InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. UniCredit reveals data breach exposing 3 millions customer records
2. Mysterious Malware Infects over 45000 Android phones
3. Pirate Bay suffer DDos attack
4. Google chrome zero day under active attack
5. Chinese hackers compromise telecom servers to spy on sms message
6. Adware Apps traced information back to developer Server
7. Microsoft SQL Server Backdoor Malware Spotted
8. Android banking Malware Uses SMS to Hack User Device

03/11/2019

www.cryptogennepal.com

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. Unicredit reveals data breach exposing 3 million customer records

Description	
Italian banking giant UniCredit has suffered a “data incident” that exposed 3 million customer records, including full names, phone numbers and email addresses.UniCredit issued an urgent security notice yesterday announcing that a file containing personally identifiable information (PII) of millions of customers had been leaked which file was created in 2015.	
Source	https://www.zdnet.com/article/unicredit-reveals-data-breach-exposing-3-million-customer-records/
Infected Industry	Banking sector

2. Mysterious Malware Infects over 45000 Android Phones

Description	
A mysterious malware named Xhelper has infected over 45,000 Android devices in the last six months. This malware reportedly reinstalls itself even after users delete it or resets their devices. It is believed that the malware may have been downloaded by users from unknown sources. After installation this malware remains hidden from the users. It downloads additional payloads such as droppers, clickers and rootkits on the compromised Android devices.	
Source	https://www.cisomag.com/mysterious-malware-infects-over-45000-android-phones/
Infected Technology	Android phones
Recommendation	Update patch when available

3. Pirate Bay Suffer DDoS attack

Description	
The Pirate Bay was down for more than a week due to a DDos (Distributed Denial of Service) attack by malicious actors. The malicious actors caused DDos attack to the site's search engine with specially crafted search queries. The attacker flooded the Pirate Bay with "searches that break the Sphinx search deamon" effectively crashing the torent download website, making site visitors unable to download magnet links or torrent files.	
Source	https://koddos.net/blog/the-pirate-bay-suffers-ddos-attack-for-more-than-a-week/
Recommendation	Wait for the fixings

4. Google Chrome Zero day under active attack

Description	
Two vulnerability - one affecting chrome's audio component while other resides in the PDFium library - is introduced in google chrome web browser which is a class of memory courruption issue that allows corruption or modification of data in the memrry, enabling an unprivileged user to escalate privileges on an affected system or software. Thus both flaw could enable attackers to gain privileges on the chrome web browser just by convincing targeted users into visiting a malicious wevsite, allowing them to escape sandbox protection and run arbitary malicious code on the target systems.	
Source	https://thehackernews.com/2019/11/chrome-zero-day-update.html
Infected Technology	chrome
Recommendation	Patch the update when available
CVE_ID	CVE-2019-13720 CVE_2019-13721

5. Chinese hackers compromise telecom server to spy on SMS message

Description

A group of chinese hacker developed a “MessageTap” the backdoor malware which is a 64-bit ELF data miner designed to spy on text messages sent or received by highly targeted individuals. The malware has been installed on a Linux based Short Message Service Center (SMSC) unnamed telecommunications company. Since SMSes are not designed to be encrypted, neither on transmitting nor on the telecom servers, compromising an SMSC system system allows attackers to monitor all network connections to and from the server as well as data within them.

Source	https://thehackernews.com/2019/10/sms-spying-malware.html
Infected Industry	Telecommunication sector

6. Adware Apps traced information back to developers server

Description

An adware family dubbed as “Ashas” developed apps with the malicious component that connects to a remote command-and-control server operated by the developer and automatically sends basic information about the android device with one of the adware apps installed. The app then receives configuration data from the c&c server responsible for displaying ads as per the attacker's choice and applying a number of tricks for stealth and resilience, some of which are mentioned below. If a user tries to uninstall the malicious app, only the shortcut ends up getting removed while the app continues to run in the background without the user’s knowledge.

Source	https://thehackernews.com/2019/10/42-adware-apps-with-8-million-downloads.html
Infected Technology	Android Smart Phones
Recommendation	Remove the app if installed

7. Microsoft SQL server Backdoor Malware Spotted

Description	

A backdoor was discovered in microsoft sql server which lets remote attackers connect to any account on the server running Mssql versions by using a “magic password”. The malware manages to remain undetected on the victim’s Mssql server by disabling the compromised machine’s logging functions, event publishing, and audit mechanisms every time the “magic passoword” is used. With this capabilities an attacker can copy, modify or delete the content stored in a database.

Source	https://www.zdnet.com/article/researchers-find-stealthy-mssql-server-backdoor-developed-by-chinese-cyberspies/
Infected Technology	MSSQL v12 v11
Recommendation	Apply the available patch when available

8. Android Banking Malware Uses SMS to Hack Users Device

Description	

The Gustuff banking malware uses SMS messages to infect users for stealing login credentials by abusing Accessibility Services in Android devices. The malware sends commands requesting credit card information, but it won’t present a form to enter the details, instead, it leverages the Android Accessibility API to harvest it. It checks or the list of apps installed and blocks the list of anti-virus /anti-malware software present.

Source	https://gbhackers.com/gustuff-banking-malware/
Infected Technology	Android Smart Phones
Recommendation	Apply the available patch provided by google

For any queries/recommendations:

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