InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Hackers Stole data of over 70% in Bulgaria
2. Faceapp's viral Success proves we will never take our digital privacy seriously
3. Spearphone Side Channel Attack
4. Microsoft, iOS Bluetooth devices able to track and identify users
5. Arbitrary Code Injection in LibreOffice
6. Google Home Silently Captures Recordings
7. Hackers spy on Linux Users
8. RCE flaw in Ring central and Zhumu for Macs

21/07/2019

Introduction to InfoSec Weekly

InfoSec Weekly is a compilation of security related news feed that aims to update the readers about cyber security, cyber threats, malware attacks, new technologies and cyber security awareness every week. We primarily cover events and news related to offensive side of the Information Security such as hacking, password and sensitive information leakage, new vulnerabilities and important CVE's that can impact an individual or an organization. We also aim to provide defensive tactics to overcome known vulnerabilities that can protect organizations and individuals from any attacks.

Our main aim is to spread awareness regarding various cyber related threats.

About Us

We are a team of security enthusiasts with an aim to provide various Information Security Services to organizations. Our company aims to provide professional grade cyber security solutions for all your Information Technology infrastructures. Our team has been demonstrating penetration testing skills using methodologies such as OSSTMM, NIST and OWASP. We aim to help companies protect their valuable data from any internal or external threats. Our team members have been practicing their skills to detect and report vulnerabilities in a live environment. Organizations such as Google, Facebook, Twitter, Yahoo!, ebay, eset, bugcrowd, under armour, coinbase, CCM, etc have recognized our team members for reporting vulnerabilities and have helped these organizations from malicious users. Our team's professional work experience consists of various Government organizations, National and International based private organizations, INGOs, etc. Our Services ranges from VAPT, Incident Response, Information Security Training, Endpoint threat analysis, Cyber security consultant, etc.

1. Hackers Stole data of over 70% in Bulgaria

Description	
Eastern European country Bulgaria has suffered the biggest data breach in its history as an unknown hacker stole data included taxpayer's personal identifiable numbers, addresses, and financial data from the Tax Agency Server.	
Source	https://www.reuters.com/article/us-bulgaria-cybersecurity/hackers-steal-millions-of-bulgarians-financial-records-tax-agency-idUSKCN1UB0MA

2. Faceapp's viral Success proves we will never take our digital privacy seriously

Description	
FaceApp has gone viral once again with 'the old age" filter proving to be popular on Twitter, Instagram and others social sites. But the terms and conditions of the app raises some serious privacy issues that should not be ignored. One major issue is that by using the app you are granting it license to use your edited photos anywhere, even for commercial purpose.	
Source	https://edition.cnn.com/2019/07/17/tech/faceapp-privacy-concerns/index.html
Infected Technology	Mobile Application
Recommendation	Due to privacy concerns, installing such apps are not recommended until further research has been performed

3. Spearphone Side Channel Attack	
Description	
An accelerometer, which comes built into most Android devices and can be unrestrictedly accessed by any app installed on a device even with zero permissions. The in-built accelerometer in the smart phones can be used to capture the sound reverberation(echo) if the sound is being played from the loudspeaker.	
Source	**https://arxiv.org/pdf/1907.05972.pdf**
Infected Technology	**Android**
Recommendation	**These solutions are for developers. Android platform could implement stricter access control policies that restrict the usage of the sensors. The internal build of the smartphone should be such that the motion sensors are insulated from the vibrations**

4. Microsoft, iOS Bluetooth devices able to track and identify users

Description	
Vulnerability in Bluetooth communication protocol was discovered which may expose these device users to tracking. Microsoft and iOS devices advertise their MAC addresses to prevent long term tracking, but it was found that it was possible to minimize the randomization of these addresses to permanently monitor a specific device using a certain algorithm. Address-carryover algorithm developed by researchers from Boston University can "exploit the asynchronous nature of payload and address changes to achieve tracking beyond the address randomization of a device."	
Source	https://petsymposium.org/2019/files/papers/issue3/popets-2019-0036.pdf
Infected Technology	Microsoft, iOS
Recommendation	Patch will be sent by the vendors

5. Arbitrary Code Injection in LibreOffice

Description	
LibreOffice was discovered to have incorrectly handled LibreLogo scripts. A remote attacker could cause LibreOffice to execute an arbitrary code if a user were tricked into opening a specially crafted document. This is possible because LibreLogo can be manipulated into executing arbitrary python commands.	
Source	https://nvd.nist.gov/vuln/detail/CVE-2019-9848
Recommendation	Apply the patch made available by the LibreOffice

6. Google Home Silently Captures Recordings

Description	
It has been claimed that Google have been capturing and recording highly personal audio of domestic violence, confidential business calls among others. It is stated in Google's terms and conditions that everything you say to your Google Smart speakers and Google Assistant is being recorded and stored. But the news of Google listening to conversations that we were not instructed have caused quite an issue. Google have been using these conversations to further develop algorithms related to speech technologies for different languages.	
Source	https://www.vrt.be/vrtnws/en/2019/07/10/google-employees-are-eavesdropping-even-in-flemish-living-rooms/
Recommendation	Do not download applications from third-party sites

7. Hackers spy on Linux Users

Description	
Evil Gnome, is a Gnome extension capable of taking screenshot, stealing files, capturing audio and downloading and executing further modules. It appears to be test version which was uploaded by mistake. It contains five modules to do malicious activities and received a new command from C&C server due to which the malware is able to download and execute files, change run time config, breakout stored data to C&C server.	
Source	https://www.securityweek.com/evilgnome-malware-helps-hackers-spy-linux-users
Infected Technology	Linux Distro
Recommendation	Update the system after it is available

8. RCE flaw in Ring central and Zhumu for Macs

Description	
Remote code execution(RCE) is a flaw that allows attacker to turn on users laptop's webcam and microphone remotely. RCE flaw has been found in ring central and zhumu software which runs a vulnerable hidden local web server on user's computer that offer an automatic click-to-join feature which was found vulnerable to remote command injection through third party website. Solution: Ring Central has already updated its version that patches the vulnerability by removing the vulnerable web server installed by software and apple silently released update for its macos user to remove all local web server for all users	
Source	https://www.andreafortuna.org/2019/07/16/zoom-rce-vulnerability-also-affects-ringcentral-and-zhumu/
Infected Technology	Desktop Application
Recommendation	Update the system after it is available

For any queries/recommendations:

Contact us: whois@cryptogennepal.com