April 13, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- Dark Nexus: A New Emerging IoT Botnet Malware
- Android Malware Keeps returning even after factory reset
- Thousands of Zoom credentials available on the dark web
- New wiper malware impersonates security researchers as prank
- San Fran Airport website hacked

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. Dark Nexuxs: A New Emerging IoT Botnet Malware

Description	
Cybersecurity researcher have found another developing IoT botnet risk that use traded off shrewd gadgets to dispatch 'circulated disavowal of-administration' assaults, possibly activated on-request through stages offering DDoS-for-employ administrations. The botnet works by utilizing accreditation stuffing assaults against an assortment of gadgets, for example, switches (from Dasan Zhone, Dlink, and ASUS), video recorders, and warm cameras, to co-pick them into the botnet	
Source	https://www.bitdefender.com/files/News/CaseStudies/study/319/Bitdefender-PR-Whitepaper-DarkNexus-creat4349-en-EN-interactive.pdf
Infected Company	Dasan Zhone, Dlink, and ASUS

2. Android Malware Keeps Returning Even After Factory Reset

Description	
Cybersecurity firm revealed a form of Android malware that keeps returning even after performing a factory reset on a smartphone. Malwarebytes discovered the Android trojan named the xHelper in May 2019. The malware can install itself on an Android device without notifying the owner, then receives remote commands and downloads additional malware into the infected smartphone or tablet. Unfortunately, it appears that xHelper is still evolving. An Android device owner reached out to the Malwarebytes support forum to seek help for a Curious case. They were able to remove two variants of xHelper and a trojan agent from their Android device through Malwarebytes' app. However, xHelper kept coming back less than an hour after it was removed, even after they performed a factory reset on her phone.	
Source	https://securelist.com/unkillable-xhelper-and-a-trojan-matryoshka/96487/
Infected Technology	Android
Recommendation	Re-flashed their Backdoored phones

3. Thousands of Zoom credentials available on the dark web

Description	
Researchers discovered a database available on an underground forum in the dark web that contained more than 2,300 compromised Zoom credentials. The leaked credentials are supposed to contain meeting IDs, names and host keys. The credentials seem to be associated with zoom accounts belonging to organization in various industries, including banks, consultancy firms, software companies and healthcare.	
Source	https://securityaffairs.co/wordpress/101475/deep-web/zoom-dark-web.html
Infected Technology	Android Devices
Recommendation	Change your password on zoom and any other web sites that you may have reused the same password

4. New wiper malware impersonates security researchers as prank

Description	
There seems to be an ongoing prank by locking victim's computers before they can start Windows and then blaming the infection on two well-known security researchers. After downloading and installing software from what appears to be free software and crack sites, people suddenly find that they are locked out of their computer before Windows starts. These infections are called MBRLockers as they replace the 'master boot record' of a computer so that it prevents the operating system from starting and displays a ransom note or another message instead.	
Source	https://www.bleepingcomputer.com/news/security/new-wiper-malware-impersonates-security-researchers-as-prank/
Infected Technology	Windows PC
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. San Fran Airport websites Hacked

Description	
In March hackers compromised two websites of San Francisco International Airport (SFO) and now it disclosed a data breach. SFO is a major gateway to Europe and Asia, it serves 45 international carriers. The attackers may have gained access to some users' login credentials after deploying malware on both websites. The attackers inserted malicious computer code on these websites to steal some users' login credentials, reads a message posted to both sites by the SFO's Airport Information Technology and Telecommunications (ITT) director. Users possibly impacted by this attack include those accessing these websites from outside the airport network through Internet Explorer on a Windows-based personal device or a device not maintained by SFO. Hackers may have accessed the impacted users' credentials and used them to log on to those personal devices. The SFO ITT urges anyone who even visited either website using the Internet Explorer web browser to change the device's password.	
Source	https://www.scmagazine.com/home/security-news/cybercrime/san-francisco-airport-websites-compromised-to-swipe-credentials/
Infected Technology	SFO Websites
Recommendation	Log and Monitor organizational traffic;

For any queries/recommendations:

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