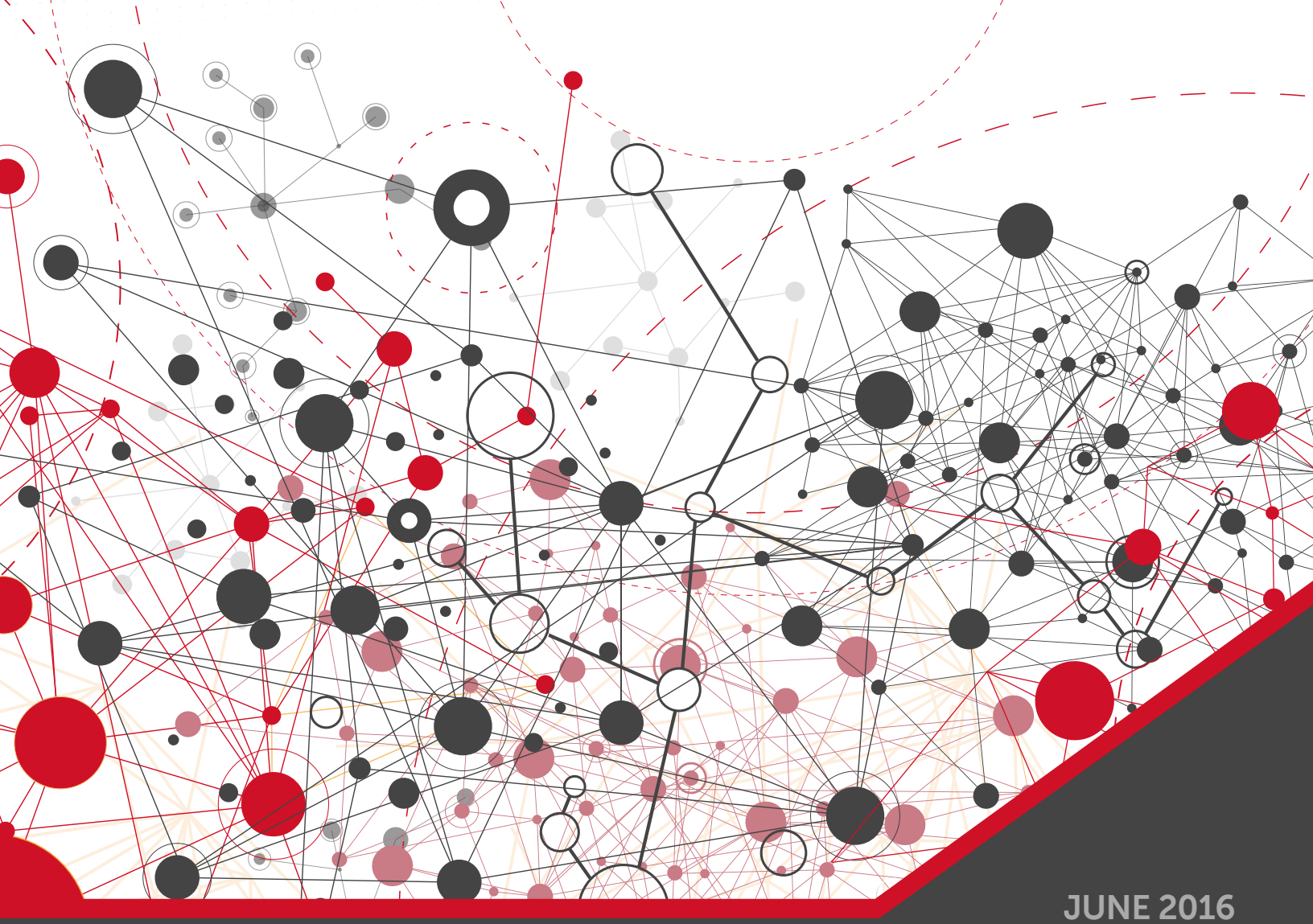


JUNE 2016

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 May 2016:

1 PRECAUTIONARY PASSWORD RESETS

Breaches of several major websites and social media portals prompted many unaffected organizations to reset passwords or ban common passwords.

