August 3, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- Industrial VPN Flaws could Let Attackers Target Critical Infrastructure
- Phishing Email to Steal Microsoft Credentials
- Undetectable Linux Malware Targeting Docker Servers With Exposed APIs
- Qsnatch Data-stealing Malware infected QNAP NAS devices
- Bypassing Windows 10 UAC with mock folders and DLL hijacking
- New Attack Leverages HTTP/2 for Effective Remote Timing Side-Channel Leaks
- GRUB2 Bootloader affecting Millions of Linux and Windows Systems

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. Industrial VPN Flaws could Let Attackers Target Critical Infrastructure

Description	
Cyber Security Researcher Disclosed critical vulnerabilities in industrial VPN implementations primarily used to provide remote access to operational technology (OT) networks that could allow hackers to overwrite data, execute malicious code, and compromise industrial control systems (ICS). These vulnerable products are widely used in field-based industries such as oil and gas, water utilities, and electric utilities to remote access, maintain and monitor ICS and field devices, including programmable logic controller (PLCs) and input/output devices. Attacker tricks the victims into visiting malicious website or opening a malicious element that triggers the flaw in ecatcher, eventually allowing attackers to take complete control of the targeted machine.	
Source	https://thehackernews.com/2020/07/industrial-vpn-security.html?m=1
Infected Technology	Secoma Gate Manager M2M Server, Moxa EDR-G902 and EDR-G903, and HMS Network eWon's ecathcher VPN client
Recommendation	All three vendors are strongly recommended to patch the update provided by vendors
CVE_ID	CVE-2020-14500, CVE-2020-14511, CVE-2020-14498

2. Phishing Email to Steal Microsoft Credentials

Description	
A new phishing campaign that tries to steal user's office 365 login credentials by tricking them into accepting a new Terms of Use and privacy has been discovered by researchers at the Cofense Phishing Defense Center (PDC). This campaign has been observed across multiple organizations and employs a number of advanced techniques, including a Google Ad services redirect, to try and steal employees login Credentials.	
Source	https://www.tripwire.com/state-of-security/security-data-protection/phishing-email-uses-google-ad-redirect-to-steal-microsoft-credentials/?web_view=true
Recommendation	• Check the source of information from incoming email • Enter your Sensitive data in Secure website only

3. Undetectable Linux Malware Targeting Docker Servers With Exposed APIs

Description	
An undetectable Linux Malware was uncovered by security researchers which exploits undocumented techniques to stay under the radar and targets publly accessible Docker servers hosted with popular cloud platforms, including AWS, Azure, ad Alibaba Cloud. There is an ongoing Ngrok mining botnet campaign that scans the internet for misconfigured Docker API endpoints which has already infected many vulnerable servers with new malware.	
Source	https://thehackernews.com/2020/07/docker-linux-malware.html?m=1
Infected Technology	Docker Server
Recommendation	• Do not expose docker APIs to the internet • Make sure that Docker APIs is reachable from trusted network or VPN to control your Docker daemon. • Must be careful with parameter checking.

4. Qsnatch Data-stealing Malware infected QNAP NAS devices

Description	
The U.S. CISA and the U. K's NCSC are investigating a data-stealing malware dubbed "QSnatch," which is targeting Network Attached Storage (NAS) devices manufactured by QNAP. The agencies stated that the number of QNAP NAS devices infected with the Qsnatch malware has reached 62,000 across the globe, of which 7,600 were in the U.S. and 3,900 in the U.K. Once a device is infected with QSnatch malware, it enables hackers to prevent administrators from installing firmware updates by modifying the system's host file, redirecting core domain name used by the NAS to local out-of-date versions.	
Source	https://thehackernews.com/2020/07/qnap-nas-malware-attack.html?m=1
Infected Technology	QNAP NAS devices
Recommendation	• Update QTS to the latest available version. • Install and update Malware Remover to the latest version. • Install and update Security Counselor to the latest version. • Update your installed QTS application to the latest versions if available to app center.

5. Bypassing Windows 10 UAC with mock folders and DLL hijacking

Description	
A new technique comes into highlight in which an attacker uses a simplifies process of DLL hijacking and mock directories to bypass Windows 10's UAC security feature and run elevated commands without alerting an user. Windows UAC is a protection mechanism which asks the user to confirm if they wish to run a high-risk application before it is executed.	
Source	https://www.bleepingcomputer.com/news/security/bypassing-windows-10-uac-with-mock-folders-and-dll-hijacking/?&web_view=true
Infected Technology	Windows 10

6. New Attack Leverages HTTP/2 for Effective Remote Timing Side-Channel Leaks

Description	
Security researchers has identified a new technique leading to remote timing-based side-channel attack. Unlike the traditional timing-based attack, the newly identified technique attempts to extract information from the order and the relative timing difference between two concurrently executed requests without relying on any timing information. For a successful execution, the bad actor initiates a pair of HTTP/2 requests to victim server either directly or tricking the victim into visiting attacker-controlled web page – to launch request via JavaScript Code. The successful attack can be used to leak information.	
Source	https://thehackernews.com/2020/07/http2-timing-side-channel-attacks.html?m=1
Infected Methodology	Remote Timing Side-Channel Leakage
Recommendation	Enable constant execution time

7. GRUB2 Bootloader affecting Millions of Linux and Windows Systems

Description	
Researcher from Eclypsium have disclosed detail of high-risk vulnerability, known as BootHole affecting billions of devices including servers and devices running any Linux and Windows System. The vulnerability resides in GRUB2 bootloader. Success exploitation could allow attacker to bypass Secure Boot feature and gain high-privileged persistent and stealthy access to the targeted systems. The vulnerability is a buffer overflow vulnerability and is caused due to the way GRUB2 parses content from the config file. According to the researchers applying the patch alone is not enough to resolve the issue. Permanent resolve would require new bootloaders to be signed and deployed and existing vulnerable bootloader should be revoked.	
Source	
Infected Technology	GRUB-2
Source	https://eclypsium.com/wp-content/uploads/2020/07/Theres-a-Hole-in-the-Boot.pdf
Recommendation	• Apply the patch released • Revoke the existing vulnerable bootloader
CVEs	CVE-2020-10713

For any queries/recommendations:

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