April 27, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- Microsoft Teams Triggered account Hijacking bug
- Hackers are exploiting Sophos firewall zero-day
- Cyber Criminals scams Three UK PE Firms in $1.3 million heist
- Nintendo confirms breach of 1,60,000
- Facebook Dark Web Deal: 267 Million user details for $600
- Zero-day vulnerability opens iPhone and iPad to Remote Code Execution
- Skype Phishing Attack targets remote workers passwords
- Crypto-mining Botnet infects more than 35,000 Windows system

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. Microsoft Teams Triggered account Hijacking bug

Description	
Microsoft has resolved security issues in Microsoft Teams that could have been utilized in an attack chain to take over user accounts - all with the assistance of a .GIF file. Cybersecurity researcher said a subdomain takeover vulnerability, joined with a malicious .GIF document, could be utilized to "scratch a user's information and at last assume take over an association's whole list of Teams accounts." The attacker could access all the data from your organization Teams accounts, gathering confidential information, competitive data, secrets, passwords, private information, business plans.	
Source	https://www.bleepingcomputer.com/news/security/microsoft-teams-patched-against-image-based-account-takeover/
Infected Technology	Microsoft Teams
Recommendation	Update Latest Patch Released by Microsoft

2. Hackers are exploiting Sophos firewall zero-day

Description	
A zero-day SQL injection vulnerability is being exploited by attackers to gain access to Sophos XG devices. Attackers are using the vulnerability to download a payload which stole files including username and hashed password used to login to the firewall. Sophos identified the issue on April 22 and has published an emergency patch on April 25th and pushed a hotfix to devices with automatic updates enabled.	
Source	https://www.zdnet.com/article/hackers-are-exploiting-a-sophos-firewall-zero-day/
Infected Technology	Sophos XG firewall
Recommendation	Ensure the update released by the OEM is released

3. Cyber Criminals scams Three UK PE Firms in $1.3 million heist

Description

Three British private equity firms were duped into making bank transfers worth £1.1 million (around US$1.3 million) following a sophisticated Business Email Compromise (BEC) attack. Check Point's Incident Response Team (CPIRT) discovered a hacker group dubbed "The Florentine Banker," which targeted three unnamed firms for several months via phishing attacks, using fake emails and look-alike domains. It is said that hackers made four separate bank transactions, in December 2019, to transfer £1.1 million to fraudulent bank accounts in Hong Kong and the U.K. An emergency intervention allowed banks to salvage £570,000 (US$702,067), the rest of the money lost permanently.

Source	https://thehackernews.com/2020/04/bec-scam-wire-transfer-money.html
Recommendation	• Enable multi-factor authentication for all email accounts. • Verify all payment changes and transactions in person or via a known telephone number. • User awareness about BEC scams

4. Nintendo confirms breach of 1,60,000

Description

Nintendo has confirmed over 160,000 user account has been compromised due to attack in a legacy login system. The attack started since the beginning of the April that abused Nintendo Network ID (NNID). Various gamers reported unauthorized logins and purchases via their account before Nintendo released the news regarding the breach. Nintendo has now restricted login via NNID.

Source	https://threatpost.com/nintendo-confirms-breach-of-160000-accounts/155110/
Infected Technology	Nintendo
Recommendation	Change the credential for the system

5. Facebook Dark Web Deal: 267 Million user details For $600

Description

Security researcher discovered 267 million Facebook profiles being sold on dark web sites and hacker forums for over $600 apiece. Researcher uncovered the stolen account credentials for sale last month. However, none of the records include passwords, instead containing information that could allow attackers to conduct spear-phishing or SMS attacks. Researcher found an open Elasticsearch database that contained the records, most of which included information on US users. The records included a full name, phone number, and a unique Facebook ID. The database has since been taken offline by the ISP hosting it after they were contacted by Researcher. However, a new server containing the same data plus an additional 42 million records was found and promptly attacked by threat actors who left a message warning owner to secure their servers.

Source	https://www.bleepingcomputer.com/news/security/267-million-facebook-profiles-sold-for-600-on-the-dark-web/
Recommendation	Tighten their privacy settings on Facebook accounts and be cautious of unsolicited emails and text messages.

6. Zero-day vulnerability opens iPhone and iPad to Remote Code Execution

Description

Two critical zero-day flaw in Apple's default mailing application. The vulnerability allows attackers to gain control over the device just by sending an email. One of the vulnerabilities can be exploited without any interaction of the victim. The vulnerabilities existed in the application since last 8 years since release of iOS 6 and is still vulnerable with no patch available. The vulnerability is being exploited in the wild at least for two years to spy on high-profile victims.

Source	https://thehackernews.com/2020/04/zero-day-warning-its-possible-to-hack.html
Infected Technology	iPhone and iPad (since iOS 6)
Recommendation	Avoid using the default Mail application by Apple (use alternative application instead) Apply the update once it is available.

7. Skype Phishing Attack targets remote workers passwords

Description

Attackers have deployed a phishing campaign against remote workers using Skype, luring them with emails that fake notifications from the service. The social engineering in this campaign is refined enough to make victims access the fraudulent login page and provide their credentials.

Source	https://threatpost.com/skype-phishing-attack-targets-remote-workers-passwords/155068/
Infected Technology	Skype
Recommendation	Always be wary when giving off sensitive personal or account information.

8. Crypto-mining Botnet infects more than 35,000 Windows system

Description

Researchers from ESET took down portion of a malware botnet used to mine Monero cryptocurrency. The botnet, named "VictoryGate", had compromised at least 35,000 Windows system and been active since May 2019. The botnet propagates between victims via removable devices and installs malicious payload into the system once connected. The researchers at ESET identified and took done Command and Control server of the botnet that is used to monitor the Botnet's activity.

Source	https://thehackernews.com/2020/04/usb-drive-botnet-malware.html
Infected Medium	USB Devices
Recommendation	Do not connect untrusted devices to your system Use anti-malware software in critical devices

For any queries/recommendations:

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