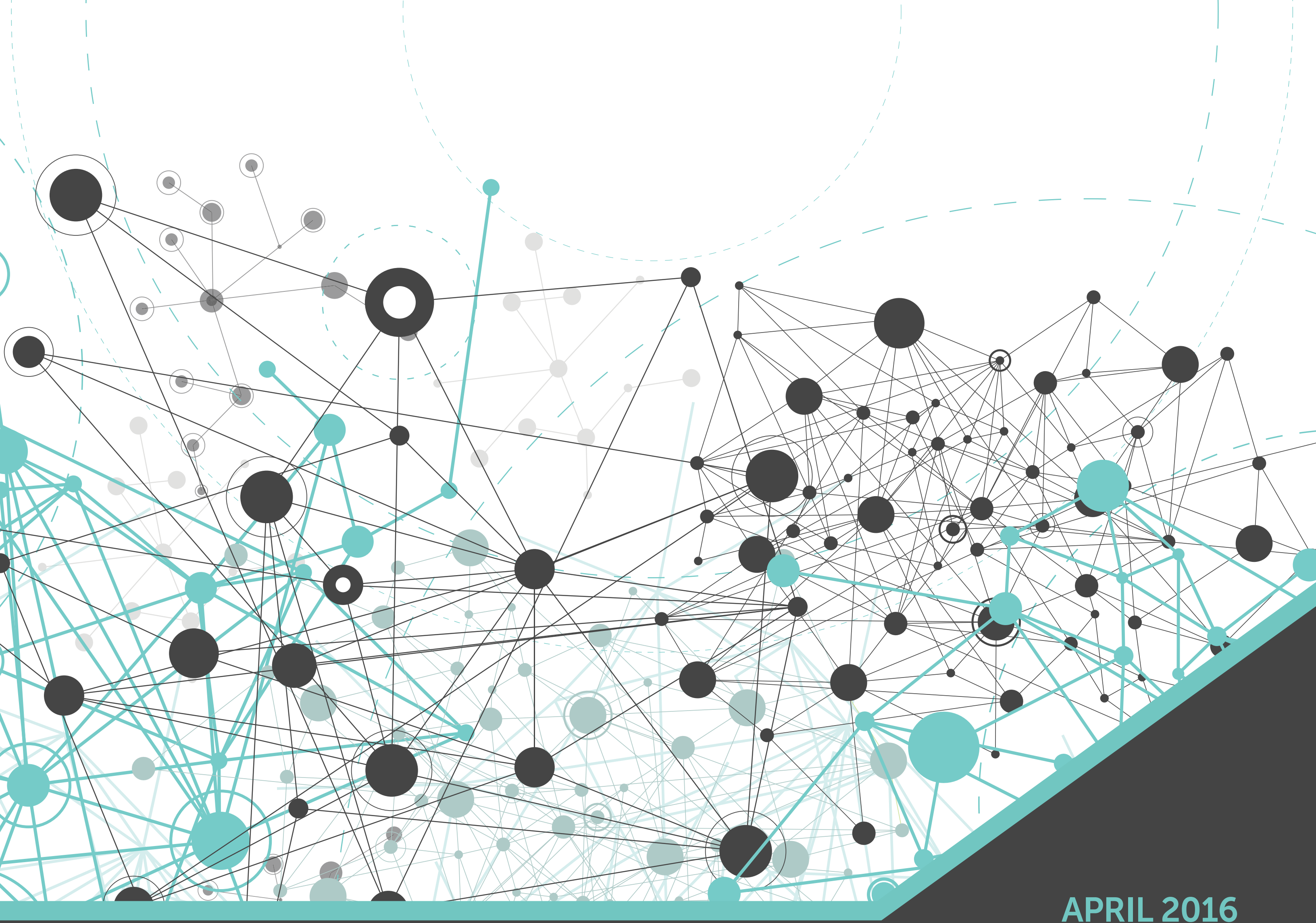

APRIL 2016

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 March 2016:

1 SYSTEMS EXPOSED

Vulnerabilities in ubiquitous corporate products and mobile devices presented lucrative targeting opportunities.

2 LAX POLICIES = RISKS

Misconfigurations and lax security policies introduced risks for data theft, financial fraud, and further compromises.

3 RANSOMWARE REIGNED

Ransomware was the most popular malware type, which led to many more infections and innovations than other malware types in March.

4 FINANCIAL ORGANIZATIONS HIT

Threat actors focused on targets in the financial vertical.

5 ENCRYPTION DEBATE UNRESOLVED

The FBI unlocked a terrorist's iPhone without Apple's assistance, continuing the war between encryption and law enforcement access.

VULNERABILITIES

Researchers discovered major flaws in several low-profile but widely used products that support corporate infrastructure. A badged door controller, a web conferencing service, a medical supply system, and many brands of mobile devices include severe remote code execution vulnerabilities that clients must address by installing and testing security updates. Using mobile device management (MDM) could assist with maintaining security policies on mobile devices connected to the corporate network.

