CPIDER

Cyber Patrol for Identification of Emergent Risks

Vulnerability in Google Chrome Browser

A serious security flaw has been detected in Google Chrome browser by security researchers Anton Ivanov and Alexey Kulaev at Kaspersky. The vulnerability which has been detected in the browsers audio component can be exploited by hackers to hijack computers. Google has urged users to upgrade to the latest version of Chrome. *(https://threatpost.com/google-discloses-chrome-flaw-exploited-in-the-wild/149784/)*

Date Leak Incident Reported by Facebook

Facebook has reported a fresh data breach incident targeting users' data in certain Facebook groups. The company admitted that around 100 app developers might have accessed user data like personal details, photos and videos unauthorisedly. Though Facebook has not revealed the total number of users affected by the breach, it has assured users that all unauthorised access has been stopped. *(https://thehackernews.com/2019/11/facebook-groups-data-leak.html*

Fake Customer Care Numbers used for Cyber Fraud

Fast emerging as one of the most common frauds on internet today, fake customer care and business helpline numbers are being used to dupe people of their hard-earned money. Fraudsters take advantage of the fact that Google allows users to edit contact details and phone numbers of businesses and other establishments on Google Maps and Google search to improve these services. Once the fake numbers are listed, a simple Google search online or a query to any of the smart voice assistants like Siri, Google Assistant or Alexa will throw up these numbers which can then used by fraudsters posing as customer care executives to scam gullible people into sharing their personal details, bank account numbers and other sensitive information as most people believe the results provided by search engines to be authentic. It is advisable to visit the official website of the concerned business or establishment for customer care details rather than use Google search.

(https://www.gadgetsnow.com/slideshows/this-is-the-most-common-google-scam-that-people-are-losing-money-to/It-is-highly-advisable-to-not-rely-on-Google-search-for-customer-care-contact-details-Visit-official-websites-for-the-same/photolist/71105252.cms)

Drones as a Network Security Threat

Security researchers have warned that drones could become a major security threat over the coming years. By flying close to the targeted network the drone can be used as a rogue access point to gain unauthorised access to the network, carry out data theft as well as carry out network reconnaissance. IoT devices and Bluetooth enabled devices are specially vulnerable to such attacks. It is advisable to use strong network credentials as well as encryption and firewall on all networks.

https://www.infosecurity-magazine.com/news/experts-warn-flying-network/

Malware targets cloud security

According to a research published by Pew Research Centre 40% of adult internet users have experienced some kind of online harassment. This includes name calling, cyber stalking, sexual harassment and physical threats. Youth comprised the most likely demographic group to experience such harassment.

(https://www.pewresearch.org/internet/2014/10/22/part-1-experiencing-online-harassment/)

http://jkpolice.gov.in/E-Crime-Awareness

Lasers Used for Hacking Smart Devices

Japanese researchers Takeshi Sugawara and Kevin Fu have discovered that lasers can be used to send voice commands to smartphones and virtual home assistants like Alexa to take control of the device. The researchers found that a laser pointed at the microphone of the device was interpreted by the device as a voice command. Suitably adjusted, the laser can be used to talk to the device and make it respond even from hundreds of feet away. Devices that use a passcode rather than a simple wake up command are less vulnerable to the breach.

(https://www.scmagazine.com/home/security-news/mobile-security/freaking-lasers-can-carry-voice-commands-to-smart-devices/)

Apple AppStore Hit by 'Clicker Trojan Malware'

17 malicious apps have been removed by Apple from AppStore that were infected with 'Clicker Trojan Malware'. The trojan has been designed to carry out malicious activities like subscribing to various paid online services in the background without user permission, generating revenue for the attacker. All 17 apps had been developed by the same developer India based AppAspect Technologies Pvt. Ltd. The company has also developed 28 applications in Google PlayStore however none of them was found to be carrying out any malicious activity.

(https://www.securityweek.com/click-fraud-trojan-found-apple-app-store)

The United Nations has been the target of a phishing attack launched with the goal of obtaining login credentials of personnel. *(https://www.scmagazine.com/home/security-news/phishing/un-ngos-targeted-by-ongoing-phishing-attack/)*