InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Critical Bug in Wordpress site
2. Zeppelin Ransomware
3. Plundervolt: New Attack Targets Intel's Overclocking Mechanisms
4. Rooster Teeth Data Breach
5. Snatch Ransomware Reboots Windows in safe mode to Bypass Antivirus

16/12/2019

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, 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. Critical Bug in Wordpress site

Description	
Security experts discovered a critical easy-to-exploit authentication bypass vulnerability in “ultimate Addons for B16/12/2019 eaver Builder,” or “Ultimate Addons for Elementor.”The vulnerability resides in the way the plugins let WordPress account holders, including administrators, authenticate via Facebook and Google login.The flaw could be exploited by remote attackers to gain administrative access to sites without requiring any password.	
Source	https://threatpost.com/critical-bug-in-wordpress-plugins-open-sites-to-hacker-takeovers/151123/
Infected Industry	Ultimate Addons for Elementor version prior or equal to 1.20.0 Ultimate Addons for beaver Builder Version prior or equal to 1.24.0
Recommendation	Install the latest version of plugins, “Ultimate for Elentor version 1.20.1” and “Ultimate for Beaver Beaver Version 1.24.1"

2. Zeppelin Ransomware

Description	
A new form of ransomware called Zeppelin is targeting tech and health companies in a campaign that has security experts worried if it spreads further afield. Zeppelin is a variant on the Vega ransomware family and is being advertised on Russian websites as an attack-as-a-service offering. According to a report by the Cylance Threat Research Team, the ransomware has been designed to have a broad reach and has been detected targeting tech and healthcare companies in Europe and the U.S.	
Source	https://www.bleepingcomputer.com/news/security/zeppelin-ransomware-targets-healthcare-and-it-companies/
Infected Area	Health Care and IT companies

3. Plundervolt: New Attack Targets Intel's Overclocking Mechanisms

Description	
Researchers have discovered a new attack impacting modern Intel CPUs, which could allow an attacker to extract highly-sensitive information – such as encryption keys – from affected processors by altering their voltage. The attack, dubbed "Plundervolt," centers around Intel Software Guard Extensions (SGX), a set of security-related instruction codes that are built into Intel CPUs. Intel SGX shields sensitive data – such as AES encryption keys – inside "enclaves," which are physically separate from other CPU memory and are protected by software encryption.	
Source	https://thehackernews.com/2019/12/intel-sgx-voltage-attack.html
Infected Technology	Intel CPUs
CVE Details	CVE-2019-11157

4. Rooster Teeth Data Breach

Description	
The popular production company Rooster Teeth Productions has suffered a data breach, hackers have stolen credit card and other payment data from users that made purchases on the company's online store. The data breach took place on December 2, and the company discovered the incident the same day. The attackers planted a malicious script into the checkout page of the online store, it was developed to redirect shoppers to a fake payment page under the control of the attackers.	
Source	https://www.bleepingcomputer.com/news/security/attackers-steal-credit-cards-in-rooster-teeth-data-breach/
Infected Industry	Rooster Teeth Production

5. Snatch Ransomware Reboots Windows in safe mode to Bypass Antivirus

Description	
A new variant of the snatch ransomware has been introduced that chooses to run in safe mode. This ransomware first reboots the infected windows computers into safe mode and only then encrypts victims' files to avoid antivirus detection. The snatch ransomware sets itself up as a service called SuperBackupMan with the help of windows registry, that will run during a safe mode. It is also a data stealer as it includes a sophisticated data-stealing module, allowing attackers to steal vast amounts of information from the target organization.	
Source	https://thehackernews.com/2019/12/snatch-ransomware-safe-mode.html
Infected Industry	Windows

For any queries/recommendations:

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