SERIANU CYBERTHREAT ALERT SERVICE

May 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. As you might be aware, we are partnering with USIU's Centre for Informatics Research and Innovation (CIRI), to establish cyber security infrastructure to support the local market needs. This report includes detailed threat intelligence report addressing threats identified in the local cyber space. We discovered a number of issues which represent real threats to the integrity and security of many organizations in Kenya.

Contents

CRITICAL: Smokescreen DDoS attacks; Millions stolen from banks

Discovery:

Cyber-attacks aimed at stealing millions from banks have been around for years; however, this time round, according to security researchers, hackers make use of two-pronged attacks as a means of exploiting the openings in bank systems to steal account information and create counterfeit debit cards. As a result, millions of shillings have been stolen from automated teller machines in 46 cities around Europe. It is not until customers complained or investigators later on uncovered the breaches that banks discovered they were losing money.

Affected systems:

These attacks target banks and bank ATMs

Exploitation:

This attack is the online equivalent of the common technique used by street hustlers to steal money from unsuspecting victims. Attackers flood a bank's computer system with information to shut it down i.e. they cause a distributed denial of service attack and plant malicious software inside a bank's system which they activate and raid compromised software.

About the Serianu Cyber Threat Alert Service

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

DDoS attacks are effective smokescreens because they overwhelm fraud-detection systems and security specialists in banks react strongly to them, out of concern that prolongedwebsite outages will damage their reputations. These attackers often cripple bank's websites just enough so they can access target accounts while customers can't, and therefore will not notice that they've lost any money until after the attacks end. They have also gone to the extent of hitting banks' phone and data networks at the same time, the idea is to prevent the banks' customers from being able to access their accounts online or over the phone while they withdraw money from ATMs or increase credit- card charges.

Mitigation:

For banks to succeed in preventing two-pronged attacks, they must have sufficient staff across multiple business lines to handle these attacks. They should also increase training for call-center staff to spot suspicious transactions. Regular review of IT Security budget should be also bedone to provide defenses that target nee forms of attacks.

CRITICAL: Sophisticated, Stealthy apache backdoor exposes Businesses

Discovery:

Security researcher's recently discovered ongoing exploits (modified binaries) in the open source Apache webserver. The binaries will load malicious code or other web content without any user interaction turning Apache-run websites into platforms that surreptitiously expose visitors to powerful malware attacks. Apache web servers are among the most well-known and widely-used in the world and are used by numerous companies. Approximately 61.8% of all websites use Apache; this means that a successful security breach can affect numerous different businesses across a diverse range of industries. The attacks are becoming increasingly sophisticated, powerful, and stealthy; they are virtually invisible without the use of specialized forensics. They open backdoors on the servers and files that indicate an infection are stored in shared memory of an infected server.

Affected Systems:

Apache web server's v2 and v1.

Exploitation:

Dubbed Linux/Cdorked.A, this backdoor turns Apache-run websites into platforms that surreptitiously expose visitors to powerful malware attacks. This means that users who visit popular websites such as *Apple.com* or *Youtube.com*which use Apache may expose visitors to powerful malware attacks. This backdoor leaves no traces of compromised hostson the hard drive other than its modified HTTP daemon binary. Its configuration is delivered by the attacker through complicated HTTP commands that aren't logged by normal Apache systems. All attacker-

About the Serianu Cyber Threat Alert Service

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

controlled data is encrypted. Those measures make it all but impossible for administrators to know anything is amiss unless they employ special methods to peer deep inside an infected machine

Mitigation: Businesses, especially small and medium sized businesses, must make sure they are always are up to date in applying all security patches. These must be completed so every employee is safe, and complemented with appropriate prevention measurements, such as anti-malware security suites.

Adobe Reader PDF-tracking flaw

Discovery:

Security researchers' recently uncovered vulnerability in Adobe Systems' Reader program that reveals when and where a PDF document is opened. Although this may not be a critical issue, malicious users, through APTs (Advanced Persistent Threat) can collect sensitive information such as IP address, Internet service provider or even the victim's computing routine.

Affected Systems:

All Adobe systems including the latest version 11.0.2

Exploitation:

Malicious users can persistently use this vulnerability to collect sensitive information from an unsuspecting user.

Mitigation:

Currently, Adobe is working on patches that would address this weakness; in the meantime, we strongly recommend that users disable java script on their computers.

