August 31, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- QakBot Banking Trojan with sneaky tricks
- Hacker-for-Hire group uses malicious 3Ds Max plugin to spread Malware
- Popular iOS SDK accused of Spying on Billions of Users
- Safari Bug revealed after Apple delay patch
- Google fixed a high severity bug in Chrome
- High severity bugs impacting Cisco's switch and fiber storage patched
- Qbot Trojan evolved to hijack email threads
- 3 Flaws in Apache Web Server Software

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. QakBot Banking Trojan with sneaky tricks

Description	
A banking trojan aimed at stealing bank account credentials and other financial information has now come back with new tricks up its sleeve to target government, military, and manufacturing sectors. These days Qbot is much more dangerous than it was previously — it has an active malspam campaign which infects organizations, and it manages to use a 'third-party' infection infrastructure like Emotet's to spread the threat even further. Attackers usually infect victims using phishing techniques to lure victims to websites that use exploits to inject Qbot via a dropper.	
Source	https://blog.morphisec.com/qakbot-qbot-maldoc-two-new-techniques
Infected Areas	Banking Sector
Recommendation	Hardened the device on your environment

2. Hacker-for-Hire group uses malicious 3Ds Max plugin to spread Malware

Description	
The APT hacker-for-hire operations and techniques used for industrial espionage. Various companies got targeted by this group with malware that can steal proprietary information. Companies across the globe got targeted by this, what seems to be, a new hacker group. The investigation showed that the unnamed victim is associated with real-estate developers in the U.S, the U.K, and Australia. APT mercenary groups have been used foe cyberespionage by private competing companies seeking financial information or negotiation details for high-profile contracts. Threat creators focused on infrastructure based on C&C servers, in South Korea. This is how traffic from malware samples in various countries get recorded and suggest other targets. This espionage is used to get information from competing private companies, so confidential information helps to take them down. Therefore, hackers-for-hire got created and is still popular.	
Source	https://www.autodesk.com/trust/security-advisories/adsk-sa-2020-0005
Infected Technology	Autodesk 3Ds Max
Recommendation	Update the latest patch available.

3. Popular iOS SDK accused of Spying on Billions of Users

Description	
A popular Chinese mobile advertising SDK has been found to contain malicious code capable of spying on iOS user and siphoning off ad revenue. The free SDK is used by both Android and iOS developers to embed third-party ads into their applications. The Mintegral SDK for iOS is said to conceal malicious code that allows it to monitor user activity and steal ad revenue from its competitors. Whenever a user clicks on an ad that is not served by the Mintegral network, the SDK inserts itself into the referral process, hoodwinking iOS into thinking the user had clicked on a different ad entirely. The SDK records details of all URL-based requests made via the compromised applications, before sending the information on to a remote logging server. The attempts to conceal the nature of the data being captured, both through anti-tampering controls and a custom proprietary encoding technique, are reminiscent of similar functionality	
Source	https://snyk.io/research/sour-mint-malicious-sdk/
Infected Technology	iOS Apps
Recommendation	Ensure the permission to the apps

4. Safari Bug revealed after Apple delay patch

Description	
Safari bug could be abused to leak or steal files from users' devices. The bug was reported the bug to Apple in this spring, but researcher decided to go public with finding after Apple informed the patch will only be available in Spring of 2021. The bug resides in safari's implementation the web share API - a new web standard that introduced a cross- browser API for sharing text, links, files and other content. This is a big privacy issue as this could lead to situations where malicious web pages might invite users to share an article via email with their friends but end up secretly siphoning or leaking a file from their device.	
Source	https://blog.redteam.pl/2020/08/stealing-local-files-using-safari-web.html
Infected Technology	iOS macOS
Recommendation	• Do not share article from untrusted web services • Apply the patch once released

5. Google fixed a high severity bug in Chrome

Description	
A code execution vulnerability in Chrome WebGL's JavaScript API has been fixed in Chrome 85 Stable channel. The API responsible for 2D and 3D rendering in the browser failed to handle objects in the memory leading. Attacker could manipulate the memory layout of the browser in way that could gain control of the use-after-free exploit, which could ultimately lead to arbitrary code execution. The vulnerability has a score of 8.3 in CVSS scale.	
Source	https://blog.talosintelligence.com/2020/08/vuln-spotlight-chrome-use-free-aug-2020.html
Infected Technology	Google Chrome versions 81.0.4044.138 (Stable), 84.0.4136.5 (Dev) and 84.0.4143.7 (Canary)
CVE	CVE-2020-6492
Recommendation	Update to the latest stable version

6. High severity bugs impacting Cisco's switch and fiber storage patched

Description	
Last week Cisco has released a patch for thirteen new bugs out of which 12 are rated with high severity. Six of the high severity bugs are present in Cisco's NX-OS software which can cause remote code injection, command injection and denial of service in the switches. Two bugs are in Cisco's implementation of Border Gateway Protocol (BGP) Multicast VPN which allowed remote unauthenticated attacker to cause denial of service due to improper validation and parsing of BGP update message. Similarly a high severity vulnerability in Distance Vector Multicast Routing Protocol (DVMRP) feature of Cisco IOS XR Software allowed unauthenticated remote attacker to exhaust process memory of affected device while other vulnerability in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) allowed remote unauthenticated attacker to read sensitive files and allowed directory traversal.	
Source	https://tools.cisco.com/security/center/publicationListing.x?product=Cisco&sort=-day_sir#~Vulnerabilities
Infected Technology	Cisco ASA; Cisco NX-OS; Cisco FXOS; Cisco BGP MVPN; Cisco DVMRP; Cisco ASA; Cisco FTD
CVE	CVE-2020-3566, CVE-2020-3452, CVE-2020-3517, CVE-2020-3415, CVE-2020-3394, CVE-2020-3398, CVE-2020-3397, CVE-2020-3454, CVE-2018-0307, CVE-2018-0306, CVE-2020-3338, CVE-2019-1896, CVE-2020-3504
Recommendation	• Apply the patch released by the OEM

7. Qbot Trojan evolved to hijack email threads

Description	
Qbot, an information gathering malware, has evolved again to hijack email threads. According to a research by Checkpoint, the malware is now able to extract all email threads from Outlook client which is forwarded to its remote server. These emails are then used to inject the malicious link in the email threads appearing as legitimate email conversation. The malware has already been known in the past to steal passwords, deliver other malware, conduct bank transaction using bot controller and so on.	
Source	https://research.checkpoint.com/2020/exploring-qbots-latest-attack-methods/
Infected Technology	Windows
Recommendation	Implement Endpoint protection Use of IOCs in reference to identify suspicious activity in your infrastructure

8. 3 Flaws in Apache Web Server Software

Description	
Apache has recently fixed several vulnerabilities in its web server that led to arbitrary code execution and sometime cause denial of service. According to researcher of Google's Project Zero the issue has been fixed in the latest version of the web server. The first vulnerability is caused due to buffer overflow that allowed attacker to view and make changes to sensitive data in the server while two other results in memory corruption which may result in denial of service.	
Source	https://bugs.chromium.org/p/project-zero/issues/detail?id=2030
Infected Technology	Apache web server
CVE	CVE-2020-9490, CVE-2020-11984, CVE-2020-11993
Recommendation	Update to the latest stable version 2.4.46

For any queries/recommendations:

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