SERIANU

CYBER USALAMA

SERIANU CYBER-THREAT ALERT SERVICE

September - October, 2013

Introduction

In this month's edition of the SC3 - Serianu CyberThreat Command Center alert our top highlight focuses on a new banking trojan that targets online banking users and is designed to beat mobile multi-factor authentication systems. We also discuss critical vulnerabilities that are found in commonly used hardware and software.

Contents

CRITICAL: HESPERBOT – THE NEW BANKING TROJAN.

Discovery: There is a new Trojan that targets online banking users and is designed to beat the mobile two factor authentication systems. Two factor authentications is a security process whereby a user provides two means of identification, the first is usually a physical token such as a card and the second a security code which can be sent to your phone. A good example is when logging in to your online banking portal and after entering the username and password, you are sent a short code to your phone to authenticate your identity.

The aim of the attacker using this Trojan is to obtain your login credentials which would enable them to gain access to your bank account and enable them to install the mobile component of the malware on your Symbian, Blackberry or Android phone.

Affected systems: Systems affected by this malware are Windows 2000, Windows 7, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Server 2008, Windows Vista and Windows XP.

Exploitation: Hesperbot the online banking trojan was detected as Win#@/Spy Hesperbot and has similar characteristics to Zeus and SpyEye banking malwares. This trojan is able to perform keylogging which is recording and keeping track of your keyboard inputs, it can create desktop screenshots, capture videos, set up remote proxies as well as create hidden remote connections to the infected system alongside network traffic interception using HTML injection capabilities. It was also discovered that this malware harvest email addresses and sends them to a remote server possibly for targeted spam and phishing attacks.

Mitigation: Remediation for this malware is as follows:

- Do not install unsigned packages
- Do not add unofficial software repositories without investigating them
- Keep your operating system up to date at all times
- Keep all browser plugins up to date
- Do not let others install software on your machines
- Use solid passwords
- Use malware removal tools
- Use best practices for web browsing
- Use best practices for email

For additional information on online best practices log on to http://cyberusalama.co.ke/awareness.html

CRITICAL: JAVA 6 ZERO DAY VULNERABILITY INTEGRATED INTO EXPLOIT KIT

Discovery: The Java 6 platform is still very popular even though it is out of date. Hackers are now using a new exploit for a bug present in this platform to attack unsuspecting victims. It is interesting to note that this bug has now been added into the Neutrino exploit kit which is now commercially available. This opens up the users of this platform to a whole new host of threats. This exploit targets an unpatched vulnerability in Java 6 identified as **CVE-2013-2463**. Oracle is aware of this vulnerability but will not patch it as the platform is no longer supported.

Affected Systems: The affected systems are all Java 6 platforms.

Exploitation: The said vulnerability lies in the Java Runtime Environment 2D sub-component which is responsible for making two-dimensional graphics. As there is no available patch, this particular exploit provides cybercriminals with the capability to launch attacks against companies and organizations using Java 6. The impact of this vulnerability will be most felt by organizations as opposed to regular internet users as they may not be quick enough to upgrade to the most current Java platform due to business or operational challenges.

Mitigation: Users should update their Java installations to the latest available version of Java 7. For the users who do not need Java 6 for day to day tasks, an alternative approach is to uninstall it.

CRITICAL: MICROSOFT SHAREPOINT SERVER VULNERABILITIES

Discovery: Microsoft issued a security update that resolves 109 vulnerabilities reported in Microsoft Office Sever software. The most severe of all of them could allow remote code execution of a service account if an attacker sends specially crafted content to the affected server.

Affected Systems: Microsoft SharePoint Server 2007 and its Excel services, Microsoft SharePoint Server 2010, Microsoft SharePoint Services 2.0, Microsoft SharePoint Services 3.0, SharePoint Foundation 2010 and Microsoft SharePoint Foundation 2013. It also applies for affected Microsoft Office Services and Web Apps on supported editions of SharePoint Server 2010.

Exploitation: Once This vulnerability allows remote code execution of a service account if an attacker sends specially crafted content to the affected server.