VMware Security Updates

VMware has updated vCenter Server Appliance (vCSA) and vCenter Server running on Windows to address multiple security vulnerabilities. These vulnerabilities include:

1. **vCenter Server AD anonymous LDAP binding credential by-pass** :-
    - vCenter Server when deployed in an environment that uses Active Directory (AD) with anonymous LDAP binding enabled doesn't properly handle login credentials. In this environment, authenticating to vCenter Server with a valid user name and a blank password may be successful even if a non-blank password is required for the account.
    - The issue is present on vCenter Server 5.1, 5.1a and 5.1b if AD anonymous LDAP binding is enabled. The issue is addressed in vCenter Server 5.1 Update 1 by removing the possibility to authenticate using blank

About the Serianu Cyber Threat Alert Service

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

passwords. This change in the authentication mechanism is present regardless if anonymous binding is enabled or not

To best workaround to this vulnerability, users are asked to discontinue the use of AD anonymous LDAP binding if it is enabled in your environment.

2. **vCenter Server Appliance arbitrary file execution**
   - The vCenter Server Appliance (vCSA) contains remote code vulnerability. An authenticated attacker with access to the Virtual Appliance Management Interface (VAMI) may run an existing file as root. In the default vCSA setup, authentication to vCSA is limited to root since root is the only defined user.
3. **vCenter Server Appliance arbitrary file upload**
   - This vulnerability allows an authenticated remote attacker to upload files to an arbitrary location creating new files or overwriting existing files. Replacing certain files may result in a denial of service condition or code execution.

New Patch Released 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

Local Threat Intelligence Report

Discovery

Our assessment found a total of 16418 unique threat events within the one month traffic analysis period. During which we were able to identify the following threat types, severity of their impacts, and descriptions of the associated services.

Threat Types

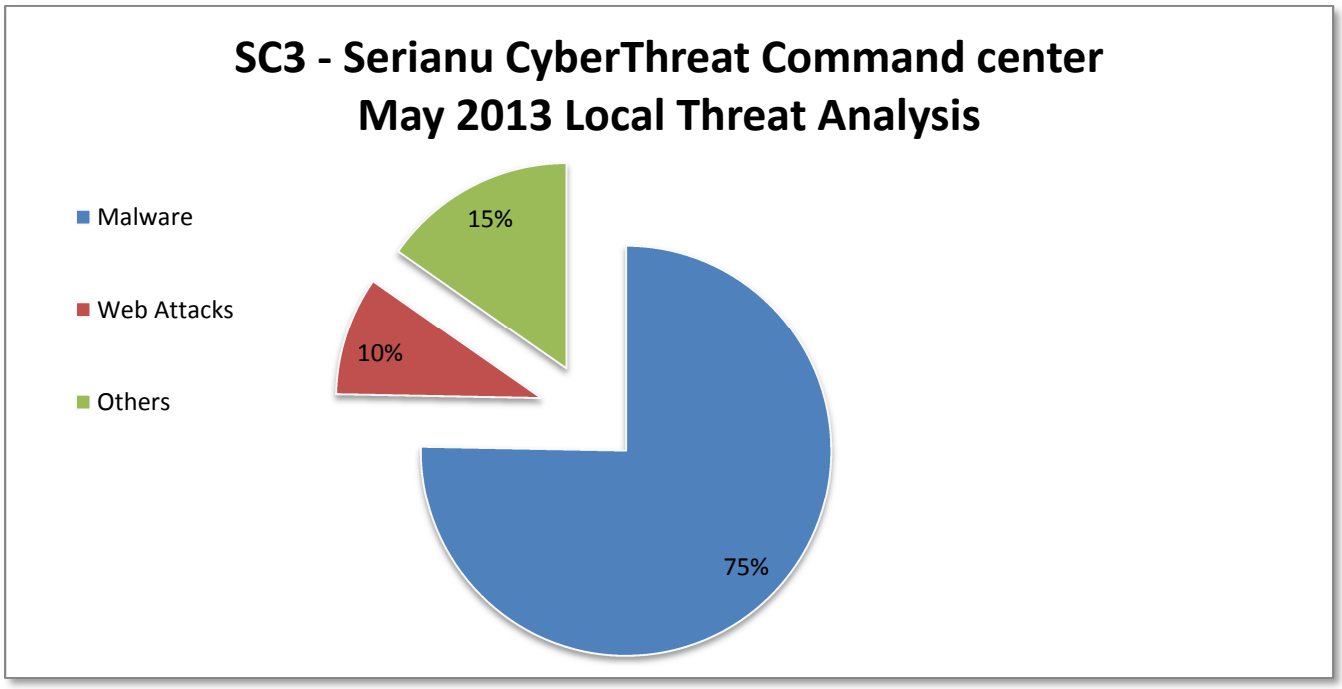
•75.3 % of the events were related to some form of malware including 4732 which were identified as Trojan related activity.

