April 20, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- 49 Google extensions were found caught Hijacking CryptoCurreny Wallets
- Sensitive information disclosure vulnerability in the VMware Directory Service
- Fake Coronavirus apps hit android and iOS users with spyware
- Nemty Ransomware goes private with RaaS (Ransomware-as-a-Service)
- Linksys router users forced to reset their passwords

and more...

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, Trip Advisor, 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. Sensitive information disclosure vulnerability in the VMware Directory Service

Description	
A sensitive information disclosure vulnerability in the VMware Directory Service (vmdir) was privately reported to VMware. vCenter updates are available to address this vulnerability. Under certain conditions[1] vmdir that ships with VMware vCenter Server, as part of an embedded or external Platform Services Controller (PSC), does not correctly implement access controls. VMware has evaluated the severity of this issue to be in the Critical severity range with a maximum CVSSv3 base score of 10.0.	
Source	https://www.vmware.com/security/advisories/VMSA-2020-0006.html
Infected Technology	VMware
Recommendation	To remediate apply the updates listed in the 'Fixed Version' column of the 'Response Matrix' below to affected deployments.
CVE-ID	CVE-2020-3952

2. Chrome extensions caught hijacking Cryptocurrency wallets

Description	
49 Google chrome extensions were discovered to be posing as legitimate cryptocurrency wallet but contained malicious code to steal private keys, mnemonic phrase and other secrets. Chrome has removed these extensions once identified. The extensions appeared on web store since February 2020 and impacted known wallets like Ledger, Electrum, Exodus, etc.	
Source	https://www.zdnet.com/article/exclusive-google-removes-49-chrome-extensions-caught-stealing-crypto-wallet-keys/
Infected Technology	Google Chrome
Recommendation	Verify authors to identify legitimate extensions

3. Fake Corona Virus Apps hits Android and iOS user

Description	
Cybercriminals are attempting each stunt at their disposal to profit by the Coronavirus pandemic and the resulting turmoil it has produced. The most recent snare they have laid to deceive clients is by discharging malevolent spying applications masked as COVID-19 updates and data applications. As per cybersecurity researcher evaluation, through Project Spy, the assailants are contaminating Android and iOS gadgets with spyware circulated through applications titled Coronavirus Updates, Wabi Music, Concipit 1248 and Concipit Shop. These applications can play out an assortment of capacities including moving information from Telegram, WhatsApp, Threema, and Facebook messages which collects voice notes, call logs, sensitive information about device and SIM information.	
Source	https://www.hackread.com/fake-coronavirus-apps-android-ios-users-spyware-adware/
Infected Technology	Android Devices and iOS
Recommendation	Do not download app from untrusted source

4. Trickbot in different COVID-19 lures per week

Description	
TrickBot is, now, the malware showing up in the highest number of unique COVID-19 related malicious emails and attachments delivered to potential victims' inboxes based on Microsoft's Office 365 Advanced Threat Protection (ATP) data. Microsoft has stated that over 60,000 attacks out of millions of targeted messages come with COVID-19 related malicious attachments or URLs through phishing campaigns.	
Source	https://www.bleepingcomputer.com/news/security/microsoft-trickbot-in-hundreds-of-unique-covid-19-lures-per-week/
Infected Medium	Weak phishing detection technology; Lack of User awareness; Incorrect implementation of host-based firewalls
Recommendation	Do not click on links you are not aware of; Update your system to the latest patch; Ensure your host firewalls are enabled

5. Mass attack on Linksys Routers resulted with password reset	
Description	
Attackers targeted home Linksys routers to change setting and redirect web traffics to malicious Coronavirus themed landing pages. Once identified, Linksys reset the password of its Linksys Smart Wi-Fi application to prevent escalation of these attacks. Attackers were able to access over 1200 accounts by credential stuffing attack before the researchers reset the credentials of the users.	
Source	https://threatpost.com/attacks-on-linksys-routers-trigger-mass-password-reset/154914/
Infected Technology	Linksys Router
Recommendation	Use of stronger password with Alphanumeric keywords

