SERIANU CYBER THREAT ALERT SERVICE

March 19, 2013

Introduction

This month's cyber threat alert highlights the latest and critical threats. Java zero day exploit has been the most talked about and critical threat to many businesses across border lines. We have also included new features and remediation to better enhance data security.

Contents

CRITICAL: Java Zero-day Vulnerabilities Persist despite Vendor Patches

Discovery:

Despite increased efforts by Oracle to continuously provide patches for Java Zero-day exploits, security experts earlier this month discovered yet another java zero-day exploit. This exploit allows cyber criminals to remotely access a victim's computer by surreptitiously installing malware labeled McRat Trojan on previously unknown and currently unpatched Java browser plugins and ultimately corrupts computer memory. The attack is triggered when vulnerable users visit a website that has been hidden with attack code. This exploit however; cannot be triggered on older versions of Java nevertheless, it's critical to remember that attackers never sleep - and they will continue to exploit already patched bugs. So going back to these older versions of Java will not be a solution.

Affected systems: The attacks work against Java versions 1.6 Update 41 and 1.7 Update 15, which are the latest available releases of the widely used software.

Exploitation: Cyber-criminals successfully exploit the Java zero-day vulnerability by secretly installing McRat trojan onto vulnerable machines. Although not very reliable, it allows them to corrupt memory by downloading malicious payload onto a targeted machine, but fails to execute.

Mitigation: Serianu recommends that you consider uninstalling Java if you have no need for it, else, consider using a dedicated browser for websites you frequent and require Java and a separate browser for accessing all other sites.

CRITICAL: Microsoft releases new patch to address USB bug that allowed complete system hijack

Early this month, Microsoft plugged-a -hole in its Windows Operating System that allowed attackers to use USB-connected drives to take full control of a targeted computer. This particular exploit requires physical access to a target machine. Like the Stuxnet worm discovered in 2010 targeting Iran's nuclear program; once malware is successfully propagated to a target computer, attackers can progressively attack sensitive networks that are not connected to the internet, otherwise referred to as "carpet bombing".

Affected Systems: Microsoft Windows Operating System

Exploitation: An attacker can own your machine when a maliciously formatted USB drive is inserted in to a computer. When Windows drivers read a specially manipulated USB, the system will execute attack code with the full permissions of the operating system kernel. According to researchers from Microsoft Security Response Center, the vulnerability requires no user intervention – it can be triggered when the workstation is locked or when no user is logged in. This means that an attacker has an un-authenticated privileged physical access to the target computer at kernel level.

Mitigation: It is important that all Microsoft users apply updates using the update management software or set it to automatically update. More importantly, this is also a good reminder for companies to include physical security in their information security policies.

CRITICAL: Apple products using iOS 6.1 are vulnerable to attacks

Discovery: Cyber security researchers discovered vulnerabilities on the iOS 6.1 (iOS is a mobile operating system used for apple iPhone devices). This vulnerability allows attackers to get past the lock screen and access a user's contacts, voicemails and more.

Affected systems: iOS 6.1 running on mobile devices (iPhone or iPad)
Exploitation*:* This vulnerability is exploited by local attackers with physical device access without privileged iOS account or required user interaction. It is located in the main login module of the mobile

iOS device (iPhone or iPad) when processing to use the screenshot function in combination with the emergency call and power (standby) button. The vulnerability allows the local attacker to bypass the code lock in iTunes and via USB when a black screen bug occurs. Successful exploitation of the vulnerability results in unauthorized device access and information disclosure.

Mitigation*:* Apple is currently working on a patch to help address this vulnerability, be on the lookout. Moreover, iOS 6.1.3 will be released to the public soon.

CRITICAL: Yahoo Mail hijacking on the rise

Discovery: Over the past couple weeks, Yahoo mail users have reported cases of their accounts being hijacked. Although Yahoo claims to have patched security holes being exploited, cases of user account compromise are still on the rise. Since the beginning of the year, a large number of vulnerabilities have been discovered, shared online and exploited by cyber scammers.

