InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Malicious Android SDKs Caught Accessing Facebook and Twitter User Data
2. Adobe Magento Marketplace Suffers data breach
3. Google Users Hit by Government Hackers
4. OnePlus Suffers New Data Breach

2/12/2019

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. Malicious Android SDKs Caught Accessing Facebook and Twitter User Data

Description	
The third-party Software Development Kits (SDK) used for advertisement purpose are not supposed to have access to user’s personal identifiable information, account password or secret access tokens generated during login with facebook or twiter processes. But OneAudience and Mobiburn- the third-party SDK integrated by hundreds of thousands of Android apps- have been caught holding unauthorized access to users’ data associated with their connected social media accounts. The OneAudience and Mobibum contains privacy-violating component which have ability to stealthy and unauthorizedly harvest users’ personal data and may have passed its users’ personal data to OneAudience servers.	
Source	https://yourstory.com/2019/11/malicious-third-party-apps-leak-personal-data-facebook-twitter
Infected Technology	Android SDK

2. Adobe Magento Marketplace Suffers data breach

Description	
Adobe disclosed today a security breach that impacted users registered on the company's Magento Marketplace, a portal for buying, selling, and downloading themes and plugins for Magento-based online stores.In an email sent to customers, the company said the point of entry was a vulnerability in the Magento Marketplace website that allowed "an unauthorized third-party" to access account information for registered users	
Source	https://nakedsecurity.sophos.com/2019/11/29/adobes-magento-marketplace-suffers-data-breach/

3. Google Users Hit by Government Hackers

Description	
Google tracked over 270 government-backed hacking group from over 50 countries that are involved in intelligence collection, stealing intellectual property or destructive cyber-attacks. According to Google, more than 90 percent of the targeted users were hit with “credential phishing emails” that tried to trick victims into handing over access to their google account. Government-backed hackers are targeting their account via phishing, malware or some other tactics, which generally targets activists, journalists, policymakers and politicians.	
Source	https://thehackernews.com/2019/11/google-government-hacking.html

4. OnePlus Suffers New Data Breach

Description	
A Chinese smartphone company OnePlus suffered a new data breach as a result of a vulnerability in its online store website. This vulnerability leads an unauthorized party to access order information of its customers, including their names, contact numbers, emails and shipping addresses. It was discovered that some of the users’ order information was accessed by an unauthorized party.	
Source	https://thehackernews.com/2019/11/oneplus-store-data-breach.html
Infected Organization	OnePlus

For any queries/recommendations:

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