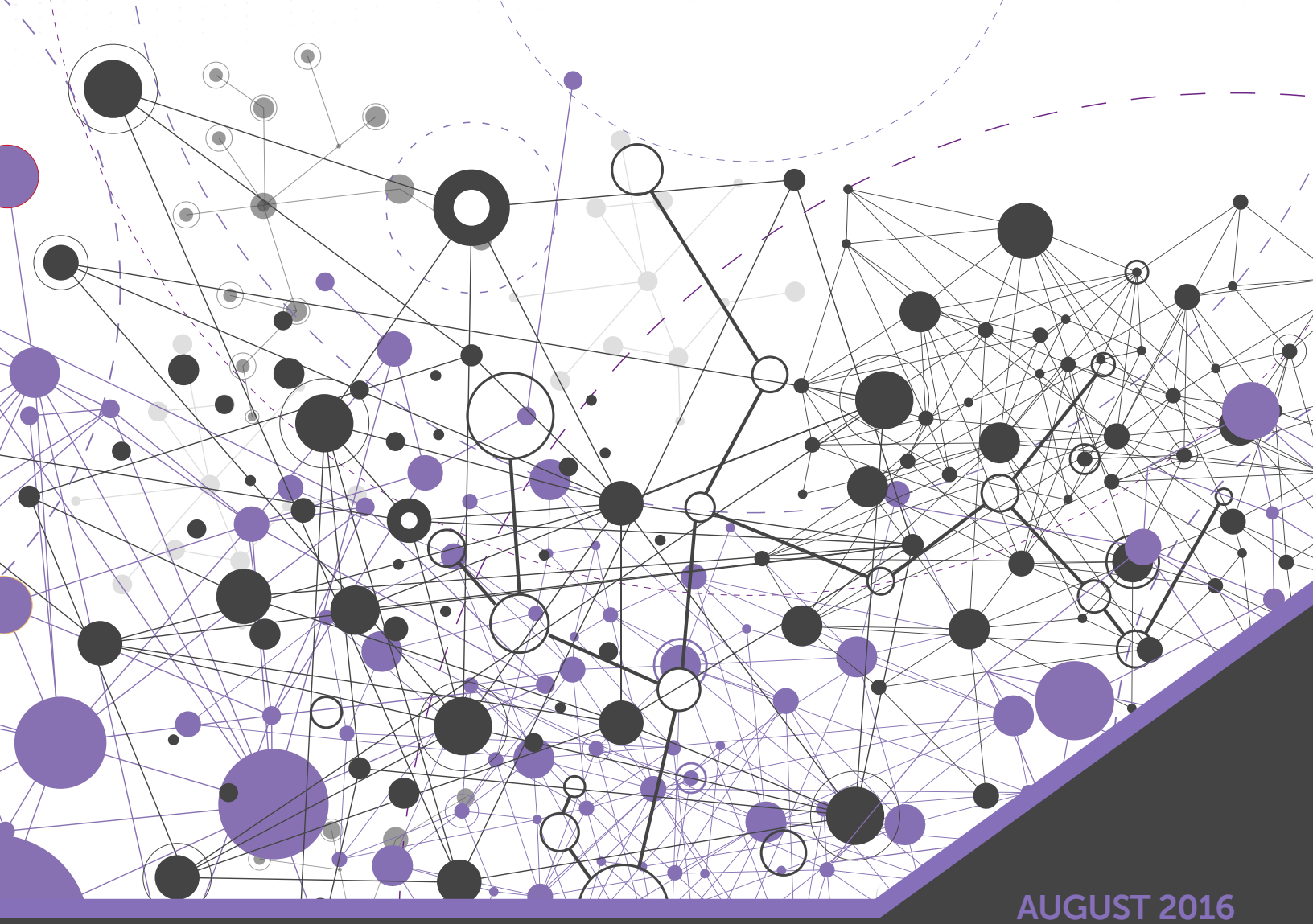


AUGUST 2016

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 July 2016:

1 VULNERABILITIES AFFECTED SENSITIVE DATA

Researchers disclosed vulnerabilities in widely deployed software that handles sensitive data.

2 BUSINESS WEBSITES COMPROMISED

Business websites and platforms were compromised and used to spread malware.