Affected systems*:* Yahoo mail accounts

Exploitation*:* Hackers are using two different tactics to hijack Yahoo Mail accounts, some users say they receive booby-trapped emails (often seemingly from friends or colleagues) that contain links that direct them to a bogus news site that hijacked their Yahoo Mail account if they were logged in. Others say they never received a similar email but that, nevertheless, their accounts got taken over. The attackers then use the compromised accounts to send out spam to the users' contacts and, indeed, to anyone from whom they ever received a message. Among this spam are also the aforementioned emails that permit cyber scammers to always access a fresh batch of accounts to continue the campaign

Mitigation: To mitigate the likelihood of receiving spam that would lead to hijacking, it is wise to always check the email headers. In doing so you are able to authenticate the source origin of the email sent.

CRITICAL: A Malicious Password and Bank Account stealing malware detected in Kenya

Discovery*:* About two weeks ago, cyber security researchers identified a very serious malware in online banking. With a valid digital signature, this Trojan allows online banking spyware to pass superficial tests as harmless. Attackers use this Trojan to steal online banking credentials such as passwords, credit card numbers and usernames to say the least.

Affected systems*:* The Trojan targets online banking systems and appears to be a certified program.

Exploitation*:* Like most secure electronic financial transactions digital signatures play a vital role in ensuring that the transaction is secure, but now this online Trojan has been certified by DigiCert certificate authority which poses a major threat in secure transaction flow.

Mitigation: To avoid being a victim, ensure that you view the details of digital signatures when transacting online and even cross referencing the certification body for validity and integrity.

High: Fake Airline Ticket Delivers Booby-trapped PDFs

Discovery: cyber-criminals are now targeting Kenyan corporates by sending out emails with a malicious PDF attachment masquerading as Air travel tickets. Serianu came across a specially crafted email with PDF attachments on March 12. This email was sent from a popular Air travel website, and appears to have been sent from compromised home computers. The Trojan initially corrupts the web browser and gradually proceeds to infect the host PC.

Affected systems: Listed Web browser and Windows PC.
Exploitation*:* Sirefef trojan virus hijacks the browser such as Google, Firefox, and IE, begins constant pop-ups, infects files, intercept /hijacks network traffic, contacts remote host to send information about your computer and turns-off security related services.

Mitigation: Ensure that you enable a firewall in your computer, there is an updated anti-virus in your computer and use caution when opening attachments and accepting file transfers. It is also important that organizations carry out frequent user training and awareness programs for information security with a bias on social engineering and phishing techniques.

Mozilla Releases a Secure and Safer PDF Viewer for Firefox

Adobe recently issued a warning on vulnerabilities in the current versions of Adobe Reader and Adobe Acrobat application plugins. This has allowed attackers to incessantly exploit it and send malware to computers. It is with this reason therefore that Mozilla released a new plugin that will let you view PDF files in Firefox for Linux, OSX and Windows.

Adobe patches critical vulnerabilities in Flash player

With vulnerabilities such as integer overflow, use-after-free, memory corruption, and a heap buffer overflow, Adobe released patches to help address them; these vulnerabilities affect Flash for Windows,

Mac OS X, Linux, and older versions of Android, as well as Adobe AIR. The vulnerabilities if exploited could cause a crash and potentially allow the attacker to take control of the affected system.

Affected Systems:

- Adobe Flash Player 11.6.602.171 and earlier versions for Windows and Macintosh,
- Adobe Flash Player 11.2.202.273 and earlier versions for Linux,
- Adobe Flash Player 11.1.115.47 and earlier versions for Android 4.x,
- Adobe Flash Player 11.1.111.43 and earlier versions for Android 3.x and 2.x.
- Users running Adobe AIR 3.6.0.597 and earlier on Windows and Mac OS X,
- The 3.6.0.597 SDK and AIR 3.6.0.599 SDL and Compiler and AIR 3.6.0.597 for Android

According to Adobe, Flash vulnerabilities for Windows systems have a higher risk of being targeted and hence imperative to patch immediately.

Microsoft releases new cumulative security updates for Internet Explorer

These severe vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Internet Explorer. An attacker who successfully exploited these vulnerabilities could perform privilege escalation, that is, gain the same user rights as the current user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

For customers who have not enabled automatic updating need to check for updates and install this update manually.