NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES
8th June 2020

COMMUNICATIONS AUTHORITY OF KENYA

Summary Headlines	Impact Metric Against Count of Events			
	Critical	High	Medium	Informative
Regional Highlights	0	0	0	0
Top Stories	0	2	0	1
System Vulnerabilities	1	0	0	1
Malware	0	1	2	0
DDoS/Botnets	0	1	0	0
Spam & Phishing	0	0	2	0
Web Security	0	0	1	1
Updates & Alerts	0	0	0	2

Top Stories

Source 1 : YonHap News (https://en.yna.co.kr/)
https://en.yna.co.kr/view/AEN20200608011200325?&web_view=true
Impact value: High
Korean credit card data leaked overseas, group reports. Details of some 900,000 credit cards held by South Koreans were leaked and traded on overseas online black markets, South Korea's credit association said Monday. The leaked information included the card numbers, expiration dates and validation codes, a three-digit security code on the back of cards. No passwords have been leaked.

Source 2 : CISO (https://ciso.economictimes.indiatimes.com/)
https://ciso.economictimes.indiatimes.com/news/80-hacking-attacks-linked-to-bad-password-habits-report/76256068
Impact value: Information
80% hacking attacks linked to bad password habits. Nearly 80% of hacking attacks are password-related breaches, claims a latest report by Secure Link. As per the report, even in 2017, almost the same amount of hacking-related breaches were linked to passwords. And the trend has continued, says the report terming it a cause of concern. The findings of the report reveal that phishing is a common way that hackers adopt to get access to internet users credentials.

Source 3 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/us-energy-providers-hit-with-new-malware-in-targeted-attacks/
Impact value: High
US energy providers hit with new malware in targeted attacks. The attacks took place between July and November 2019, and the threat actor behind it — tracked as TA410 by Proofpoint researchers who spotted the campaigns — used portable executable (PE) attachments and malicious macro laden Microsoft Word document to deliver the malicious payload.

System vulnerabilities

Source 1 : Security Affairs (https://securityaffairs.co/)
https://securityaffairs.co/wordpress/104459/breaking-news/digilocker-critical-falw.html
Impact value: Critical
Digilocker. Digilocker, an app by the Indian government for securely storing personal documents, was found to have a critical flaw that could have allowed attackers to bypass mobile one-time passwords (OTP) and access the sensitive documents of any user. The flaw was fixed by the government on May 28 with the release of the latest version of the app.

Source 2 : ZDnet (https://www.zdnet.com/)
https://www.zdnet.com/article/vulnerabilities-in-popular-open-source-projects-doubled-in-2019/
Impact value: Informative
Vulnerabilities in popular open source projects doubled in 2019. A study that analyzed the top 54 open source projects found that security vulnerabilities in these tools doubled in 2019, going from 421 bugs reported in 2018 to 968 last year. According to RiskSense's "The Dark Reality of Open Source" report, released today, the company found 2,694 bugs reported in popular open source projects between 2015 and March 2020. The report didn't include projects like Linux, WordPress, Drupal, and other super-popular free tools, since these projects are often monitored, and security bugs make the news, ensuring most of these security issues get patched fairly quickly.

Malware

Source 1 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/kupidon-is-the-latest-ransomware-targeting-your-data/
Impact value: High
Kupidon ransomware. Researchers from MalwareHunterTeam discovered a new ransomware called Kupidon. The ransomware target both corporate networks and personal devices of individuals. It drops different ransom notes based on the targets and encrypts and appends the victims' file names after encryption with the ".kupidon" extension.

https://www.bleepingcomputer.com/news/security/honda-investigates-possible-ransomware-attack-networks-impacted/
Impact value: Medium
Honda investigates possible ransomware attack, networks impacted. Computer networks in Europe and Japan from giant car manufacturer giant Honda have been affected by issues that are reported related to a SNAKE Ransomware cyber attack. Details are unclear at the moment but the company is currently investigating the cause of the problems that were detected on Monday.

Source 2 : Trend Micro (https://blog.trendmicro.com/)
https://blog.trendmicro.com/trendlabs-security-intelligence/new-tekya-ad-fraud-found-on-google-play/
Impact value: Medium
Tekya ad fraud app. Check Point researchers found a new variant of the Tekya Android ad fraud malware family. The new variant was being distributed by masking as five legitimate-looking apps on the Google Play Store. The new Tekya variant is designed to target up to 11 different advertising networks including Admob, Facebook, and Unity. Following the discovery, Google removed the five apps from the store.

Botnets/DDoS

Source 1 : Krebsonsecurity (https://krebsonsecurity.com/)
https://krebsonsecurity.com/2020/06/owners-of-ddos-for-hire-service-vdos-get-6-months-community-service/?web_view=true
Impact value: High

Owners of DDoS-for-Hire Service vDOS Get 6 Months Community Service. The co-owners of vDOS, a now-defunct service that for four years helped paying customers launch more than two million distributed denial-of-service (DDoS) attacks that knocked countless Internet users and websites offline, each have been sentenced to six months of community service by an Israeli court.

