JULY 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 June 2016:

1 LAX SECURITY CAUSED LEAKS

Data from several organizations was leaked online due to inadequate security controls on the software that manages or stores the data.

2 SERIOUS VULNERABILITIES SURFACED

Severe vulnerabilities in security software and networking hardware, as well as the perennial Adobe Flash zero-day vulnerabilities in exploitation, raised tensions for network administrators.

3 MALWARE ACTIVITY FLUCTUATED

Malware and botnet activity mysteriously and abruptly ceased, and in some cases later resumed.

4 U.S. CAMPAIGN TARGETED

Threat Group-4127 targeted a U.S. presidential campaign.

5 CYBERSECURITY PRINCIPLES REAFFIRMED

The European Union (EU), United Kingdom (UK), and United States (U.S.) reaffirmed cybersecurity governance principles following the UK's decision to leave the EU.

VULNERABILITIES

Researchers discovered threat actors exposing sensitive data from inadequately protected networks and databases. Details from healthcare provider and health insurer databases, online forums, a travel agency, and more than 100 poorly secured MongoDB databases were made available, and many of the impacted organizations were unaware of a breach. Organizations should employ a brand surveillance service to monitor for potential threats, should audit systems for vulnerabilities, and should apply security updates and security controls to systems handling sensitive data.

Several severe vulnerabilities in popular hardware and software products reinforced the need to apply timely security updates:

- Symantec addressed a flaw in multiple security software products that could lead to a full compromise without user interaction. Other vendors announced updates and workarounds for several routers, firewalls, and security appliances. Organizations should prioritize security updates for security and networking products, as exploitation could have serious consequences.
- Adobe scrambled to address a Flash zero-day vulnerability used in targeted attacks by the newly identified ScarCruft threat group. Foxit also addressed 12 vulnerabilities in its PDF reader software. Organizations should routinely audit systems to identify which software packages are deployed, determine if any should be uninstalled due to security risks, and ensure that even lesser-used software packages are regularly updated.
- Research on original equipment manufacturer (OEM) updaters revealed that most computer vendors continue to ship preconfigured systems with vulnerable software and lax default security settings. Organizations should fully erase hardware and provision software from known clean images prior to deploying the system in the organization.

MALWARE

Multiple exploit kits and botnets abruptly ceased activity or operated at a reduced capacity in June, and in one case subsequently resumed normal operations. The reemergence of activity reinforces the importance of continuing to update security controls even if a threat seems to have disappeared. Organizations should apply emerging indicators to intrusion detection systems, secure all systems with security updates, make personnel aware of new attack vectors, and monitor networks for anomalous activity.

- The Angler exploit kit's code and infrastructure was continually updated until it became inactive in early June. Criminals shifted to using Neutrino, possibly finding appeal in its improved exploits and well-developed attack infrastructure.
- The Necurs botnet vanished and then reemerged later in the month. Prior to its disappearance, it was the largest botnet and distributed the Locky ransomware and Bugat v5 (Dridex) banking trojan. When Necurs resumed activity, it was distributing a Locky variant named Zepto.
- Bugat v5 botnet activity reportedly stopped, but CTU™ researchers concluded the botnet was functioning at a reduced capacity.

THREAT ACTORS AND METHODOLOGIES

Threat Group-4127 (TG-4127) has historically targeted governments, military, and international non-governmental organizations. In June 2016, TG-4127 abused the Bitly URL-shortening service to launch spearphishing campaigns against Gmail accounts belonging to staff associated with Hillary Clinton's U.S. presidential campaign and the Democratic National Committee. Because threat actors shift targets based on opportunistic factors and unknown objectives, clients should educate personnel about recognizing and handling spearphishing emails, confirming that websites are legitimate, and using caution when accessing shortened URLs. For example, users can access the full URL associated with the Bitly link by appending a plus sign (+) to the Bitly URL in the web browser address bar.

LAW ENFORCEMENT AND GOVERNMENT

Cybersecurity governance practitioners expressed concern in the wake of the United Kingdom's (UK) decision to leave the European Union (EU). The United States (U.S.) and the EU reaffirmed existing agreements to address business uncertainties. The EU-approved General Data Protection Regulation (GDPR) that covers data privacy and management will likely be replicated in the UK to minimize trade barriers, and exit negotiations are expected to take between two and six years. Organizations that have been preparing for or complying with the GDPR for international data storage and transfer should be optimally positioned but should continue to monitor developments.

Several notable arrests, pleas, and convictions occurred in June:

- U.S. prosecutors charged a Filipino man accused of running a large identity-theft scheme targeting celebrities, and charged a Chinese national with economic espionage for stealing his employer's source code. U.S. Securities and Exchange Commission (SEC) regulators froze the assets of a British citizen accused of hacking brokerage accounts to manipulate stock prices.
- A telecommunications employee in the Czech Republic was arrested before he could sell data belonging to 1.5 million customers, and the Russian police arrested 50 members of a cybercrime group that stole more than $45 million from Russian banks.
- Courts worldwide obtained guilty pleas from a Kosovo national who stole and dumped U.S. service members' data on behalf of the Islamic State, two of three men who stole a database and generated more than $2 million in identity theft, and two Israeli citizens extradited to the U.S. who stole personal information from 83 million customers.
- The decade-long case against spam king Sanford Wallace concluded when he was sentenced to 2.5 years of prison for compromising 500,000 Facebook accounts and using them to send 27 million spam messages. Brian "DoctorClu" Farrell, the second-in-command at the Silk Road 2 underground website, was sentenced to eight years of prison.

CONCLUSION

Organizations can take proactive steps to improve their security profile. Regularly evaluating and applying software and firmware security updates can minimize the number of vulnerable systems within an organization and reduce possible attack vectors. Brand surveillance services can identify breaches or unintended exposure that threat actors might be able to leverage. Malware and threat groups are constantly changing tactics, often for unknown reasons, so a takedown or disappearance of malware activity is not a reason for complacency.

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