About the Serianu Cyber Threat Alert Service

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

• 9.4% of the events were classified as other risk types including suspicious email activity, suspicious active network services, and connections to known infected sites. Including spyware and protocol attacks

• 15.3% of the events were classified as others for any minor configurations challenges; this includes issues around poor server configuration and other related weaknesses.



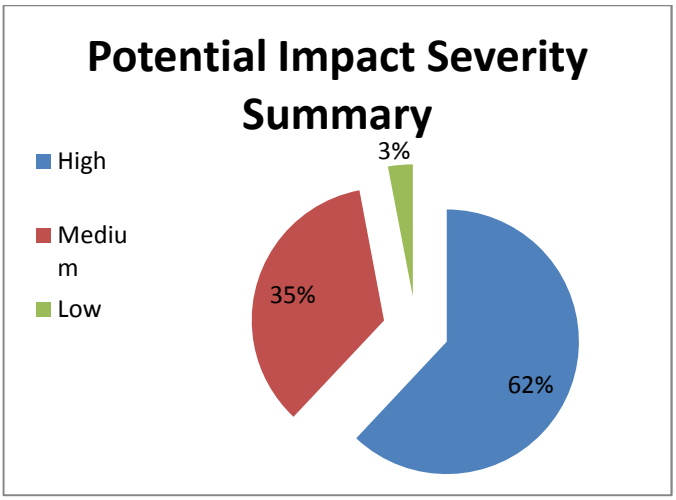
Affected Systems:

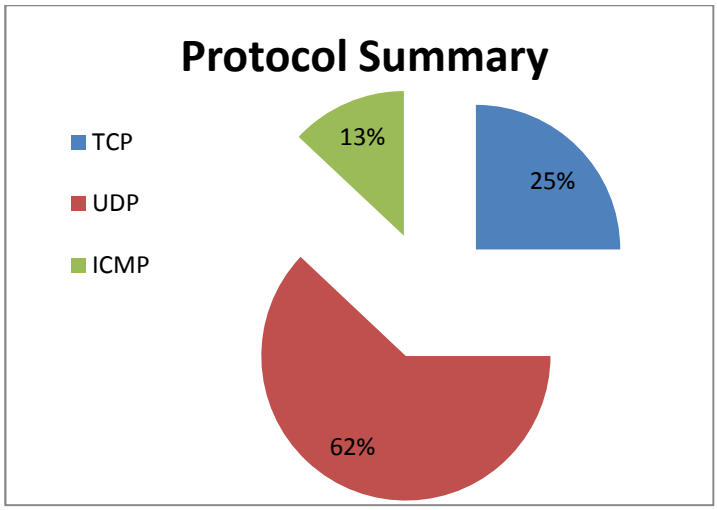
Malware- Microsoft Office Excel 2000 Service Pack 3 and rated Important for Excel 2002 Service Pack 3, Excel 2003 Service Pack 2, Excel 2003 Service Pack 3, Excel Viewer 2003, Excel Viewer 2003 Service Pack 3, Excel 2007, Excel 2007 Service Pack 1, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Service Pack 1, Microsoft Office Excel Viewer, and Microsoft Office SharePoint Server 2007

Exploitation

About the Serianu Cyber Threat Alert Service

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





Successful exploitation of web services and distribution of malware is done through UDP and TCP protocols by attackers. This is because TCP protocol is the original core protocol for the internet suite and UDP is the communication protocol used for exchange of messages in a network, these are commonly used protocols for web services.

In the case of policy violation, employee's who access restricted sites pose a threat to the organization by exposing them to malware and malicious sites.

The most commonly attacked ports are;

- Port 53- DNS servers bind to this port, it commonly used for DDoS attacks
- Ports 60937/5222/49209- UDP/TCP bind to this port, it is commonly used for web attacks and distribution of malware

Mitigation:

- Examining preventative controls such as user awareness around safe-computing habits and behaviors.
- Reviewing the detective/preventative controls such as host-based anti-virus, DNS black-holing, network content inspection, intrusion detection/prevention, and network access controls such as firewalls, isolation/segmentation and host-based protections.
- Assessing the corrective controls such as security incident response and the investigation and reporting of any security breaches.
- Improving security control policies.
- Delivering specific training and awareness to those involved.
- Building procedures and processes to identify current vulnerabilities and manage them.
- Selecting, designing and implementing technologies to automate control enforcement.
- Implementing procedures to ensure security controls are regularly reviewed and improved and necessary.

About the Serianu Cyber Threat Alert Service

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