NOVEMBER 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 October 2016:

1 ZERO-DAY VULNERABILITIES EXPLOITED

Threat actors exploited Windows and Flash Player vulnerabilities prior to vendors issuing out-of-band updates.

2 DEVICES CAUSED DATA LEAKS

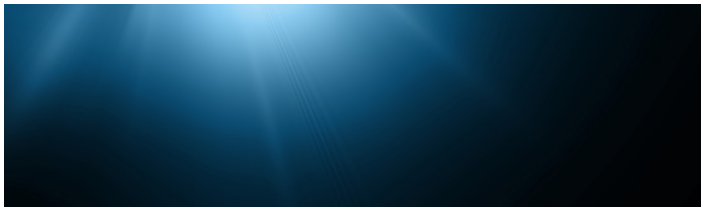
Researchers discovered data leaks in sensitive networks from devices that were not originally intended to be connected to the Internet.

3 RANSOMWARE CHANGED TACTICS

Ransomware experimented with delivery mechanisms and varied encrypted file formats and extensions.

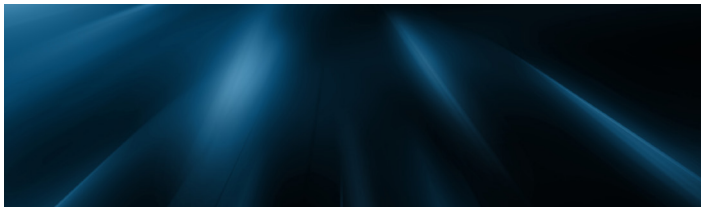
4 BANKING TROJAN REUSED CODE

Code from the defunct Dyre banking trojan was reused in the TrickBot banking malware.



5 GOVERNMENT ORGANIZATIONS TARGETED

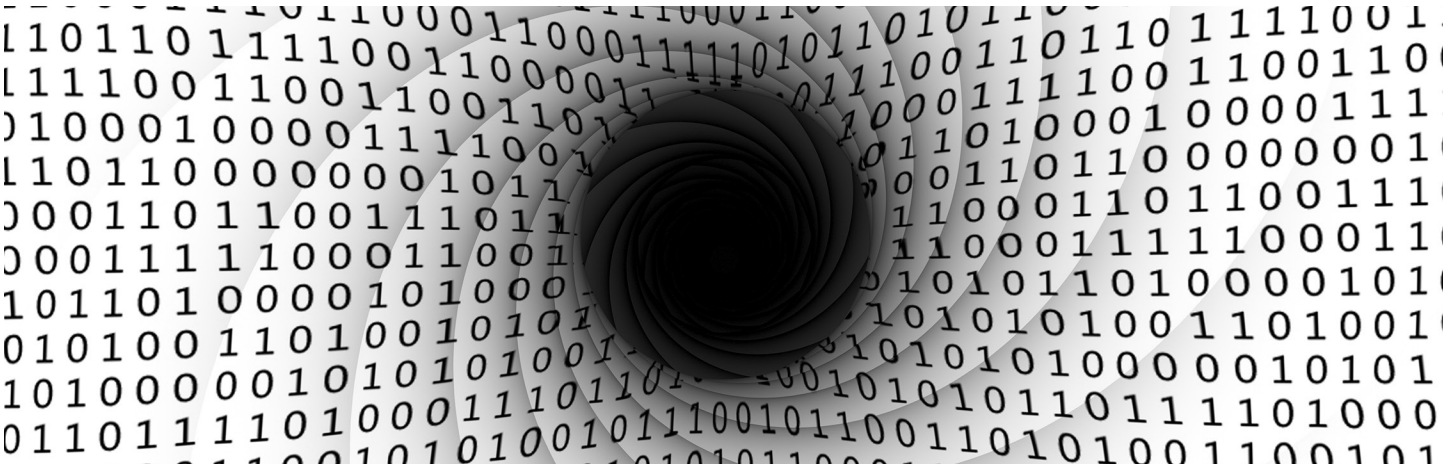
Politically inspired threat actors targeted governmental departments and organizations.



6 ATTACKS PROMPTED GOVERNMENT RESPONSE

The Mirai botnet DDoS attacks prompted legislators to propose solutions and implement rules.

VULNERABILITIES



Threat actors exploited several zero-day vulnerabilities in Microsoft and Adobe software. In addition, several critical vulnerabilities in content management systems (CMS) such as Joomla and WordPress were weaponized shortly after updates were released. Security researchers noted that one threat group increased attacks after updates were available to maximize their infection rate prior to victims applying updates. Organizations should maintain a timely process for applying security updates, implement mitigations where possible to minimize impact from a compromise, and educate personnel on how to detect and avoid threats.

Researchers disclosed how data leaks from devices such as pagers connected to sensitive networks are trivial to decode and leverage in attacks. Communications from healthcare networks, nuclear plants, power substations, manufacturers, and defense contractors leaked alarm and status notifications, diagnostics, contact information, and personnel data. Organizations should use encrypted paging systems, authenticate incoming pager messages, and audit data leakage from sensitive networks.