3 RANSOMWARE ADDED FEATURES

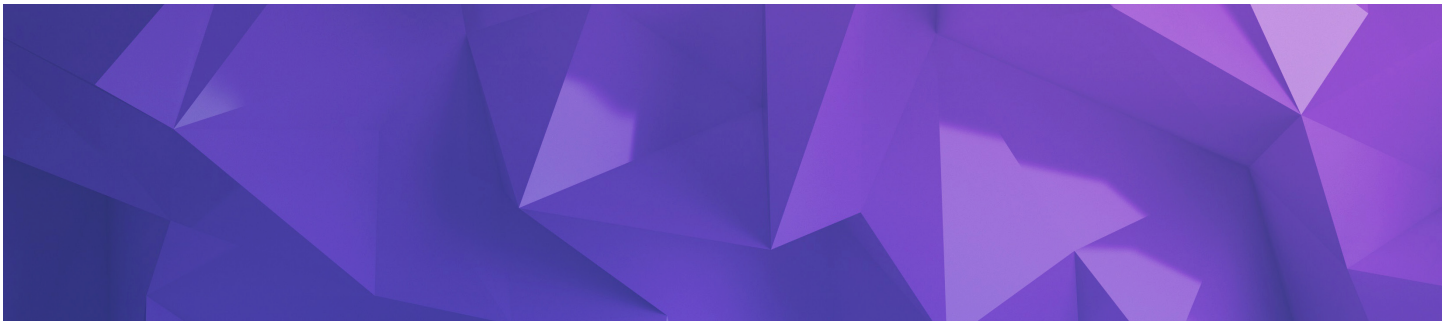
Ransomware added conventional malware features, and exploit kit and downloader capabilities were enhanced to support ransomware.

4 DATA STOLEN AND LEAKED

Many threat groups committed cyberespionage and leaked data to support various causes or for financial gain.

5 GOVERNMENTS ADDRESS THREATS

Computer security-related government initiatives and legislation addressed emerging threats, but some of the policies were criticized.



VULNERABILITIES

Researchers disclosed vulnerabilities threatening secure communication, data transmission, and storage in several mobile apps and personal security software platforms. Software that interacted with sensitive data, such as the WhatsApp, FaceTime, and Telegram messaging apps, the Amazon Kindle web browser, the Micro Focus Filr file-sharing manager, the Little Snitch Mac OS X firewall, and the LastPass password manager, issued updates to address the weaknesses. Organizations should regularly update software and develop a whitelist of approved apps to facilitate maintenance and limit exposure.

Threat actors compromised multiple content management systems (CMS) and ecommerce websites to ultimately infiltrate business websites to host and propagate malware. In addition to updating software, organizations should consider the risks versus benefits of incorporating third-party extensions and plugins, and should segregate Internet-facing systems from internal networks. For example, employees' workstations should use sandboxing software when accessing Internet-facing systems to avoid infecting internal networks.

MALWARE

Ransomware is increasingly used for financial fraud due to its low risk, low maintenance, and quick financial returns. In addition to the introduction of many new ransomware families in July, the Ranscam ransomware incorporated destructive wiper features present in conventional malware, and the Troldesh ransomware added downloader capabilities. Exploit kits and downloader trojans also evolved to support ransomware. These developments underscore the importance of protecting against all malware types with host-based countermeasures, continuing regular patching, and performing "cold" or unconnected data backups.

Ransomware effectiveness was weakened by threat group sabotage and flawed code. The criminals operating the Petya ransomware released decryption keys for the competing Chimera ransomware, and operators of the CryptXXX ransomware provided decryption keys for the .crypz and .cryp1 versions. One CryptXXX version featured a defective decryptor that could not recover compromised data. Researchers can exploit these flaws to develop decoders that could allow victims to recover their damaged data. CTU researchers and others in the security community recommend avoiding contact with threat groups, as payment does not guarantee recovery. In addition, organizations should research if decoders are available for ransomware that infects their networks.