Mitigation: Users of the affected systems are advised to configure automatic update checking using the Microsoft Update Service. However, if this is already enabled, the security updates may have been downloaded and installed automatically. The other alternative is to check for updates from the Microsoft Update website and install this update manually and immediately.

CRITICAL: INTERNET EXPLORER ZERO DAY EXPLOIT

Discovery: Microsoft released an emergency fix for their users to protect them against a number of attacks directed at Internet explorer 8 and 9 but has the potential to affect all versions of the web browser. The vulnerability is referred to as the CVE-2013-3893.

Affected Systems: Internet Explorer 6.7.8, 9, 10 and 11

Exploitation: This vulnerability could allow remote code execution if an affected system browses a website containing malicious content directed towards the specific browser type. This vulnerability has already been targeted by hackers and is complicated to fix. If an attacker successfully exploits this vulnerability, s/he could gain the same user rights as the current user, due to this reason Microsoft has advised that user accounts be configured with fewer user rights on the system as this would have a lesser impact as opposed to those who operate with administrative user rights.

Mitigation: Microsoft is working on a developing a proper update to fix this flaw but has released a temporary fix using their "Fix-It" tool. In order to protect your copy of internet explorer you have to download this tool and install it. This applies to all windows users, especially if they user internet explorer to visit websites.

CRITICAL: BRUTE-FORCE MALWARE TARGETS E-MAIL AND FTP SERVERS

Discovery: Fort Disco is a type of malware that is designed to launch brute-force password guessing attacks against websites built with popular content management systems such as WordPress and Joomla. This malware has evolved and is now being used to target email and FTP servers. It is estimated that it has infected over 25,000 windows computers and has been used to guess admin account passwords on over 6,000 WordPress, Joomla and Datalife Engine website. This is not to mention, it having a hit list of 411,667 domains with 1200 domains already compromised with at least one shell script installed and 4800 domains with compromised admin areas awaiting backdoor installation on the servers.

Affected Systems: WordPress, Joomla and Datalife Engine websites

Exploitation: When this malware infects a server and is now compromised, the attackers upload shell scripts in order to maintain access to the system. The scripts enable the attackers to upload additional files to modify the server assuming it was not properly configured and a given vulnerability is exploited.

It periodically connects to a command and control (C&C) server to retrieve instructions, which is a list of thousands of websites to target and the passwords that should be tried to access their administrator accounts. The malware targeted blogging and CRM platforms which have been poorly implemented with the use of default credentials, and weak and easily guessable passwords.

However, now it has evolved to the level of brute-forcing Post Office Protocol version 3 (POP3) which is responsible for allowing email clients to connect to email servers and retrieve messages from existing accounts. This is facilitated by the malware being supplied with a list of domain names accompanied by corresponding MX records (mail exchanger records) which specify which servers are handling email services on the respective domains. The command and control (C&C) server also supplies the malware with a list of standard email account names such as admin, info and support to name a few, that the malware should try and brute force the password.

Mitigation: In order to remediate against this malware the best defense or preventive measure is to first of all embrace best practices in passwords use such as the use of a combination of alphanumeric and special characters. For more tips, a best practice guide on passwords can be found on the cyber Usalama website at http://www.cyberuslama.co.ke/passwords.html The scripts that are supplied by the C&C server make heavy use of PHP's fopen and fwrite functions, therefore; a good defense approach is to ensure all your servers are hardened, so as to to limit functions that can be leveraged using scripts. This would also heavily assist in mitigating the damage caused on shared hosting environments on a single domain as the scripts will be unable to operate outside the user's folder. In the unfortunate event a server compromise, the use of malware removal tools will come in very handy.

HIGH: NEW OS X BUG ALLOWS USE OF 'SUDO' WITHOUT A PASSWORD

Discovery: For the last 5 months, researchers have been analyzing a flaw in OS X which allows a malicious user to gain nearly full access to the system without supplying a password.

