SERIANU CYBER-THREAT ALERT SERVICE

August, 2013

Introduction

In this month's edition of the SC3 – Serianu CyberThreat Command Center alert our top highlight focuses on a new skimming trend where cybercriminals are now using 3D printers to make the skimming device look exactly like the ATM machine slot. In addition, we provide you with details on the recent announcement by Microsoft to stop supporting one of its supported Windows systems.

Contents

CRITICAL: Hand of the Thief Trojan targets Linux Desktop systems.

Discovery: For many years, Linux desktop systems have been known to be more secure than their counterparts, Windows systems, however; RSA, the security division of EMC, recently reported a new banking Trojan that steals login credentials from users who use the different distributions of Linux while internet banking.

Affected systems: Linux Desktop distribution (Fedora, Ubuntu, Debian)

Exploitation: Dubbed, 'Hand of the Thief', this Trojan grabs the victim's username and passwords with a "Form Grabber" as they enter the details into their bank's online system. In addition, the Trojan also steals the timestamp of when you visited the website, URLs of websites you visited and possibly your web browser's cookies. Finally, all this is then passed on over the Internet to a command-and control server. From there, a cybercrime team can get to work selling your information to people who will start running up your credit-card or debit-card bills (malware designed by criminals for criminals).
The attack specifically targets common Web browsers such as Firefox, Google Chrome, as well as several other that others that are often found on Linux such as Chromium, Aurora, and Ice Weasel.

About the Serianu Cyber Threat Alert Service

For more detailed and customized vulnerability management service, e-mail us at info@serianu.com

Visit: www.cyberusalama.co.ke for more information on cyber security incidents in Kenya

Fortunately, the Trojan can only get into a user's Linux system through an e-mail attachment/URLS or social engineering. Also, I must have the root (or sudo) password in order to install in your machine. There are no other smart attack vectors reported.

Mitigation: As described above, the attack vectors are through email or social engineering, therefore, as users, you should be more vigilant about how you use your Linux system; the following should be practiced:

- Do not install unsigned packages
- Do not add unofficial repositories without investigating said repository
- Keep your system up to date at all times
- Keep all browser plugins up to date
- If your distribution has SELinux, use it
- Do not let others install software on your machines
- Use solid passwords
- If asked to enter root user (or sudo) password, always know why

CRITICAL: Cybercriminals use 3D Printers to make better ATM Skimmers.

Discovery: Not long ago, one of Kenya's major banks experienced ATM skimming, this time, in Australia; ATM theft criminals are using 3D printers and CAD technology to tailor skimming devices. The Cybercrime squad in Australia identified one gang that targeted 15 ATMs across metropolitan Sydney, affecting tens of thousands of people and stealing around US$92,000.

Affected Systems: ATM Machines

Exploitation: These cybercriminals specially craft skimmers for different models of ATM machines so that they fit better and cannot be easily detected. According to a security researcher, the better a skimmer fits, the more smoothly it blends with the ATM's shape and the closer the color, the more likely it is go unnoticed.
Once installed, the skimmers read and extract data from the magnetic stripe of an ATM card. Skimmers are often used in conjunction with a hidden miniature pin-hole video camera, or an unobtrusive keypad overlay, to record PIN data. The collated information is then sent to the criminals through mobile phone technology (or stored later for retrieval) for cloning a magnetic stripe only ATM card. These cards, together with the stolen PINS, are used to make fraudulent withdrawals.

About the Serianu Cyber Threat Alert Service

For more detailed and customized vulnerability management service, e-mail us at info@serianu.com

Visit: www.cyberusalama.co.ke for more information on cyber security incidents in Kenya

Mitigation: The use of ATM skimmers is a global problem, at this time; the best remediation is for banks to ensure that consumer awareness is reinforced and better security is deployed where ATM machines are located.
EuroPay, MasterCard and Visa (EMV) standard aims at improving security by mitigating risks of card cloning; in Kenya, the Kenya Bankers Association (KBA), is in the forefront of ensuring that all banks migrate to EMV, Chip and Pin technology by end of September 2013.

