NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES
21st 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	0	0	2
System Vulnerabilities	0	2	0	0
Malware	0	0	0	1
DDoS/Botnets	0	0	0	0
Spam & Phishing	0	0	0	1
Web Security	0	0	0	1
Updates & Alerts	0	0	0	1

COMMUNICATIONS AUTHORITY OF KENYA

Top Stories

Source 1 : info Security (https://www.infosecurity-magazine.com/)

https://www.infosecurity-magazine.com/news/sophisticated-statebacked-attack/

Impact value: Informative

Australian Prime Minister Scott Morrison warned of a high threat state-sponsored cyber espionage campaign targeting both the government and private sector within the country. Morrison urged domestic organizations to improve their security practices such as enabling multi-factor authentication and installing released patches immediately. Morrison also stated that the threatening activity is targeting Australian organizations across sectors including political organizations, education, health, critical infrastructure, government, and industry. Australian officials have confirmed that it is a sophisticated state-backed cyber actor due to the scale and advanced nature of the targeting and techniques used. The cybercriminals have shown that they can quickly leverage public proofs-of-concept to target their victims, seeking vulnerable services to launch remote code execution.

Source 2 : The Straits Time (https://www.straitstimes.com/)

https://www.straitstimes.com/asia/se-asia/indonesia-probing-alleged-covid-19-test-data-breach

Impact value: Informative

An unknown hacker has allegedly breached a government database of 230,000 people who have undergone COVID-19 testing. The hacker, under the username Database Shopping, offered the personal data of COVID-19 test-takers in Indonesia on the data-exchange platform Raid Forums, where another member put up for sale the personal information of 15 million users from homegrown e-commerce unicorn Tokopedia's internal database for US$5,000.

System vulnerabilities

Source 1 : info Security (https://www.infosecurity-magazine.com/)
https://www.infosecurity-magazine.com/news/malicious-chrome-extensions/
Impact value: High
Malicious Chrome browser extensions were used in a massive surveillance campaign aimed at users working in the financial services, oil and gas, media and entertainment, healthcare, government organizations, and pharmaceuticals. The malicious Chrome browser extensions were discovered by researchers from Awake Security that shared their findings with Google. Experts pointed out that the attackers also used the Google Chrome browser extensions to create persistent footholds on corporate networks. The malicious Chrome browser extensions were free, they are masqueraded as applications to either alert users to questionable websites or to convert files.

Malware

Source 1 : The Sydney Morning Herald (https://www.smh.com.au/)
https://www.smh.com.au/technology/cyber-crisis-deepens-at-lion-as-second-attack-bites-beer-giant-20200618-p5540c.html

Impact value: Informative

A threat actor group with potential ties to China called Cycldek may have more sophisticated capabilities than researchers previously thought after security vendor Kaspersky released an analysis The Australian beverages company and dairy conglomerate Lionwas the victim of a new cyberattack, Sydney Morning Herald reported. Lion is a beverage and food company that operates in Australia and New Zealand, and a subsidiary of Japanese beverage giant Kirin. It produces and markets a range of beer, wine, cider, RTDs and spirits, as well as dairy and other beverages. This is the second cyber attack is a few days, last week the systems at Lion were infected with the REvil ransomware and attackers demanded a ransom of reportedly $1 million last week. At the time of the first attack, the security breach caused the disruption of manufacturing processes and customer service.

Spam & Phishing

Source 1 : Business Today (https://www.businesstoday.in/)
https://www.businesstoday.in/latest/trends/massive-phishing-attack-could-steal-all-your-bank-account-personal-details-warns/story/407558.html

Impact value: Informative

There is an imminent threat of a massive phishing attack in India, according to the Cert-In. The new phishing attack could imitate government organizations and can steal sensitive personal data and financial information. The new advisory claims that the phishing attack, conducted by "malicious actors", will be done in the guise of a Covid-19 related directive and it is expected to begin on 21 June. These cyber-attacks will be focused on both individuals and business organizations ranging from small to large.

Web Security

Source 1: The Tech Education (https://thetecheducation.com/)

https://thetecheducation.com/microsoft-adding-chromium-based-edge-browser-to-even-unsupported-windows-7/

Impact value: Informative

Thanks to a surprise update in Windows 7 through Windows Update, the new Edge browser will be installed without replacing the long-lived Internet Explorer. Windows 7 and Windows 8.1 users will also be able to enjoy the new Edge browser via update through Windows update. Although Microsoft announced that Windows 7 and Windows 8.1 users would also be able to enjoy Microsoft's new browser, this would have to be through a manual update if they wanted, but now it has been discovered that through Windows update In an update, the new Edge is coming.

Bulletins

Source 1: US-CERT - Security Bulletin Mailing List (http://www.us-cert.gov/cas/bulletins/)

https://www.us-cert.gov/ncas/bulletins/sb20-167

Vulnerability Summary for the Week of June 8, 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: 9to5mac (https://9to5mac.com)

https://9to5mac.com/2020/06/21/kuo-13-3-inch-macbook-pro-and-imac-will-be-the-first-arm-macs-to-be-released-as-soon-as-q4-after-redesigned-intel-imac-launch/

Impact value: Informative

Apple's annual Worldwide Developers Conference (WWDC) keynote is happening on Monday, June 22nd, however in a very different form than usual, due to the COVID-19 pandemic. The show must go on, so Apple will soon be presenting the complete conference in a new, digital-only format. The company remains expected to unveil the very first look at the future of iOS, macOS, watchOS, and tvOS — the different suites of software that power all Apple's hardware.

COMMUNICATIONS AUTHORITY OF KENYA

www.ke-cirt.go.ke