Affected Systems: OS X Versions 10.7 through 10.8.4

Exploit: The exploit revolves around "sudo" Unix command which is used in place before other commands, to run commands as another user, and primarily the root or system account to allow full access for administrative purposes. Normally the sudo command is off-limits to everyone except administrators, and even with administrative access it requires a supply of your password to run. If you set the Mac's clock back to January 1, 1970, (the epoch, or logical "beginning of time" for Unix systems), apparently you can use the sudo command to gain root access and use it without authenticating.

This flaw circles around the way the system stores prior credentials for the sudo command. While at first glance it appears this issue allows anyone access to the system, it only affects systems in specific ways -- it only works if the current user is an administrator, is currently logged in, and has authenticated the sudo command in the current log-in session.

Mitigation: While not necessarily a significant bug, it is one that could potentially be exploited. It has been given a Common Vulnerabilities and Exposures ID to hopefully get it addressed as quickly as possible

CRITICAL: CISCO CATALYST 3750 –X SERIES VULNERABILITY

Discovery: CISCO recently reported a vulnerability which affects their Service Module for Cisco Catalyst 3750-X Series Switches. This vulnerability could allow an authenticated, local attacker to gain root access to the kernel running on the Cisco Service Module.

Affected Systems: Cisco IOS 6.8/5.6

Exploit: The vulnerability is due to default credentials on the Cisco Service Module. An attacker could exploit this vulnerability by logging in using the default credentials. An exploit could also allow the attacker to take complete control of the operating system running on the service module. This then enables him/her to perform remote code executions.

Mitigation: Cisco has released updates to work around this vulnerability. Users are urgently requested to update their devices.

CRITICAL: BACKDOOR FOUND IN D-LINK ROUTER

Discovery: A backdoor found in firmware used in several D-Link routers could allow an attacker to change a device's settings - a serious security problem that could be used for surveillance.

Affected Systems: The affected models likely include D-Link's DIR-100, DI-524, DI-524UP, DI-604S, DI-604UP, DI-604+, TM-G5240 and possibly the DIR-615

Exploit: The technology industry has been rattled by documents leaked by former NSA contractor Edward Snowden, which indicate the spy agency pursues ways to subvert security measures through backdoors. But developers sometimes make mistakes and in other cases, make poor security decisions. With access to a router's settings, an attacker could potentially steer someone's Internet traffic through their own server and read their unencrypted data traffic.

Mitigation: Unfortunately, at the moment, we have not come across any remediation.

CRITICAL: PHP SOURCE COCE RETREIVAL VULNERABILITY

Discovery: This attack allows an attacker exploit vulnerability (CVE-2012-1823) to retrieve the source code of an application and gain code execution by placing command-line options in the query string.

Affected Systems: This flaw affects webservers with PHP CGI configurations on windows systems running Red Hat Enterprise Linux.

Exploit: With this vulnerability, an attacker could inject arguments into the PHP-CGI binary and make changes to php.ini directives, allowing for remote code execution. When this happens, there is considerable informational disclosure where you could find out the database passwords, file locations etc., execute any files on disk and possibly upload a file to the server and execute any code. It should be noted that authentication is not required to exploit the vulnerability.

Mitigation: You can prevent this by using the latest stable PHP version located at the download page on the PHP website**.**

LOW: NEW MAC OS MALWARE EXPLOITING TWO KNOWN VULNERABILITIES

Discovery: A new Mac OS malware called OSX/Leverage.A has been discovered. This is a command and control (C&C) Trojan horse that creates a backdoor on an infected user’s machine. The name emanated from how the application is distributed i.e. an application disguised as a picture.

Affected Systems: Mac OS

Exploit: The attack is launched via a Java applet from a compromised website and which drops a Java archive with the backdoor to the visitor's computer and launches it without a user's interaction. To perform the attack, malware uses two recently disclosed java vulnerabilities known as CVE-2013-2465 and CVE-2013-2471. Once it is installed, the Trojan connects to the C&C server on port 7777.

Mitigation: The threat level of this malware appears to be low as it has affected few people. However, Apple has come in and updated *XProtect* to detect the malware and prevent if from launching.

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.