CRITICAL: Apache Strut servers targeted by Hackers.

Discovery: Security researchers recently uncovered a tool on Chinese underground forums that automates attacks against vulnerable Struts versions. Apache Struts is a popular open-source framework for developing Java-based Web applications and is maintained by the Apache Software Foundation. Although security updates were released to address critical vulnerabilities affecting Apache Struts, hackers used this as an opportunity to actively exploit these vulnerabilities.

Affected Systems: Apache Struts

Exploitation: Once hackers break into a Linux-based or Windows-based server using the Struts attack tool, they can execute pre-configured commands in order to extract information about the server's operating system, directory structure, active users and network configuration. This tool also allows attackers to plant a so-called Web shell called JspWebShell that acts as a backdoor, giving them persistent access to the servers to execute other commands and use them as they see fit.

Mitigation: It is highly recommended that users of Apache struts upgrade to the latest version.

CRITICAL: Joomla exploits results in thousands of exploited systems

Discovery: Earlier this month, security researchers at the Versafe Security Operations Center, discovered a vulnerability that has put websites hosted on the Joomla content management system at risk of being hijacked for use in malware payload and phishing attacks. In addition, the researchers also discovered a zero-day attack found in the wild, which enabled attackers to gain full control over the compromised systems.

Affected Systems: Joomla hosted websites.

Exploitation: The attackers' IPs originate from China, they infiltrate a user's system using a drive by malware called "Blackhole" when the victim visit a Joomla hosted website. This then enables the

attackers to have full control over systems, meaning that, they can make changes to system configuration settings at their discretion.

Mitigation: The Joomla Security strike team has developed a patch for this vulnerability and is now available on the Joomla Developer Network.

CRITICAL: Windows XP, 'zero-day-forever'

Microsoft has announced the end of support for Windows XP SP3. After **April 8, 2014**, users running Windows XP Service Pack (SP) 3 -- the last service pack delivered for the 11-year-old operating system – will not get any more updates. That includes both security and "non-security" hot fixes, free or paid support options and online technical content updates.

Users are requested to make plans of migrating to other supported Windows operating systems. Microsoft is frequently experiencing new forms attacks on their systems, although they release updates for these vulnerabilities, these updates will not be enough to safeguard Windows XP.

According to Microsoft officials, after April 8, 2014, attackers will likely have more information about vulnerabilities in Windows XP than defenders. The very first month that Microsoft releases security updates for supported versions of Windows, attackers will reverse engineer those updates, find the vulnerabilities and test Windows XP to see if it shares those vulnerabilities. If it does, attackers will attempt to develop exploit code that can take advantage of those vulnerabilities on Windows XP

Mitigation: If your organization in still using Windows XP SP3, especially to run mission critical business processes, it is about time you prioritized the migration process to protect the confidentiality, integrity and availability of your information assets.

PCI 3.0 Highlights

Earlier this month, the PCI Security Standards Council (PCI SSC) published PCI Data Security Standard (PCI DSS) and Payment Application Data Security Standard (PA-DSS) 3.0 Change Highlights as a preview of the new version of the standards coming in November 2013. The changes will help companies make PCI DSS part of their business-as-usual activities by introducing more flexibility, and an increased focus on education, awareness and security as a shared responsibility.

These changes are aimed at helping organizations which are working towards becoming PCI DSS compliant make payment security business-as-usual in a more flexible, objective and consistent manner.

