NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES
9th September 2019

COMMUNICATIONS AUTHORITY OF KENYA

Top Stories

Source 1: Wired (https://www.wired.com/)
https://www.wired.com/story/ios-hacks-apple-response/

Apple Finally Breaks Its Silence on iOS Hacking Campaign. A sustained attack against iPhone users that compromised their devices almost instantly when they visited certain websites was launched. When compromised, the malware could steal user files, access their iOS Keychains—which store passwords and other sensitive data—and monitor live location data. It requested new instructions remotely from a command and control server every 60 seconds that means attackers could also potentially read or listen to communications sent through encrypted messaging services, like iMessage or Signal, because these programs still decrypt data on the sender's and receiver's devices.

Source 2: ZDNet (https://www.zdnet.com/)
https://www.zdnet.com/article/protonmail-pushes-back-against-claims-it-is-partnering-with-huawei/
ProtonMail pushes back against claims it is partnering with Huawei. Swiss-based encrypted email provider ProtonMail has hit back at claims it is forming a partnership with Huawei. ProtonMail published a blog post saying it is not partnering with Huawei but considering allowing ProtonMail to be used by people with Huawei devices by simply looking to publish its Android apps on F-droid, and was considering the Samsung Galaxy Store, the Amazon App store, and the Huawei AppGallery as alternate distribution channels.

Source 3: The Economic Times (https://economictimes.indiatimes.com/)
https://economictimes.indiatimes.com/tech/internet/atm-hacking-tools-trending-on-the-dark-web/articleshow/71041673.cms
ATM hacking tools trending on the dark web. An ATM can now be hacked in less than 15 minutes using tools such as malware cards which includes PIN descriptor, trigger card and an instruction guide, and USB ATM Malware.

System vulnerabilities

Source 1: Bleeping Computer (https://thehackernews.com/)

https://thehackernews.com/2019/09/facebook-hhvm-vulnerability.html
Facebook Patches "Memory Disclosure Using JPEG Images" Flaws in HHVM Servers. Facebook has patched two high-severity vulnerabilities in its server application that could have allowed remote attackers to obtain sensitive information or cause a denial of service just by uploading a maliciously constructed JPEG image file.

Source 2: CNBC (https://www.cnbc.com/)
https://www.cnbc.com/2019/09/06/hack-of-jack-dorseys-twitter-account-highlights-sim-swapping-threat.html
Here's how the recent Twitter attacks probably happened and why they're becoming more common. Scammers are increasingly using SIM swapping as a means of taking over phones and going after online accounts. Internet companies are taking a lot of the blame, but the phone carriers are also at fault. SIM swap involves a scammer who has obtained the phone number and other personal information of someone else calls a wireless carrier pretending to be the victim and requests that number be transferred to a new SIM card. Its in doing this that an attacker will receive messages with one-time passwords, negating the effectiveness of two-factor authentication thus impersonating individuals.

Malware

Source 1: CYWARE (https://cyware.com/)

https://cyware.com/news/orcus-rat-a-sneak-peek-into-the-remote-access-trojans-malicious-campaigns-5ff1a239/

Orcus RAT: A sneak peek into the Remote Access Trojan's malicious campaigns. Orcus RAT is a Remote Access Trojan (RAT) that has been active since 2016. Orcus was developed by a malware author who goes under the name 'Sorzus'. This RAT has been sold for $40 since April 2016, with the ability to build custom plugins. Orcus RAT is primarily distributed via spear-phishing emails and drive-by-downloads. Its capabilities include keylogging, stealing system information and credentials, taking screenshots, recording audio/video and real-time scripting among other capabilities.

Source 2: Bleeping Computer (https://www.bleepingcomputer.com/)

https://www.bleepingcomputer.com/news/security/fake-paypal-site-spreads-nemty-ransomware/

Fake PayPal Site Spreads Nemty Ransomware. A web page pretending to offer an official application from PayPal promises to return 3-5% from purchases made through the payment system is currently spreading a new variant of Nemty ransomware to unsuspecting users. The operators of this file-encrypting malware are trying various distribution channels as it was recently observed as a payload from the RIG exploit kit (EK). The ransom demand from tests was 0.09981 BitCoin (BTC), which is about $1,000, and that the payment portal is hosted in the Tor network for anonymity. Fortunately, the malicious executable is detected by most popular antivirus products on the market. A scan on VirusTotal shows that it is detected by 36 out of 68 antivirus engine.

DDoS/Botnets

Source 1: CYWARE (https://cyware.com/)

https://cyware.com/news/fakespy-operators-target-japanese-users-with-new-funkybot-malware-ba2f035e/

FakeSpy operators target Japanese users with new FunkyBot malware. FunkyBot harvests a victim's list of contacts to ease its propagation process. In its last stage, the malware alters the device settings to make itself the default SMS handler application. It then uses this to upload to the C2 all the received messages. This functionality can be very dangerous, considering that most banks currently use two-factor authentication through SMS," Durando noted.

