OCTOBER 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 September 2016:

1 SEVERE VULNERABILITIES EXPOSED

Researchers disclosed several severe vulnerabilities in Apple, Cisco, and Microsoft products.

2 MALWARE MODIFIED

Malware authors experimented with changes to the Bugat v5 (Dridex) trojan, Cerber and Locky ransomware, and RIG exploit kit to increase their success.

3 SOURCE CODE RELEASED

After the Mirai botnet unleashed a record-breaking distributed denial of service (DDoS) attack, the malware developers released Mirai's source code.

4 BREACH PROMPTED REACTIONS

A threat group stole data from Yahoo users, leading to government investigations, acquisition delays, and allegations of a culture that values convenience over security.

5 SECURITY INITIATIVES ANNOUNCED

The United Kingdom (UK) and Russia announced initiatives to strengthen IT security and encourage security innovation.

VULNERABILITIES

Several severe vulnerabilities in Apple, Cisco, and Microsoft products weakened the security of affected systems. Awareness of disclosed vulnerabilities and emerging threats could facilitate scheduling and applying security updates when they become available.

- Apple confirmed a researcher's findings that iOS 10's backup password system allows attackers to brute-force passwords 2,500 times faster than in previous releases. In addition to applying updates when available, CTU™ researchers recommend protecting Mac OS or Windows systems that store local backups with strong passwords and a whole-disk encryption system.
- Cisco addressed flaws exposed by the Shadow Brokers group (also known as Equation Group). Scans revealed 840,000 vulnerable devices worldwide.
- Microsoft confirmed multiple vulnerabilities in the Journal file format and advised customers to apply the security update that removes the Journal application from all Windows products. Researchers also documented weaknesses in Windows Safe Mode that allowed attackers to launch undetectable attacks, steal credentials, and disable security software. Unexpected reboots into Safe Mode could indicate malicious activity.

MALWARE

The Bugat v5 (Dridex) banking trojan, Cerber and Locky ransomware, and RIG exploit kit experimented with various infection vectors, infrastructure changes, and malware coinfections to increase compromises.

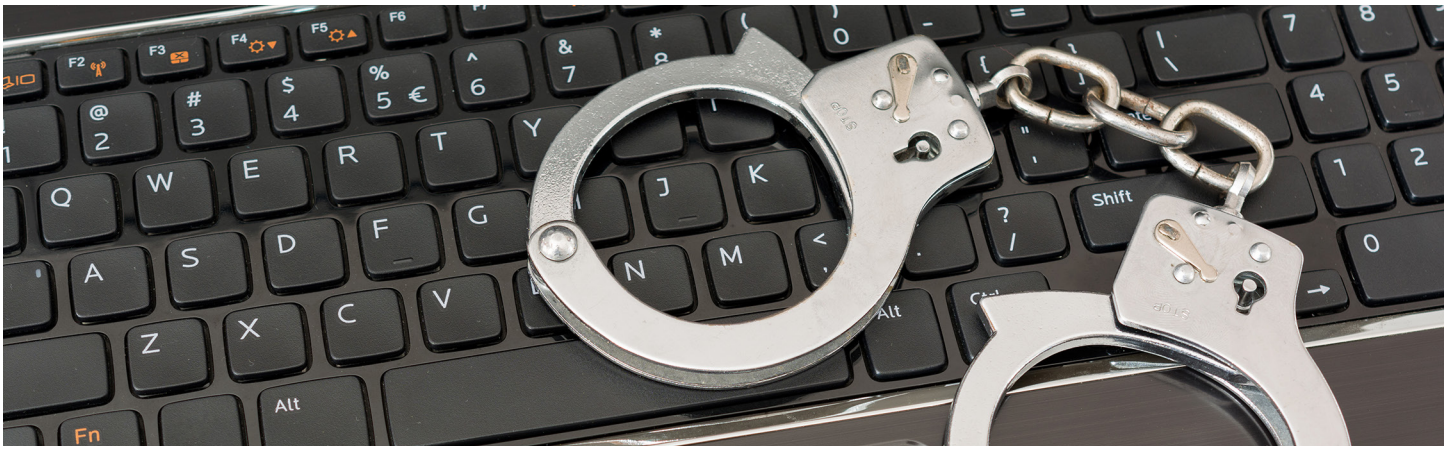
- Deviating from its tradition of targeting large countries such as the United States, Bugat v5 (Dridex) targeted smaller countries with password-protected Office documents in spam attachments delivered from legitimate but compromised servers. Security software did not detect the malware attachments, and the change from using a dedicated malicious hosting site to deliver malware delayed antispam countermeasures. Users should be suspicious of unexpected email bearing attachments, and organizations should disable macro script execution across all affected applications.
- Cerber maximized profits by using the Betabot password-stealing trojan to harvest credentials before encrypting a system with ransomware. In addition to disabling the macro scripting capability used to install the malware, organizations should discourage users from storing usernames and passwords in web browsers.
- Most Locky affiliates discontinued "offline mode," where the ransomware encrypts the compromised system without contacting a command and control (C2) server. While this change makes it easier for network defenders to detect anomalous network activity, it also allows operators to monitor the effectiveness of their distribution campaigns.
- The RIG exploit kit swiftly incorporated features from Neutrino, tested new infection methods, changed its C2 communication to be less predictable, and delivered several different malware payloads. Because exploit kits are often the initial attack vector for a wide range of malware, organizations should implement security updates in a timely manner and use available controls to restrict access based on rapidly changing threat indicators.