2 UBIQUITY COMPLICATES PATCHING

Multiple flaws in widely used software, including some in active exploitation, resulted in hurried patches and organizations struggling to identify affected systems.

3 RANSOMWARE SHIFTS

TeslaCrypt ransomware developers ceased operations and voluntarily released its decryption keys, but threat actors migrated to CryptXXX (also known as UltraCrypter) and Cerber.

4 ATTACKERS EXPAND OPERATIONS

Anonymous factions conducted attacks against multiple verticals, and CTU™ researchers discovered that Threat Group-2633 (TG-2633) upgraded one of its key malicious tools.

5 GDPR ENTERS GRACE PERIOD

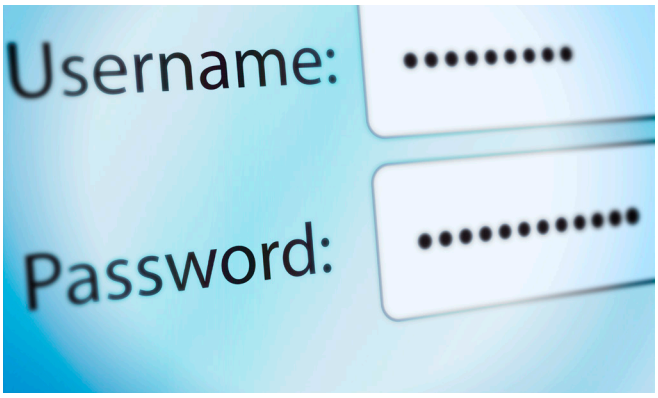
Following the termination of the Safe Harbor agreement, the European Union (EU) ratified the General Data Protection Regulation (GDPR) and started its two-year grace period, encouraging organizations to examine their storage and sharing controls.

6 U.S. HOUSE SUSPENDS ACCESS

The U.S. House of Representatives suspended access to Google and Yahoo services pending resolution of security concerns.

VULNERABILITIES

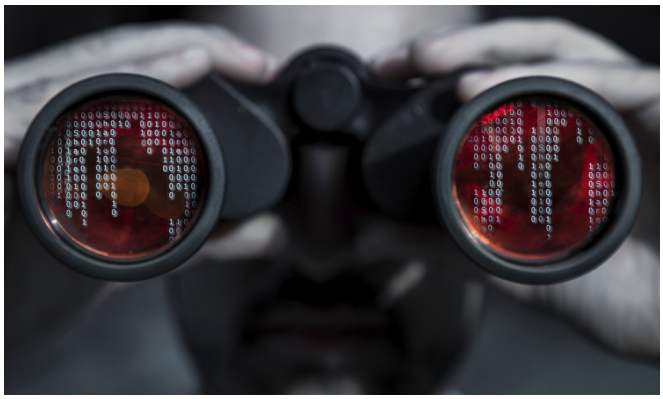
Large breaches and the subsequent disclosure of user credentials and sensitive data prompted owners of unaffected sites to reset passwords or ban commonly used passwords that appeared in data dumps. Clients may want to implement security controls that prevent credential reuse, discourage similar passwords across platforms, and establish password-aging policies.



Organizations struggled to determine if they were affected by vulnerabilities in several popular software products that are commonly included in other software or integrated into corporate infrastructure. Some issues were recent, while others had persisted for years. Adobe released updates to address zero-day vulnerabilities that have been exploited by malware since March 2016. Exploitation of an SAP vulnerability addressed in 2010 reportedly compromised at least 36 organizations, illustrating the challenge of identifying cybersecurity risks affecting installed software products. Clients should audit systems for weaknesses, work with vendors to identify product vulnerabilities and produce security updates in a timely manner, and test and apply appropriate software updates as soon as possible.

MALWARE

Developers of the popular TeslaCrypt ransomware shut down operations and released the master decryption key, allowing most victims to decrypt affected computers using a third-party application. The threat actors gradually migrated to the CryptXXX (also known as UltraCrypter) and Cerber ransomware families, which provide more features and correctly implement strong encryption. Clients can reduce the impact of ransomware by preventing arbitrary software installations, limiting write access to static archives, instituting regular off-site backups, and installing security updates.



