InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. 5 High Impact Flaws Affect Cisco Routers, Switches, IP Phones and Cameras
2. Critical Android Bluetooth Bug Enables RCE, No User Interaction Needed
3. Metamorfo Returns with Keylogger Trick to Target Financial Firms
4. U.S. Finance Sector Hit with Targeted Backdoor Campaign
5. Ransomware Exploits GIGABYTE Driver to Kill AV Processes

10/02/2020

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. 5 High Flaws Affect Cisco Technologies

Description
Several Cisco-manufactured network equipments have been found vulnerable to five new security vulnerabilities that could allow hackers to take complete control over them, and subsequently, over the enterprise networks they power.These vulnerabilities reside in the various implementations of the Cisco Discovery Protocol (CDP) that comes enabled by default on virtually all Cisco devices and can not be turned OFF. Four of the five high-severity bugs are remote code execution issues affecting Cisco routers, switches, and IP cameras, whereas the fifth vulnerability is a denial-of-service issue affecting Cisco IP phones.

Source	https://thehackernews.com/2020/02/cisco-cdp-vulnerabilities.html
Infected Technology	Cisco Routers, Switches, IP Phones and Cameras
Recommendation	Install the Latest Software Updates
CVE Details	CVE-2020-3119, CVE-2020-3118, CVE-2020-3111, CVE-2020-3110, CVE-2020-3120

2. Critical Android Blutooth Bug Enables RCE

Description
A critical vulnerability in the Bluetooth implementation on Android devices running Android versions Pie (9.0) and Oreo (8.0, 8.1) was found which could allow attackers to launch remote code execution (RCE) attacks without any user interaction. Remoter Attackers can silently execute arbitrary code with the privileges of Bluetooth daemon. The flaw is particularly dangerous because no user interaction is required and only the Bluetooth MAC address of the target devices has to be known to launch the attack.

Source	https://threatpost.com/critical-android-bluetooth-bug-enables-rce-no-user-interaction-needed/152699/
Infected Industry	Android versions Pie (9.0) and Oreo (8.0, 8.1)
Recommendation	Update the Latest Patch Available
CVE Details	CVE-2020-0022

3. Metamorfo targeting Financial Firm with Keylogger

Description
Metamorfo is a malware family that was targeting the customers of online financial institutions. It was found that it adds a new technique which targets payment-card data and credentials at financial institutions with Windows platforms. Once executed, the malware kills the auto-suggest data entry fields in browsers, forcing victims to write out their passwords – which it then tracks via a keylogger. This is first spread via phishing emails that distribute a ZIP archive containing an MSI file (named "view-(AVISO)2020.msi"). Once executed it terminates running browsers and then modifies various registry keys to disable Internet Explorers' functions, like auto-complete and auto-suggest.

Source	https://threatpost.com/metamorfo-variant-keylogger-financial/152640/
Infected Technology	Windows

4. U.S. Finance Sector Hit with Backdoor Campaign

Description	
The Backdoor campaign was initiated via phishing emails with attached documents containing malicious macros. The attached phishing documents used the “VBA Stomping” tactic to hide their malicious macros. If the document is “detonated” and the malicious macros are executed, the code fetches a ZIP file containing legitimate files required to execute an older copy of Microsoft TeamViewer, which is then renamed to “wpvnetwks.exe.” This malicious TeamViewer instance then side-loads a DLL containing the Minebridge backdoor.The ultimate goal of the document is to infect victims with the Minebridge backdoor. It’s a powerful piece of malware that gives attackers full control of the target environment including downloading and executing other malware, downloading arbitrary files, self-deletion and many more.	
Source	https://threatpost.com/us-finance-sector-targeted-backdoor-campaign/152634/
Infected Technology	Finance Sector

5. Ransomware Exploits GIGABYTE Driver to kill AV Processes

Description	
The attackers behind the RobbinHood Ransomware were found exploiting a vulnerable GIGABYTE driver to install a malicious and unsigned driver into Windows that is used to terminate antivirus and security software. The RobbinHood Ransomware are utilizing a custom antivirus killing package that is pushed out to workstations to prepare it for encryption. The criminals used the Gigabyte driver as a wedge so they could load a second, unsigned driver into Windows.This second driver then goes to great lengths to kill processes and files belonging to endpoint security products, bypassing tamper protection, to enable the ransomware to attack without interference.	
Source	https://www.bleepingcomputer.com/news/security/ransomware-exploits-gigabyte-driver-to-kill-av-processes/
Infected Technology	Windows

For any queries/recommendations:

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