Proposed updates include:

Recommendations on making PCI DSS business-as-usual and best practices for maintaining ongoing PCI DSS compliance

- Security policy and operational procedures built into each requirement
- Guidance for all requirements with content from Navigating PCI DSS Guide
- Increased flexibility and education around password strength and complexity
- New requirements for point-of-sale terminal security
- More robust requirements for penetration testing and validating segmentation
- Considerations for cardholder data in memory
- Enhanced testing procedures to clarify the level of validation expected for each requirement
- Expanded software development lifecycle security requirements for PA-DSS application vendors, including threat modeling

Note that these updates are still under review by the PCI community. Final changes will be determined after the PCI Community Meetings and incorporated into the final versions of the PCI DSS and PA-DSS published on November 7, 2013 and become effective January 1, 2014.

The change highlights document with tables outlining anticipated updates is available on the PCI SSC website: https://www.pcisecuritystandards.org/security_standards/documents.php

About the Serianu Cyber Threat Alert Service

For more detailed and customized vulnerability management service, e-mail us at info@serianu.com

Visit: www.cyberusalama.co.ke for more information on cyber security incidents in Kenya

Microsoft Patches 23 Vulnerabilities in Windows, IE, and Exchange

Microsoft released 8 security bulletins addressing 23 vulnerabilities in Microsoft Windows, Internet Explorer and Exchange Server. We have summarized the updates below:

Update		Description
MS13-059		Cumulative update for Internet Explorer, and patches 11 separate vulnerabilities, 9 of which are rated critical on one or more platforms. The 9 critical vulnerabilities are all memory corruption vulnerabilities. The other 2 are only rated as Moderate severity on some platforms for privilege escalation or information disclosure.
MS13-061		This security update for Exchange Server 2013 has been pulled back by Microsoft as the update affects all Mailbox server installations. Microsoft is urging all Exchange Server 2013 users to hold off on deploying the patch until a corrected version can be issued. For those that have already installed the MS13-061 security faulty update, Microsoft has shipped a workaround (KB 2879739) that provides steps on how to resolve the problem. This workaround is trivial and involves resetting registry entries.
MS13-060		(Vulnerability in Unicode Scripts Processor Could Allow Remote Code Execution) affects only Windows XP and Server 2003. "The vulnerability could allow remote code execution if a user viewed a specially crafted document or webpage with an application that supports embedded OpenType fonts."
MS13-062		A single privilege escalation vulnerability which affects the RPC handling code in all versions of Windows and is rated Important.
MS13-063		Describes 4 vulnerabilities, all rated Important, affecting most versions of Windows. One allows bypass of ASLR (Address Space Layout Randomization), a technique used by Windows to defeat many attacks. The other 3 are kernel corruption vulnerabilities which could allow elevation of privilege. These vulnerabilities have been publicly disclosed already. For reasons unclear to me, Microsoft does not provide an exploitability index number for the ASLR bypass vulnerability.
MS13-064		A single denial of service vulnerability in the Windows Server 2012 NAT Driver. A specially-crafted ICMP packet could cause the service to stop responding.

About the Serianu Cyber Threat Alert Service

For more detailed and customized vulnerability management service, e-mail us at info@serianu.com

Visit: www.cyberusalama.co.ke for more information on cyber security incidents in Kenya

MS13-065		A single denial of service vulnerability in the IPv6 stack in all versions of Windows except XP and Server 2003. This vulnerability is also triggered by a specially-crafted ICMP packet.
MS13-066		Information disclosure vulnerability in the Active Directory Federation Services (AD FS) in all Intel-based versions of Windows Server other than Server Core. According to Microsoft, "…the vulnerability could reveal information pertaining to the service account used by AD FS. An attacker could then attempt logons from outside the corporate network, which would result in account lockout of the service account used by AD FS if an account lockout policy has been configured. This would result in denial of service for all applications relying on the AD FS instance.

Microsoft also released 3 non-security updates, as well as the monthly Malicious Software Removal Tool and an update to root certificates.

About the Serianu Cyber Threat Alert Service

For more detailed and customized vulnerability management service, e-mail us at info@serianu.com

Visit: www.cyberusalama.co.ke for more information on cyber security incidents in Kenya