SERIANU CYBER THREAT ALERT SERVICE

June-July 2013

Introduction

In this month's edition of the SC3 – Serianu CyberThreat Command Center alert we provide you with an update on global attacks and an analysis of local attacks. Our top highlight focuses on a new trend where cybercriminals are increasingly hacking into Kenyan based shared Web hosting servers in order to use the domains hosted on them for cybercriminal activity. Over the past couple months we have detected over 1 million events and based on these events there is a sudden. In the 2nd Quarter of 2013, we detected a total of 300 locally hosted websites that had been compromised by cybercriminals. We are advising organisations that host their websites on local shared hosting servers, to perform a small audit on the server to see if it is indeed vulnerable. We can assist you with the audit – since we are already aware of the vulnerable servers.

Launch of Cyberusalama.co.ke

As you might be aware, in May 2013 we signed a Memorandum of Understanding with USIU's Centre for Informatics Research and Innovation (CIRI), to establish cyber security infrastructure to support the local market needs. Our first initiative with USIU has focused on working with Telecommunications Service Providers Association of Kenya (TESPOK) to establish a security awareness website targeting general and technical internet users. We would like to invite you to visit this website at www.cyberusalama.co.ke. While on the website, please visit the resources section where you will get access to the following reports:

Contents

CRITICAL: 1. Cybercriminals Increasingly Targeting Kenyan based shared Web hosting servers

Discovery: Over the past couple months we have detected an increase in cybercriminals targeting Kenyan based shared Web hosting servers in order to use the domains hosted on them for cybercriminal activity.

Affected systems: Locally based shared webhosting services

Exploitation: Based on data reviewed and analyzed by Serianu, cybercriminals are breaking into shared Web hosting servers, updating their configuration so that they are able to deface or distribute malicious applications from particular subdirectories of websites hosted on the servers. Our analysis has shown that a single shared hosting server in Kenya can host hundreds or even thousands of websites at a time. In the 2nd Quarter of 2013, we detected a total of 300 locally hosted websites that had been compromised by cybercriminals.

In order to break into shared hosting servers, attackers exploit vulnerabilities in Web server administration panels like cPanel or Plesk and popular Web applications like WordPress or Joomla. These attacks highlight the vulnerability of local hosting providers and software, exploit weak password management, and provide plenty of reason for Kenyan internet users to worry.

Reasons why sites hosted shared hosting servers are vulnerable to cyber-attacks

- If any one site on the server is compromised, it literally opens a gateway for the attacker to gain access to the other sites hosted on the same server as well.
- A malicious user can buy the hosting from a shared hosting Provider and use his site to gain access to other sites on the same server.
- There is also the disadvantage of not being able to harden the server. If you are on a shared hosting server, you would not have access to the PHP and Apache configuration of the server.

Mitigation: If your organisation has hosted a site on a Kenyan based shared hosting server, you need to perform a small audit on the server to see if it is indeed vulnerable and allows you to read files of other sites on the same server. If it is, you can inform the Hosting Provider about this and help them harden the server before a malicious Attacker takes control of it. We can assist you in performing this audit - we already have a list of hosting servers that have been compromised and can help in confirming if your website is vulnerable/at risk.

CRITICAL: Exploited Attacks Targeting Government Agencies in Europe, Asia

Discovery: Security researchers recently uncovered targeted attacks to personnel at Government agencies in Europe and Asia. Attackers used phishing e-mails to exploit a vulnerability found in Microsoft Office.

Affected systems: Microsoft Office

Exploitation: Attackers would send Government personnel an e-mail which included malicious attachments (TROJ_DROPPER.IK). However, contrary to the other attacks reported on our monthly reports, this attack was not sophisticated; the attackers sent an e-mail from a Gmail account.
The exploit is used to drop a backdoor (BKDR_HGDER.IK) onto the system, which steals login credentials for websites and email accounts from Internet Explorer and Microsoft Outlook. The exploit also opens a legitimate "dummy" document e.g. a legal document, to make the target believe that nothing malicious happened. Any stolen information is uploaded to two IP addresses, both of which are located in Hong Kong.
According to Trend Micro, the malicious attachment is a malicious backdoor virus that would give access to isolated hackers to make changes to regulate the contaminated system and perform malicious activities on the system.
Mitigation: Microsoft Office users should ensure that they have installed all the necessary updates provided by Microsoft.