6. Nemty Ransomware goes private with RaaS (Ransomware-as-a-Service)	
Description	
Operators behind Nemty ransomware are shutting down their open Ransomware-as-a-Service (RaaS) activity and changing to a private activity. Nemty is a great Ransomware-as-a-Service plan of action that has been in activity since the late spring of 2019. It gave clients who joined to the administration an entrance to a web-based interface where they can make their own variant of Nemty ransomware and pick their own technique for dissemination, for example, email spam, misuse units, or by animal constraining RDP endpoints. When distributors got a payoff ransom, they got the chance to keep 70% of the sum, while the staying 30% went to RaaS administrators. In an ongoing declaration on a Russian programmer gathering the Nemty administrator said they were shutting their RaaS activity to people in general and "going private." Victims have been given seven days to pay for decryptors before all servers would be closed down.	
Source	https://www.bleepingcomputer.com/news/security/nemty-ransomware-shuts-down-public-raas-operation-goes-private/
Recommendation	Do not click on links you are not aware of; Update your system to the latest patch; Ensure your host firewalls are enabled

7. GitHub accounts stolen in ongoing phishing attacks

Description	
GitHub's SIRT published information on this ongoing phishing campaign dubbed *Sawfish* to increase awareness and allow users that might be targeted to protect their accounts and repositories. The phishing emails use various lures to trick targets into clicking the malicious link embedded in the messages: some say that unauthorized activity was detected, while others mention repository or settings changes to the targeted user's account.	
Source	https://www.bleepingcomputer.com/news/security/github-accounts-stolen-in-ongoing-phishing-attacks/
Infected Technology	GitHub
Recommendation	Reset password & 2FA recovery codes. Be aware of the URLs before entering your passwords

8. Slack Phishing Attacks using webhooks

Description	
Slack is a cloud-based messaging platform that is commonly used in workplace communications. Slack Incoming Webhooks allow you to post messages from your applications to Slack. By specifying a unique URL, your message body, and a destination channel, you can send a message to any webhook that you know the URL for in any workspace, regardless of membership. Using this technique, the attacker could then steal private information from the Slack users that download the harmful app. Alien Labs researchers discovered some 130,989 Slack webhook URLs available online, with the majority containing the full information needed to carry out the phishing attack. The researchers also claim that compromising a Slack webhook can give the attacker the **ability to alter channel posting permissions,** allowing them to push out the malicious app to multiple channels.	
Source	https://cybersecurity.att.com/blogs/labs-research/slack-phishing-attacks-using-webhooks
Infected Technology	Slack
Recommendation	Only allow apps to be installed from Slack's app directory.

9. Microsoft Issus Patches for 3 Zero-day bugs

Description	
Microsoft released patch for 113 vulnerabilities along with 3 identified as zero-day vulnerabilities. The zero-day vulnerabilities resided in Adobe Font Manager Library, Adobe Type Manager Library and Windows kernel which allowed remote code execution and privilege escalation in Windows 10, 8.1 as well as Windows Server 2008-2019. Other 14 patch released alongside were identifies as critical while rest 96 were marked important in severity.	
Source	https://thehackernews.com/2020/04/windows-patch-update.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.2207.qx0a00e50w.1dsu
Infected Technology	Windows Operating System
Recommendation	Apply the update released by Microsoft

10. U.S. offering rewards for information on North Korea Hackers

Description	
U.S. States agency released a joint advisory warning cyber threat posed by North Korean state-sponsored hackers to global banking and financial institutions. The advisory states that U.S. government is now offering monetary reward of up to $5 million to who share information regarding illicit North Korea's activities in cyberspace.	
Source	https://thehackernews.com/2020/04/north-korea-hackers.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.2207.qx0a00e50w.1dsi

11. 700 Malicious Typosquatted Libraries found on RubyGems Repository	
Description	
As Developers progressively grasp off-the-rack programming segments into their applications and administrations, danger on-screen characters are manhandling open-source archives, for example, Ruby Gems to appropriate pernicious bundles, planned to bargain their PCs or secondary passage programming ventures they take a shot at. In the most recent research, cybersecurity specialists at Reversing Labs uncovered more than 700 pernicious jewels — bundles written in Ruby programming language — that production network assailants were gotten as of late circulating through the Ruby Gems repository. The vindictive battle utilized the typosquatting procedure where aggressors transferred purposefully incorrectly spelled genuine bundles with the expectation that accidental engineers will mistype the name and unintentionally install the malicious library.	
Source	https://thehackernews.com/2020/04/rubygem-typosquatting-malware.html
Infected Medium	Ruby Gems Repository
Recommendation	Recommended to check if downloaded package is correct or typosquatted version

For any queries/recommendations:

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