The Mirai distributed denial of service (DDoS) botnet is composed of Internet of Things (IoT) devices that use default passwords. The botnet initiated a sustained DDoS attack peaking near 1 Tbps against a security researcher and an Internet service provider (ISP). The developers then published Mirai's source code, which other threat groups could use to create new malware. Organizations should develop and test a DDoS mitigation plan, as attackers can be arbitrary about targets and collateral damage.

THREAT ACTORS AND METHODOLOGIES

Yahoo suffered a record-breaking breach of user data when a reportedly government-sponsored threat group stole data from 500 million Yahoo users. The fallout has led to delays with acquisition plans, a material impact to Yahoo's valuation, and investigations by the U.S. government. This example provides a case study of the implications of sacrificing security for convenience. Users should change the password on their Yahoo accounts and on any other accounts that use the same password.

LAW ENFORCEMENT AND GOVERNMENT



The UK and Russia focused on improving security and recalibrating enforcement of cybercrime.

- The UK created two startup accelerators to encourage new solutions that protect against cyberattacks, tasked the National Cyber Security Centre (NCSC) with developing automated defenses for high-volume unsophisticated attacks, and introduced the Cyber Highway initiative for enterprises to strengthen the security of their supply chain. Organizations should consider whether they could leverage these programs to improve security controls.
- Russia introduced a law that equated cybercrime to theft and established stronger punishments. In the past, prosecutions were few and sentencing was light because cybercrime was considered fraud and could not account for financial damages. The change makes it easier for law enforcement and the legal system to convict cybercriminals for serious crimes, and harmonizes sentencing terms with international norms. Victims could notice an improving legal climate in Russian-attributed cybercrimes if these laws are enforced.

Arrests, raids, pleas, convictions, and sentencing of cybercriminals continued at a steady pace:

- UK police arrested three suspects of online marketplace fraud and business email compromise (BEC), and arrested a UK citizen for illegally accessing delivery data and intercepting more than $100,000 of gold bullion. A multinational operation targeting an ATM skimming group that was active since 2013 resulted in the arrests of six suspects in Romania and Italy. Israeli law enforcement arrested two suspects alleged to be co-owners of the now-defunct vDOS attack-for-hire service. Two U.S. citizens allegedly associated with the Crackas With Attitude threat group were arrested for compromising the personal email of the Central Intelligence Agency (CIA) director, as well as email accounts of other government systems.
- An individual associated with the KYAnonymous threat group pleaded guilty to assuming control of an adversary's email account and website, and a member of the Syrian Electronic Army (SEA) pleaded guilty to extortion. A former Verizon Wireless technician charged with selling private call records between 2009 and 2014 pleaded guilty to unauthorized access.
- Ardit Ferizi, also known as "Th3Dir3ctorY," was sentenced to 20 years for leaking military personnel data to the Islamic State of Iraq and the Levant (ISIL; also known as ISIS). Marcel Lazar, also known as Guccifer (no relation to the "Guccifer 2.0" threat actor), was sentenced to 52 months for accessing email accounts between 2012 and 2014. In London, a member of the D33Ds Company threat group was sentenced to two years in prison for breaching the Yahoo Contributor Network, as well as a video game reseller and SMS messaging service. Mircea-Ilie Ispasoiu, a Romanian national extradited to the U.S, was sentenced to three years in prison and $907,204.88 restitution for wire fraud, identity theft, and unauthorized access.

CONCLUSION

The Mirai botnet and the Yahoo breach underscore the importance of using non-default, unique, and strong usernames and passwords on all Internet-connected systems. Timely security updates are important to strengthen systems against exploit kits and other malware families that evolve to exploit the latest vulnerabilities. Organizations should continue educating users about the threats posed by phishing emails, opening untrusted attachments, and macro scripting.

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