THREAT ACTORS AND METHODOLOGIES

Threat groups committed cyberespionage and leaked data for ideological and economic motivations:

- WikiLeaks dumped 20,000 stolen emails from the Democratic National Committee (DNC), and unknown threat actors sympathetic to Russia may have attacked the Democratic Congressional Campaign Committee (DCCC) to gather information on donors. Organizations should employ multifactor authentication and use end-to-end encryption to protect sensitive data in emails and attachments.
- Chinese hacktivists targeted systems at two Vietnamese airports and compromised an airline website that contained passenger data, causing banks to take defensive measures. Individuals should be vigilant for anomalous activity on their payment cards and carry a rarely used additional card as a backup.
- The Anonymous hacktivist group launched distributed denial of service (DDoS) attacks against Brazil for blocking the WhatsApp messenger service, planned cyberattacks to coincide with Black Lives Matter protests, and leaked data from South Africa's arms procurement agency. In addition, Anonymous dumped data supplied by the Phineas Fisher threat group in protest of the Turkish administration and Syrian attacks. Organizations in targeted verticals or working with targeted companies should review DDoS mitigation tactics, ensure that Internet-facing systems are up to date and secured, and advise personnel to be vigilant for spearphishing attacks.
- CTU researchers profiled the North Korea and China governments' use of threat groups to wage economic espionage against a broad range of targets. Organizations that generate or manage intellectual property, particularly those in the agriculture, energy and mining, services, construction, manufacturing, and retail verticals, are at increased risk of attack. Clients at high risk should consider intelligence-driven endpoint threat detection tools as part of an overall threat mitigation plan.

LAW ENFORCEMENT AND GOVERNMENT

Several countries attempted to improve cybersecurity via legislative, regulatory, and quasi-governmental initiatives, but critics considered some of the policies misguided or harmful:

- U.S. Presidential Policy Directive PPD-41 defined a comprehensive process for the U.S. government to evaluate, rank, and respond to significant Internet-based threats. The directive also clarified how information may be shared among public and private organizations and government agencies. Criticism is mixed, with some security professionals saying the process is too complex and others claiming it does not address emerging threats. Organizations should monitor the implementation and evolution of this initiative to leverage intelligence-sharing channels and efficiently coordinate threat responses.
- U.S. industry groups and regulatory agencies issued new guidance and best practices for mitigating threats to new technologies. The Automotive Information Sharing and Analysis Centers (Auto-ISAC) issued best practices for vehicle cybersecurity. The U.S. Department of Health and Human Services (HHS) released guidance for ransomware that included a discussion of ransomware's impact on Health Insurance Portability and Accountability Act (HIPAA) regulations, specifically for incident response and reporting. Organizations affected by these regulations should monitor changes to ensure compliance.

- Russia and Ireland sought to expand communication interception powers. Russian president Vladimir Putin ordered intelligence services to produce Internet decryption keys, a request many researchers consider unpractical. The Irish deputy prime minister requested laws to intercept criminals' email and social media communications, similar to the United Kingdom's (UK) Investigatory Powers bill pending in the UK Parliament. Organizations doing business in these countries should follow developments and consider the risks of storing or transiting data through affected jurisdictions.

Notable arrests, pleas, and convictions occurred in July:

- Europol arrested 105 suspects across 15 countries for credit card fraud, and INTERPOL arrested a Nigerian national for masterminding business email compromise (BEC) scams valued at $60 million. A couple offering malware encryption services to cybercriminals was arrested in the UK, and three suspects were arrested in Taiwan for stealing $2.5 million from more than 1,000 ATMs.
- Five executives from a UK-based security reseller pleaded guilty to breaching a rival's database to steal customer information and pricing data.
- Five Russian nationals living in the UK received sentences ranging from 18 weeks to more than seven years for their roles in a money laundering scheme that used malware to steal $1.31 million. The head of the international "StubHub hackers" scam ring who stole $1.6 million was sentenced to at least four years in jail, and the cases of three codefendants are pending. A system administrator for a large bank was sentenced to 21 months in jail for deleting 90% of the bank's router configurations and disrupting the network for hours. The former scouting director for the St. Louis Cardinals baseball team was sentenced to 46 months in jail for illegally accessing another team's player database.

CONCLUSION

Fundamental information security practices can minimize the impact of evolving threats and techniques. CTU researchers recommend that organizations focus on deploying timely security updates, using strong encryption for data in transit and in storage, enforcing multifactor authentication for access to sensitive systems and data, and implementing off-site data backups.

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