Spam & Phishing

Source 2 : Threat Post (https://threatpost.com/)
https://threatpost.com/phishing-attack-german-coronavirus-task-force/156377/
Impact value: Medium

Phishing Attack Hits German Coronavirus Task Force. Researchers are warning of an ongoing phishing attack that's targeting the credentials of more than 100 high-profile executives at a German multinational corporation that's tasked with procuring coronavirus medical gear for Germany. Researchers who discovered the phishing attack believe its perpetrators may be targeting multiple firms, and third-party supply chain partners, associated with the task force.

Source 3 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/new-avaddon-ransomware-launches-in-massive-smiley-spam-campaign/
Impact value: Medium

New Avaddon Ransomware launches in massive smiley spam campaign. The new Avaddon Ransomware has come alive in a massive spam campaign targeting users worldwide. Avaddon was launched at the beginning of this month and is actively recruiting hackers and malware distributors to spread the ransomware by any means possible. As its first known attack, the Avaddon Ransomware is being distributed in a spam campaign reminiscent of February's Nemty Ransomware Love Letter campaign.

Web Security

Source 1 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/facebook-sues-company-for-registering-impostor-domains/
Impact value: Informative
Facebook sues company for registering impostor domains. Facebook filed a lawsuit today against Compsys Domain Solutions Private Ltd, an Indian provider of proxy/privacy services, for registering domains that impersonate Facebook apps and were allegedly used for malicious purposes. According to the social network's IP Litigation Director and Associate General Counsel Christen Dubois, Compsys did not respond to any requests to clarify their intents. This lawsuit was filed by Facebook "to prevent fraud and stop the malicious use of our company and product names.“

Source 2 : ZDnet (https://www.zdnet.com/)
https://www.zdnet.com/article/privacy-browser-brave-busted-for-autocompleting-urls-to-versions-it-profits-from/
Impact value: Medium
Privacy browser Brave busted for autocompleting URLs to versions it profits from. Brave, the privacy-focused Chromium browser from Mozilla co-founder and JavaScript creator Brendan Eich, has come under fire for automatically redirecting URLs typed into the browser's address bar to a version of the URL it profits from. Brave is trying to carve out a new business model by offering users the choice of viewing ads in exchange for Brave's cryptocurrency, the Basic Attention Token (BAT).

Bulletins

Source 1: US-CERT - Security Bulletin Mailing List (http://www.us-cert.gov/cas/bulletins/)
https://www.us-cert.gov/ncas/bulletins/sb20-160
Vulnerability Summary for the Week of June 1, 2020. 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/security-alerts/cpujan2020.html
Oracle Critical Patch Update Advisory - January 2020; advised action to run available security updates.

https://www.oracle.com/security-alerts/alert-cve-2019-2729.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/security-alerts/bulletinoct2019.html
Oracle Solaris Third Party Bulletin - October 2019; advised action to apply necessary patches.

https://www.oracle.com/security-alerts/linuxbulletinoct2019.html
Oracle Linux Bulletin - October 2019; advised action to apply necessary Oracle Linux Bulletin fixes.

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

https://www.oracle.com/security-alerts/linuxbulletinoct2019.html
Oracle VM Server for x86 Bulletin - October 2019; advised action to apply necessary Oracle VM Server for x86 Bulletin fixes.

Updates & Alerts

Source 1 : ZDnet (https://www.zdnet.com/)
https://www.zdnet.com/article/ibm-announces-exit-of-facial-recognition-business/
Impact value: Informative
IBM announces exit of facial recognition business. IBM has announced it will no longer be offering general purpose facial recognition technology in fear that it could be used to promote racial discrimination and injustice. "IBM firmly opposes and will not condone uses of any technology, including facial recognition technology offered by other vendors, for mass surveillance, racial profiling, violations of basic human rights and freedoms, or any purpose which is not consistent with our values and Principles of Trust and Transparency," IBM CEO Arvind Krishna wrote in a letter to Congress on Monday.

Source 2 : Duo (https://duo.com/)
https://duo.com/decipher/google-adds-webauthn-support-for-security-keys-on-ios?&web_view=true#eyJoYXNoIjoiIiwic2VhcmNoIjoiPyZ3ZWJfdmlldz10cnVlIn0=
Impact value: Informative
Google Adds Webauthn Support For Security Keys On Ios. “Starting today, we’re rolling out a change that enables native support for the W3C WebAuthn implementation for Google Accounts on Apple devices running iOS 13.3 and above. This capability, available for both personal and work Google Accounts, simplifies your security key experience on compatible iOS devices and allows you to use more types of security keys for your Google Account and the Advanced Protection Program,” Christiaan Brand, a product manager for Google Cloud, said.

www.ke-cirt.go.ke