Several reports of misconfigured systems and weak security policies illustrated the importance of evaluating systems and processes to avoid an incident or close call:

- Use of default manufacturer passwords on legacy systems such as SAP exposed sensitive data to the Internet. Clients should use available tools to scan for credential weaknesses, apply security updates, and enforce strong usernames and passwords.
- Attackers leveraged shared accounts and remote administrative access to impersonate employees and attempt financial fraud at Kenyan and Ugandan banks. Clients should establish individual accounts for authorized users that use the principle of least privilege, log access and activity on sensitive systems, and implement out-of-band verification for financial integrity.
- Scans of popular web servers and virtual private network (VPN) services revealed misconfigurations that exposed systems and users to attacks that could compromise encrypted data and potentially allow cross-site scripting (XSS), cross-origin resource sharing (CORS), and cross-site request forgery (CSRF) compromises. Clients should periodically evaluate servers and services for insecure settings and deprecated protocols.

MALWARE

Ransomware dominated malware activity and mainstream media coverage in March. Hospitals were reportedly a favorite target of ransomware threat actors, with some reports attributing the attacks to Chinese and Turkish criminals. CTU researchers investigated incidents that used SamsamCrypt (also known as SamSam or Samsa) and Maktub Locker ransomware to compromise targets via phishing emails and exploit kits. Ransomware authors also added capabilities and features:

- The Petya ransomware overwrites the master boot record (MBR) to prevent file recovery.
- TeslaCrypt leveraged Windows management instrumentation (WMI) to delete shadow volume copies and disrupt automatic backups.
- KeRanger became the first Mac OS X ransomware, and threat actors compromised the popular Transmission BitTorrent software to infect systems.
- The Android-based LockDroid ransomware spread to Japan via direct downloads and malvertising.

Clients should adopt a multi-pronged defense and mitigation strategy that includes educating users about evolving infection vectors, whitelisting software installation, using host-based security software to detect compromise, implementing offline backups, and identifying available ransomware decryption keys. CTU researchers also recommend that clients verify data-restoration processes and rehearse business continuity from non-compromised systems such as paper-based records.

THREAT ACTORS & METHODOLOGIES

Experienced threat actors attacked the central bank of Bangladesh, reportedly accessing the bank's SWIFT payment system to attempt to transfer $951 million to Asian accounts. Suspected fraud and a misspelling in one of the transfers stopped all but $81 million. The threat actors bypassed fraud detection systems, exploited reduced security during a bank holiday, and moved currency across international borders. Financial clients should verify data used to create accounts, implement strong access controls such as multifactor authentication, independently validate transactions, and be suspicious of activity at irregular times.

CTU researchers and others in the security community documented methodologies that threat actors are increasingly employing to attain their objectives. These techniques included stealing credentials, targeting exploits on unpatched systems, using a combination of stolen code-signing certificates to gain victims' trust, and socially engineering victims via a business email compromise (BEC). Multifactor authentication, host-based detection systems, timely application of security updates, out-of-band verification, awareness training, installation restrictions, and rapid incident response can help prevent and mitigate compromises.

LAW ENFORCEMENT AND GOVERNMENT

The U.S. Federal Bureau of Investigation (FBI) dropped its legal demand that Apple unlock a device implicated in a terrorist investigation after the FBI was able to access the device's contents. The issue of mandating encryption backdoors remains unresolved, and the FBI is not required to disclose the exploited zero-day vulnerability. Clients should employ management software to secure data on corporate-issued devices or devices that connect to a corporate network, apply security updates to guard against known vulnerabilities, and retain control of the computing asset or its data.

Law enforcement and judiciaries issued indictments, arrests, and convictions, while self-incriminating and escaping cybercriminals also made the news:

- The U.S. charged seven Iranians suspected of attacking financial institutions as part of Operation Ababil, and three alleged members of the Syrian Electronic Army (SEA). Israel indicted an Islamic Jihad member for compromising drones and spreading laterally to other networked systems, such as airport databases.
- A UK citizen was arrested, pleaded guilty, and was given a token sentence for several attacks on the Moonpig website. Other guilty pleas include a Turkish citizen charged with hacking into ATM and payment card processing systems, and a Chinese national who illegally accessed U.S. defense contractor computer systems.
- The New York man who broke into his former employer's network, erased data, and installed backdoors was convicted and could be sentenced to prison and a fine.
- A Romanian hacker known as GhostShell provided lengthy press interviews and disclosed self-incriminating evidence in the hopes of being arrested and eventually gaining a job in the security industry. Another Romanian suspect arrested as part of an international ATM cybercrime group escaped from prison and is still at large.

CONCLUSION

Threat groups interested in ill-gotten financial gains are gravitating towards ransomware, which involves less risk and has advanced much faster than other types of malware. Clients must focus on the fundamentals of a security plan that emphasizes user awareness training, appropriate rights management, early host-based detection, timely security updates, continuous offsite backups, and a rapid incident response team.

www.secureworks.com

D16

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