March 30, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- Hackers Hijack Router's DNS to spread malicious COVID-19 APP
- Critical RCE BUGS Affects millions of OpenWRT
- Bypassed 2FA for Various bank using TrickBot App
- Hackers use news site to install spyware on iPhones
- WordPress Malware distributed via corona virus plugin
- Targeted attacks on Citrix, cisco and Zoho appliances rise

CryptoGen Nepal

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. Hackers Hijack Router's DNS to spread malicious COVID 19 App

Description
The attackers are changing DNS settings on Linksys routers to redirect users to a malicious website promising an informative COVID-19 app. A recently discovered campaign that targets home and small-office routers is redirecting users to fake COVID-19 informational sites that attempt to install password stealing malware.

Source	https://labs.bitdefender.com/2020/03/new-router-dns-hijacking-attacks-abuse-bitbucket-to-host-infostealer/
Infected Technology	Linksys Router
Recommendation	• Change the routers control panel access credentials. • users should change their Linksys cloud account credentials, or any remote management account for their routers • Router firmware to be up to date

2. Critical RCE Bugs Affects millions of OpenWrt-based Network devices

Description
Security researcher uncovered a critical remote code execution vulnerability in OpenWrt operating system that allows attackers to inject the malicious payload on the vulnerable systems. The flaw is a critical remote code execution vulnerability affecting the operating system, which is a widely used Linux-based operating system for network devices such as routers and residential gateways. The vulnerability exists in the OPKG package manager of OpenWrt, it is related to the way it performs integrity checking of downloaded packages using the SHA-256 checksums that are embedded in the signed repository index.

Source	https://thehackernews.com/2020/03/openwrt-rce-vulnerability.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.2194.qx0a00e50w.1dh4
Infected Technology	• OpenWrt versions 18.06.0 to 18.06.6 and 19.07.0
Recommendation	To upgrade their device firmware to the latest OpenWrt versions 18.06.7 and 19.07.1
CVE_ID	CVE-2020-7982

3. TrickBot uses a malicious Android app to bypass 2FA by various bank

Description	
The operators of the TrickBot banking malware have developed an Android app that can bypass some of the two-factor authentication (2FA) solutions employed by banks. This Android app, which security researchers from IBM have named TrickMo, works by intercepting one-time (OTP) codes banks send to users via SMS or push notifications. TrickMo collects and then sends the codes to the TrickBot gang's backend servers, allowing the crooks to bypass logins or authorize fraudulent transactions.	
Source	https://thehackernews.com/2020/03/trickbot-two-factor-mobile-malware.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.2194.qx0a00e50w.1dgy
Infected Technology	Android
Recommendation	Do not install application from unknown source

4. Hackers use news site to install spyware in iPhones

Description	
A newly discovered attack in Hong Kong targets iPhone users by infecting website visitors with custom spyware. The code dubbed as “TwoSail Junk” targets vulnerabilities in iOS version 12.1 and 12.2. The attack uses malicious website links to lure visitor with targeted content which infects user with malware with the help of background code in the malicious website	
Source	https://threatpost.com/emerging-apt-mounts-mass-iphone-surveillance-campaign/154192/
Infected Technology	iPhone (iOS version 12.1 and 12.2)
Recommendation	Update to the latest iOS version

5. WordPress Malware distributed via corona virus plugin

Description	
The attackers behind WP-VCD, a family of WordPress infection, have started distributing pirated version of Corona virus plugin named, "COVID-19 Coronavirus - Live Map WordPress Plugin" which creates a backdoor in a website. These sites are then used to attacks various websites in same shared host or display pop-ups and redirect traffic to other malicious/revenue generating websites.	
Source	https://www.bleepingcomputer.com/news/security/wordpress-malware-distributed-via-pirated-coronavirus-plugins/
Infected Technology	WordPress
Recommendation	Do not use pirated version of WordPress plugins

6. Targeted attacks on Citrix, Cisco and Zoho appliances rises

Description	
According to recent research done by FireEye, Chinese hacking group APT41 was found launching targeted attacks on Cisco, Citrix and Zoho appliance across but not limited to US, the UK, France, Italy, Japan, Saudi Arabia, and Switzerland. These attacks use multiple vulnerabilities in the devices to execute arbitrary code on system/root.	
Source	https://www.bleepingcomputer.com/news/security/chinese-hackers-use-cisco-citrix-zoho-exploits-in-targeted-attacks/
Infected Technology	Cisco, Citrix, Zoho
Recommendation	• Update the systems to the latest version

For any queries/recommendations:

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