July 27, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- New 'Meow' attack has deleted almost 4000 unsecured databases
- US govt confirms active exploitation of F5 Big-IP RCE Flaw
- New cryptojacking botnet uses SMB exploit to spread to Windows systems
- Cisco patches ASA/FTD firewall flaw actively exploited by hackers
- New security flaw affecting China's DJI Drones revealed
- 5 severe D-Link router vulnerabilities disclosed
- Lazarus hackers deploy ransomware
- Twitter hackers read private messages of 36 high-profile account

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. New 'Meow' attack has deleted almost 4000 unsecured databases

Description	
An automated Attack 'meow' that destroy data without any explanation exposed hundreds of unsecured databases. The activity started recently by hitting Elasticsearch and MongoDB instances without leaving any explanation, or even a ransom note. Attacks then expanded to other database types and to file systems open on the web. The IoT Search engine Shodan initially found dozens of databases that have been affected by this attack- researched by Bleeping Computer. These attacks have pushed researchers into race to find the exposed databases and report them responsibly before they become 'meowed'.	
Source	https://cert.bournemouth.ac.uk/new-meow-attack-has-deleted-almost-4000-unsecured-databases/
Infected Technology	Elastic Search DB, Mongo DB, Cassandra, Couch DB, FTP(NAS), Redis, Hadoop, Jenkins
Recommendation	Administrator Should make sure that they expose only what needs to be exposed and make sure the assets are properly secured.

2. US govt confirms active exploitation of F5 Big-IP RCE Flaw

Description	
The US CISA published a warning confirming the active exploitation of unauthenticated remote code execution (RCE) vulnerability affecting F5 Big-IP ADC devices. CISA provides mitigations and detection measures to help victims find out if their systems may be compromised and recover after attacks that successfully exploited unpatched F5 devices.	
Source	
Infected Technology	F5 Big-IP ADC
Source	https://www.bleepingcomputer.com/news/security/us-govt-confirms-active-exploitation-of-f5-big-ip-rce-flaw/
Recommendation	• Reimaging compromised hosts • Provisioning new account credentials • Limiting access to the management interface to the fullest extent possible • Implementing network segmentation • Update the latest patch available
CVEs	CVE-2020-5902

3. New cryptojacking botnet uses SMB exploit to spread to Windows systems

Description	
A new cryptojacking botnet is spreading across compromised networks via multiple methods that include the EternalBlue exploit for Windows Server Message Block (SMB) communication protocol. The new botnet Prometei and determined that the actor has been active since March. They tagged the attacks as a complex campaign that relies on multi-modular malware. The researchers noticed that its modules fall into two categories that have fairly distinct purposes: mining-related operations (dropping the miner, spreading on the network) and gaining access by brute-forcing logins using SMB and RDP.	
Source	https://us-cert.cisa.gov/ncas/alerts/aa20-206a
Infected Technology	Windows Server
Recommendation	Disable SMB and RDP

4. Cisco patches ASA/FTD firewall flaw actively exploited by hackers

Description	
A read-only path traversal vulnerability in web service interface of two of the Cisco's firewall devices are being actively exploited by attackers. The vulnerability, addressed by CVE-2020-3452, allows unauthenticated attacker to read sensitive file stored in webs services file system. The impacted software are Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software. While the patch for the vulnerability has been released by Cisco, a publicly available exploit and NMAP script has been released with active exploitation of the affected devices. The patch has only been applied by 10% of the affected devices until the weekend as per Rapid7.	
Source	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ro-path-KJuQhB86
Infected Technology	• Cisco Adaptive Security Appliance (ASA) Software • Cisco Firepower Threat Defense (FTD) Software
CVEs	CVE-2020-3452
Recommendation	Update the patch released by Cisco

5. New security flaw affecting China's DJI Drones revealed

Description	
Researchers from *Synacktiv* and *GRIMM* identified a flaw in Android application, DJI's Go 4, developed by Chinese drone-maker Da Jiang Innovations (DJI). The application asks for wide range of phone permission and makes use of anti-bug and encryption to bypass security analysis. The application contains a URL that is used to download an application update, bypassing the official Play Store, and prompts user to allow "*Install Unknown Apps*" permission. The permission includes but is not limited to IMEI and IMSI number, carrier name, SIM Serial Number, Mac address, BSSID, OS language and kernel version.	
Source	https://blog.grimm-co.com/2020/07/dji-privacy-analysis-validation.html
Infected Technology	DJI's Go 4
Recommendation	Verify necessary permission before installing application Do not install application requesting unnecessary permissions

6. 5 severe D-Link router vulnerabilities disclosed

Description	
Ace Team of Loginsoft Pvt. Ltd. has released 5 new severe vulnerability in various products, some of which has reached end-of-life. The vulnerabilities include XSS, buffer overflow leading to obtaining of admin credentials, bypassing authentication and executing arbitrary code. The vulnerability can not only be exploited in local network but also remotely when remote management is enabled. The PoC for the vulnerability has been released, making the devices more vulnerable to the attack. Some of the vulnerability can be exploited easily by changing the parameters in the URL making it act as a backdoor.	
Source	https://www.bleepingcomputer.com/news/security/5-severe-d-link-router-vulnerabilities-disclosed-patch-now/
Infected Technology	DAP-1520 v1.10B04 & Below DAP-1522 v1.42 & Below DIR-816L v12.06.B09 & Below
CVEs	CVE-2020-15896, CVE-2020-15894, CVE-2020-15893, CCVE-2020-15892, CVE-2020-15895
Recommendation	Update the patch released for affected device Replace the device reaching End of Support/End of Life

7. Lazarus hackers deploy ransomware

Description	
Lazarus Group, the notorious hacking group with ties to the North Korean regime, has unleashed a new multi-platform malware framework with an aim to infiltrate corporate entities around the world, steal customer databases, and distribute ransomware. Among the targeted countries, security researchers who spotted MATA mentioned Poland, Germany, Turkey, Korea, Japan, and India. Lazarus used MATA to compromise and infect machines of companies with activities in various industries, including but not limited to a software development company, an internet service provider, and an e-commerce company.	
Source	https://www.bleepingcomputer.com/news/security/lazarus-hackers-deploy-ransomware-steal-data-using-mata-malware/
Infected Areas	Software Development Companies, ISPs, E-commerce

8. Twitter hackers read private messages of 36 high-profile account

Description	
Twitter admitted that the attackers behind last week's incident read the private message of 36 out of a total of 130 high-profile accounts targeted in the attack. An elected official in the Netherlands was one of those whose DMs were compromised, the company tweeted as part of Twitter's interest in sharing 'more specifics about what the attackers did with the accounts they accessed.	
Source	https://www.bbc.com/news/technology-53510574#:~:text=Twitter%20has%20revealed%20that%20hackers,elected%20official%20in%20the%20Netherland
Infected Technology	Twitter
Recommendation	Twitter needs to follow end-to-end encryption suit.

For any queries/recommendations:

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