InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. NASA hacked because of Unauthorized Raspberry Pi connected to its network
2. Microsoft Outlook For Android recently patched a Spoofing Vulnerability
3. Remote Users can cause Arbitrary Code Execution on target computers using VLC Media Player v3.0.6 and below
4. New Malware named OSX/Linker can execute untrusted code without warning on infected Apple's Mac based computers
5. Linux based cryptocurrency miners on Windows and macOS systems
6. Nepal 37000+ Email Leakage

30/06/2019

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. NASA hacked because of Unauthorized Raspberry Pi connected to its network

Description	
A light and compact micro-computer named 'raspberry pi' was used to steal data from Nasa's Jet Propulsion Laboratory. An audit report shows that the device managed to steal about 500MB of data. The device was undetected for 10 months. The OIG report blamed the JPL's failure to segment its internal network into smaller segments. The NASA OIG also blamed the JPL for failing to keep the Information Technology Security Database (ITSDB) up to date.	
Source	https://oig.nasa.gov/docs/IG-19-022.pdf
Infected Organization	NASA
Recommendation	Awareness about connected device in your organization is necessary.

2. Microsoft Outlook For Android recently patched a Spoofing Vulnerability

Description	
Outlook app with versions before 3.0.88 for Android contains a stored cross-site scripting vulnerability (CVE-2019-1105) in the way the app parses incoming email messages. If exploited, remote attackers can execute malicious in-app client-side code on the targeted devices just by sending them emails with a specially crafted message.	
Source	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1105
Infected Technology	Android Devices
Recommendation	Apply the patches sent by the vendor

3. Remote Users can cause Arbitrary Code Execution on target computers using VLC Media Player v3.0.6 and below

Description	
VLC media player software versions prior to 3.0.7 contain two high-risk security vulnerabilities, besides many other medium- and low-severity security flaws, that could potentially lead to arbitrary code execution attacks.	
Source	https://www.videolan.org/security/sa1901.html
Infected Technology	VLC installed devices
Recommendation	Apply the patches sent by the vendor

4. New Malware named OSX/Linker can execute untrusted code without warning on infected Apple's Mac based computers

Description	
A possible exploitation of an unpatched security vulnerability in Apple's Gatekeeper security feature were disclosed and found four samples of new macOS malware on VirusTotal that can leverage the GateKeeper bypass. This vulnerability can execute untrusted code on macOS without displaying users without warning.	
Source	https://www.intego.com/mac-security-blog/osx-linker-new-mac-malware-attempts-zero-day-gatekeeper-bypass/
Infected Technology	iMac
Recommendation	Apply the necessary patches and updates provided by the vendor.

5. Linux based cryptocurrency miners on Windows and macOS systems

Description	
Windows and macOS are very common for personal use, business use and windows are also being used as servers by many organizations. The Cryptocurrency miners named "LoudMiner" and "Bird Miner" leverages command-line based virtualization software on target machine to boot Tiny Core Linux OS that has a hacker-activated cryptocurrency mining software in it.	
Source	https://blog.malwarebytes.com/mac/2019/06/new-mac-cryptominer-malwarebytes-detects-as-bird-miner-runs-by-emulating-linux/
Infected Technology	Windows and Mac based systems
Recommendation	Keep an active track of any malware detection.

6. Nepal 37000+ Email Leakage

Description	
Recently, a link was viral of a GitHub where 37000+ Nepali email addresses were leaked. We suspect the leak could have been a database dump from sites of mercantile. People use 'https://register.com.np/ 'to register their domains in Nepal. The possibility is, the largely found emails could have been taken from their database. The attackers have not posted anything about leaked credentials/passwords, and we believe even if the attackers have the passwords, they might have it in a hash format.	
Source	https://gist.github.com/caphilates/f037644e473c36608d8d1e86b987f3dd
Recommendation	Change your passwords as a precaution.

For any queries/recommendations:

Contact us: whois@cryptogennepal.com