CRITICAL: Unusual File Infector Malware Uses Multiple Exploits to Capture FTP Credentials

Discovery: Security researcher's recently discovered a new attack that leverages a combination of exploits to infect systems and target FTP credentials and other information on Windows-based systems. This threat is a file infector malware that is part of the PE_EXPIRO family; malware that was first discovered in 2010.

Affected Systems: Windows-based systems

Exploitation: This file infector arrives on a system as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites. Exploits used in the attacks include two Java exploits which target CVE-2012-1723 and CVE-2013-1493, and an unnamed PDF exploit. Trend detects the malicious PDF file as TROJ_PIDIEF.JXM. If successful, the malware searches all available storage drives (including network drives) for .EXE files to infect. The malware then captures system and

user information, including Windows product ID, drive volume serial number, Windows version and user login credentials. The malware also steals stored FTP credentials from Filezilla, a popular FTP client.

Mitigation: Businesses, especially small and medium sized businesses, must make sure they are always are up to date in applying all security patches. The days when patch management was a luxury are long gone.

CRITICAL: Exploit Tool Targets Vulnerabilities in McAfee ePolicy Orchestrator (ePO)

Discovery: According to US-CERT, a new exploit was recently discovered that were specifically built to attack McAfee's ePolicy Orchestrator (ePO) targets two vulnerabilities found in ePO versions 4.6.5 and earlier. In order to exploit these vulnerabilities the attacker must be on the local network.

Affected Systems: McAfee ePolicy Orchestrator (ePO)

Exploitation: If successful, the attack allows an attacker on the local network to add rogue systems to an enterprise ePO server, steal domain credentials if they are cached within ePO, upload files to the ePO server, and execute commands on the ePO server as well as any systems managed by ePO.

Mitigation: This exploit poses as a huge risk to organizations that use McAfee ePO and the following mitigation steps are strongly advised:

Upgrade ePO to one of the following versions:

- ePO 5.0, released March 25, 2013;
- ePO 4.5.7, released on May 23, 2013; or
- ePO 4.6.6, released on March 26, 2013.

CRITICAL: Mac Malware Uses Encoding Trick to Hide File Extensions

Discovery: Malware that targets Mac OS X uses a right-to-left override ploy to avoid detection. The trick is used to hide the actual extension of executable files. The malware, known as Janicab, is signed with what appears to be a valid Apple Developer ID. It takes screen shots and records audio through infected machines, and sends the data to a command-and-control server. It also maintains contact with the command-and-control server for instructions.

Affected Systems: Mac operating system

Exploitation: The malware, Janicab spreads through spear- phishing and spam messages/e-mails, if a user clicks on the supposedly 'harmless' file, it drops and opens a 'dummy' document on execution to

keep up appearances. It actually masks the creation of a hidden folder in the home directory of the infected user to store its components.

Mitigation: Although Mac operation system will flag these 'dummy' documents as potentially problematic, users should take precautions when downloading documents from unknown sources.

CRITICAL: Multiple Java Instances Keep Enterprise Systems Vulnerable to Attack

Discovery: In an analysis of "approximately one million endpoints" across "several hundred deployments," Bit9 researchers found that 42 percent of endpoints had more than two versions of Java installed at the same time. IT administrators should be aware that when installing new Java updates, the software does not remove older versions of itself, hence the multiple instances.

Affected Systems: Java Systems

Exploitation: The malicious code can specify which version of Java to use, and attackers can target any of the vulnerabilities in the older software. There is no need to bother with finding zero-days or uncovering new vulnerabilities in the latest version of the software.

Mitigation: The best remedy for this vulnerability is to remove Java completely from systems especially if there is no justified reason for having it.

New Patch Releases by Microsoft

Microsoft recently made available a new patch for Windows after an earlier version led to some machines crashing and suffering the 'blue screen of death'. The previous patch, security update 2823324, which fixed flaws in the NTFS kernel-mode driver of Windows, was early April after some users reported getting a "STOP: c000021a {Fatal System Error}" error message after installation.
According to Microsoft, the patch fixes three privately disclosed and one publicly disclosed flaw in an NTFS kernel-mode driver that could allow a user to elevate their privilege level. An attacker would need valid logon credentials and be able to log on locally to "exploit the most severe vulnerabilities"
Microsoft recommends that customers uninstall the earlier security update 2823324 that triggered the initial error message. This can be done by restoring the computer to the state that it was in before the security update was installed or manually uninstalling the security update through the control panel