MALWARE

Ransomware employed various novel methods to circumvent defenses and trick victims into paying ransoms. Exploit kits and phishing emails are the primary infection vectors for ransomware, so organizations should keep software up to date, implement protections against emails containing suspicious links and attachments, and advise users to avoid untrusted emails. Infected systems should be restored from known good backups and examined offline for additional malware, ransomware identification, and possible recovery with decryption tools.

- Locky deployed several variants that used different encrypted file formats and extensions, switched malicious attachment types, and experimented with multiple downloader trojans.
- Cerber used random file extensions to confuse detection tools, and terminated database processes to allow it to encrypt the data.
- A Jigsaw ransomware variant contained code to steal and leak a victim's files.

Researchers discovered that the TrickBot banking malware was similar to the Dyre banking trojan, which ceased activity in November 2015. It is likely that a Dyre developer is involved with TrickBot, or that the private codebase was shared in an underground community. Organizations should use security controls to restrict access to indicators related to the TrickBot trojan, and exercise caution with spam email and exploit kits that may install this malware.

THREAT ACTORS AND METHODOLOGIES

Politically inspired threat actors ostensibly from Russia, Ukraine, and China targeted governmental departments and organizations. Because threat groups can be opportunistic and choose seemingly arbitrary targets, organizations in all verticals should be vigilant for suspicious activity and should implement a comprehensive incident response plan that includes detection for emerging threats as well as distributed denial of service (DDoS) mitigation.

- Russia was accused of interfering with the U.S. presidential election, but officials in Moscow said the accusations were flattering but false. The Russian government reportedly claimed it would prevent further attacks on the World Anti-Doping Agency (WADA) by the Fancy Bear threat group if investigations are halted.
- The CyberJunta Ukrainian threat group leaked emails allegedly from a key aide to the Russian president outlining a plan to destabilize Ukraine.
- Chinese threat groups TG-3390 and TG-0416 were suspected of targeting U.S. defense contractors with malware connected to the Anthem and U.S. Office of Personnel Management (OPM) data breaches.

LAW ENFORCEMENT AND GOVERNMENT

The Mirai botnet DDoS attack that began in September and exploited weakly protected Internet of Things (IoT) devices drew the attention of legislators proposing solutions and regulations. A U.S. senator asked the Federal Communications Commission (FCC) for recommendations on vetting IoT device security and whether Internet service providers (ISPs) could deny network connections for insecure devices. The European Commission is considering labeling IoT devices with a security rating similar to safety certifications on consumer appliances. Organizations should verify that unique and complex passwords are used on all software and hardware, install the latest security updates, disable remote access such as Telnet when it is not needed, employ a DDoS mitigation service for all critical systems, consider implementing a redundant DNS service, and increase vigilance in case an attack is a distraction from a more serious security threat.

Many suspects involved with financial fraud, hacktivism, and e-currency crime were arrested, charged, and prosecuted in October:

- A U.S. citizen suspected of hacking nine financial institutions was detained in Russia for visa violations and requested asylum to avoid extradition. A fourth suspected member of an ATM malware gang responsible for stealing $2 million was arrested in Romania and extradited to the UK. In the U.S., Dwayne C. Hans was charged with financial fraud for allegedly masquerading as a company representative to steal $134,000 and then trying to steal an additional $1.5 million. An Iranian citizen pleaded guilty in Mississippi for selling the data from 2.5 million stolen credit cards. Europol arrested 42 alleged members of an ecommerce fraud ring that stole $3.7 million worth of online goods. Indian law enforcement arrested 772 individuals suspected of scamming $1.4 million by impersonating U.S. tax collectors.
- An Anonymous hacktivist charged with hospital DDoS attacks as part of the #opJustina campaign pleaded not guilty, although he had admitted culpability to the media. A Dutchman accused of the 2013 DDoS attack on the Spamhaus spam blacklisting service went on trial but denounced the charges. Two teenagers suspected of being part of the Lizard Squad and PoodleCorp threat groups were arrested for providing DDoS-for-hire and phone call harassment services. Another UK teen pleaded guilty to running a DDoS-for-hire service that generated $385,000 in rentals.
- Two unrelated individuals, one in the Czech Republic and one in the U.S., were arrested for stealing Bitcoin by stealing the credentials of Bitcoin exchange and dark web marketplace users. A Florida resident running an illegal Bitcoin exchange pleaded guilty to laundering ransomware transactions.
- A Pennsylvania man known as the "Fappening hacker" was sentenced to 18 months in prison for compromising Apple and Google email accounts. Two individuals involved with the Dridex malware were sentenced in the UK to 12 years in prison for laundering more than $3.2 million in stolen funds.

CONCLUSION

Threat actors and malware developers continually experiment to maximize their ill-gotten gains and achieve their objectives. Their techniques often fluctuate between exploiting cutting-edge zero-day vulnerabilities, employing old schemes, and repurposing malware that had been rendered inactive. Network defenders cannot assume that emerging threats only use new techniques. Organizations must consider a wide range of old and new threats when implementing a comprehensive incident response and mitigation plan.

As an administrative note, SecureWorks will not publish a Threat Intelligence Executive Summary report in December. A variation of this report will be published every other month starting in January 2017.

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