Spam & Phishing

Source 1: Gulf News UAE (https://gulfnews.com/)

https://gulfnews.com/uae/dubai-police-warn-residents-against-fake-calls-and-anonymous-people-to-avert-financial-scams-1.66281458

Dubai police alert on fake calls. Dubai police have once again warned residents against fake callers and anonymous people who try to different tricks to extort money by employing social engineering techniques.

Spam & Phishing

Source 2: CYWARE (https://cyware.com/)

https://cyware.com/news/what-is-bait-switch-attack-and-how-is-it-different-from-clickjacking-d33b450a/

What is Bait & Switch attack and how is it different from Clickjacking? Both these techniques can be used to steal login credentials and personal details using relatively trusted avenues. 'Bait & Switch' is a type of fraud that uses relatively trusted avenues - ads - to trick users into visiting malicious sites. Whereas is a malicious technique that tricks a user into clicking a webpage that is invisible or disguised as another element.

Web security

Source 1: CYWARE (https://cyware.com/)

https://cyware.com/news/how-can-remote-browser-isolation-secure-you-from-web-based-threats-e9da13ea

How can remote browser isolation secure you from web-based threats? Remote browsing isolation is a method to enjoy a seamless malware-free version of the internet. It isolates the web-based malware from reaching your computer, thus securing the integrity of a network. This done by executing codes from a web page in a secure virtual container on a server situated between a user's device and the internet. Only the visual content of the web page along with files are sent to the users. Therefore confining attack impact to the container which is destroyed after every session.

Source 2: Bleeping Computer (https://www.bleepingcomputer.com/)

https://www.bleepingcomputer.com/news/security/critical-exim-tls-flaw-lets-attackers-remotely-execute-commands-as-root/

Critical Exim TLS Flaw Lets Attackers Remotely Execute Commands as Root. The flaw tracked as CVE-2019-15846 is exploitable by sending a Server Name Indication (SNI) ending in a backslash-null sequence during the initial Transport Layer Security (TLS) handshake which leads to Remote Code Execution (RCE) with root privileges on the mail server.

Bulletins

Source 1: US-CERT - Security Bulletin Mailing List (http://www.us-cert.gov/cas/bulletins/)
https://www.us-cert.gov/ncas/bulletins/sb19-245
Vulnerability Summary for the Week of August 26, 2019. Recorded by National Institute of Standards and Technology and National Vulnerability.

Source 2: Oracle Security Bulletins (http://www.oracle.com/technetwork/topics/security/alerts-086861.html)

https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html
Oracle Critical Patch Update Pre-Release Announcement - July 2019; advised action to run available security updates.

https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2729-5570780.html
Oracle Security Alert Advisory - CVE-2019-2729. Decentralization vulnerability in Oracle WebLogic Server exploitable without authentication requirements; advised action to run security updates.

https://www.oracle.com/technetwork/topics/security/bulletinjul2019-5600410.html
Oracle Solaris Third Party Bulletin - July 2019; advised action to apply necessary patches.

https://www.oracle.com/technetwork/topics/security/linuxbulletinjul2019-5600392.html
Oracle Linux Bulletin - July 2019; advised action to apply necessary Oracle Linux Bulletin fixes.

https://www.oracle.com/technetwork/topics/security/public-vuln-to-advisory-mapping-093627.html
Map of CVE to Advisory/Alert; advised action to apply the critical patch update for protection against known vulnerabilities.

https://www.oracle.com/technetwork/topics/security/ovmbulletinjul2019-5600406.html
Oracle VM Server for x86 Bulletin - July 2019; advised action to apply necessary Oracle VM Server for x86 Bulletin fixes.

Updates & Alerts

Source 1: Cisco Security Advisories & Alerts(http://tools.cisco.com/security/center/publicationListing.x)

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190513-secureboot

Cisco Secure Boot Hardware Tampering Vulnerability. Due to an improper check on the area of code that manages on premise updates to a Field Programmable Gate Array (FPGA) part of the Secure Boot hardware implementation an attacker could write a modified firmware image to the component.

Source 2: Bleeping Computer (https://www.bleepingcomputer.com/)

https://www.bleepingcomputer.com/news/security/google-calendar-spam-got-you-down-a-fix-is-on-the-way/

Google Calendar Spam Got You Down? Google is working on a solution to stop spammers from abusing a Google Calendar feature designed to automatically add event invitations to its users' calendars after receiving countless reports about spam events over the last few months.

COMMUNICATIONS AUTHORITY OF KENYA

COMMUNICATIONS AUTHORITY OF KENYA

www.ke-cirt.go.ke