In May, CTU researchers analyzed multiple Angler exploit kit campaigns that used spam, malvertising, and spearphishing to deliver malware such as the Bugat v5 (also known as Dridex) and Nymaim trojans. In addition to applying network and host-based countermeasures, clients should educate employees about new spam techniques, limit the ability to run software from arbitrary folders, and set up security controls using threat indicators associated with the malicious activity.

THREAT ACTORS AND METHODOLOGIES

Threat actors invested considerable effort into evading traditional network-based protections such as intrusion detection systems (IDS) and firewalls by leveraging native applications and features, such as the Windows Management Instrumentation (WMI) toolset and the PowerShell automation framework. Host-based security software may be more efficient at detecting anomalies from malware or advanced persistent threat (APT) activity.

Multiple threat groups using the Anonymous moniker dumped sensitive data and launched distributed denial of service (DDoS) attacks against the financial, government, and education verticals. In addition to implementing a DDoS mitigation strategy, clients should monitor brands and other indicators associated with their business activity for threatening or malicious activity, and respond accordingly to reduce the impact of an attack or data leak.

CTU researchers analyzed the activity of Threat Group-2633 (TG-2633) and Threat Group-2889 (TG-2889), which both maintain and deploy custom information-stealing malware for different goals. TG-2633 traditionally targets healthcare, technology, and telecommunication organizations in the United States, Korea, Japan, and Australia and was observed upgrading its AceHash credential-theft tool to steal intellectual property, possibly for financial gain. TG-2889 uses social networks to target the telecommunication vertical in the Middle East and compromise networks with the Helminth remote access trojan, possibly for government intelligence. Clients in all industries, particularly in the targeted regions and verticals, should establish guidance for social media interactions, instruct employees on how to handle phishing attempts, monitor externally facing systems and employee workstations for unauthorized accesses or modifications, limit privileges and avoid credential reuse across systems that threat actors could use for lateral movement, centralize logs in real-time, and create alerts for local modifications to log files.

LAW ENFORCEMENT AND GOVERNMENT

The EU General Data Protection Regulation (GDPR) started its two-year grace period preceding implementation of new regulations and obligations for any organization handling EU citizens' data, regardless of its location. Clients that store EU data or share data with organizations in the EU, especially via cloud-based applications, should evaluate the regulations, examine their storage and sharing controls, and verify their systems are in compliance.

In reaction to an increase in ransomware phishing attacks, the U.S. House of Representatives blocked access to Yahoo Mail and Google Gmail. The House also temporarily blocked access to Google-hosted cloud apps until a vulnerability identified by the Federal Bureau of Investigation (FBI) was addressed. Clients should evaluate potential attack vectors and the risks they pose to networks, considering scenarios where a service in widespread use must be withdrawn for security reasons. Identifying similar services such as an alternate cloud app, web browser, or software may lessen the disruption.

Law enforcement and the court system arrested, indicted, and prosecuted multiple individuals, including several security researchers. Techniques for legal security research vary by country, and clients engaging in independent research must use documented procedures when investigating and disclosing security issues.

- Four unrelated researchers who uncovered flaws in an elections website, a governmental tax website, medical software, and a government's secure communications system face charges and sentencing. In addition to publicly disclosing the weaknesses, the researchers illegally intruded upon the systems to demonstrate the vulnerabilities and exposed sensitive data.
- Courts obtained guilty pleas from a New Zealand man accused of accessing financial networks to obtain bank and credit card details for fraud, U.S. and Bahamian citizens who hacked into celebrities' accounts, and a Ukrainian national who accessed three business newswires to commit securities fraud.
- A Louisiana man was sentenced to prison and supervised release after being convicted of compromising computers to obtain credit card data, bitcoins, and access credentials, and selling stolen information on the Darkode hacking forum. A Russian man convicted of creating the Gozi malware was sentenced to $6.9 million restitution and three years of time served.

CONCLUSION

The threat activity in May illustrates how an evolving and adaptive security environment that provides host-based detection, brand and social media surveillance, contingency processes, employee awareness of new threats, credential aging, and timely security updates can provide early warning of malicious activity, minimize risk, and promote business continuity.

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