InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. iOS 12.4 allows iPhone to be Jail-broken
2. Russian Hacking Group Targeting Banks
3. Google, Mozilla, Apple Block Kazakhstan's Root CA Certificate to Prevent Spying
4. New Bluetooth Vulnerability allows attackers to spy on encrypted connections
5. Use this privacy tool to view and clear 'Off-Facebook Activity' Data
6. Webmin infected with a backdoor by hackers

25/08/2019

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, Trip Advisor, 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. iOS 12.4 allows iPhone to be jail-broken again

Description

A rare pubic jailbreak for the most up-to-date version of iOS is circulating online after it was found that the recently released iOS 12.4 undid a patch in iOS 12.3. Researchers warn users to be cautious about installing apps from the App Store until Apple releases a patch.

Source	https://www.wired.co.uk/article/iphone-jailbreak-ios-12-4-update
Infected Technology	iOS
Recommendations	Do not install suspicious apps until further patch

2. Russian Hacking Group Targeting Banks

Description

Silence apt-a Russian hacking group is targeting financial organizations in more than 30 countries across America, Europe Africa and Asia. The group leverages more sophisticated TTP's (tactics, techniques and procedures) and deploy additional malware to collect information about an infected system and send it to command and control server.

This group is most sophisticated advanced persistent threat (APT) group that is now posing threats to banks worldwide. The APT group most recent successful campaign was against Bangladesh- based Dutch-Bangla Bank, which lost over $3 million ATM cash withdrawals.

Source	https://www.cybersecurity-review.com/news-august-2019/russian-hacking-group-targeting-banks-worldwide-with-evolving-tactics/
Infected Industry	Banks
Recommendations	Patch all available technologies in the organization; User awareness is critical

3. Google, Mozilla, Apple Block Kazakhstan's Root CA Certificate to Prevent Spying

Description

Major browsers like google, apple and Mozilla blocked Kazakhstan's government-issued root CA certificate as its government has intercept on internet traffic which undermines the integrity of a critical network security mechanism.

Source	https://arstechnica.com/tech-policy/2019/08/chrome-firefox-and-safari-updated-to-block-kazakhstan-government-spying/

4. New Bluetooth Vulnerability allows attackers to spy on encrypted connections

Description

Researchers at the Center for IT-Security, Privacy and Accountability (CISPA) found a new Bluetooth vulnerability, referred as Key Negotiation of Bluetooth (KNOB) attack, that could allow attackers to spy on encrypted connections. The vulnerability, tracked as CVE-2019-9506, resides in the way 'encryption key negotiation protocol' let's two Bluetooth Basic Rate/Enhanced Data Rate (also known as "Bluetooth Classic ") devices choose an entropy value for encryption keys while establishing a connection. An attacker near the victim's device could trigger the vulnerability to intercept or manipulate encrypted Bluetooth traffic between two paired devices.

Source	https://www.bluetooth.com/security/statement-key-negotiation-of-bluetooth/
Infected Technology	Bluetooth

5. Use this privacy tool to view and clear 'Off-Facebook Activity' Data

Description	
Facebook released a long-awaited privacy feature that will let user's clear information from apps and websites they browse outside of the social network. The social network is releasing the tool first in Ireland, South Korea and Spain.	
Source	https://thehackernews.com/2019/08/clear-off-facebook-activity.html

6. Webmin infected with a backdoor by hackers

Description	
A backdoor was found in a popular tool in *nix application that helps users to manage Unix-based systems. The bug was verified as a pre-authenticated command-injection that was installed during the development and Joe Cooper confirms that only the SourceForge repository contains the code and not the Webmin's Github repository.	
Source	https://www.theregister.co.uk/2019/08/19/webmin_project_zero_day_patch/
Infected Technology	Webmin
Recommendation	Update your Webmin as soon as possible

For any queries/recommendations:

Contact us: **whois@cryptogennepal.com**