InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Vulnerability in Zoom Client for Mac
2. Microsoft Patches 80 Vulnerabilities including two Privilege Escalation
3. New Ransomware Targets qnaps NAS devices
4. Astaroth: Fileless Malware
5. Canonical Ubuntu's Github get hacked
6. Android Apps Collecting Data Even When Denying Permission

14/07/2019

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. Vulnerability in Zoom Client for Mac

Description	
A vulnerability has been discovered for Zoom Client in Macs which allows attackers to force a user into joining a video call with video camera active. Zoom allows joining a meeting by simply clicking on a recieved message link, it also starts a web server on port 19421 upon installation and while these features may be user friendly, it certainly puts the user at risk due to its insecurity. This allows an attacker to send a link to a user and if the user gets tricked into clicking the link the attacker will also be able to get the video feed.	
Source	**https://www.securityweek.com/vulnerability-gives-attackers-remote-access-zoom-users’-cameras**
Infected Technology	**Mac OS**
Recommendation	**A patch will be sent by zoom for all Apple Clients.**

2. Microsoft Patches 80 Vulnerabilities Including two Privilege Escalation

Description	
For the month of July's patch, Microsoft fixed nearly 80 vulnerabilities, including two zero-days which could allow attackers to achieve privilege escalation on the compromised machines. The first major vulnerability was caused by how windows handled 'splwow64.exe' components. The service was used to provide 64-bit printer spooler service to 32-bit applications. The Second zero-day vulnerability Took advantage of Win32k component and how it handled objects in memory. These two vulnerabilities could let an attacker execute arbitrary code in the compromised windows machines.	
Source	https://www.securityweek.com/two-windows-privilege-escalation-vulnerabilities-exploited-attacks
Infected Technology	Windows
Recommendation	A patch has been sent by Microsoft on July's update.

3. New Ransomware Targets qnaps NAS devices

Description	
A new ransomware has been targeting QNAP Systems' Network Attached Storage (NAS) devices users. The malware was found to be brute-forcing weak credentials or exploiting known vulnerabilities in those devices.	
Source	https://www.darkreading.com/attacks-breaches/new-ransomware-targets-qnaps-network-attached-storage-devices/d/d-id/1335210
Infected Technology	Windows
Recommendation	Apply patches to your QNAP devices and use stronger credentials

4. Astaroth: Fileless Malware

Description	
Astaroth is able to steal users' credentials, keystrokes, etc. without dropping any executable file on the disk. It runs payload directly into a computer's memory. The malware relies on system tools and commands during its entire attack chain. Astaroth malware is being distributed through spear-phished email.	
Source	https://gbhackers.com/microsoft-spotted-new-fileless-malware-astaroth/
Infected Technology	Malicious E-mail
Recommendation	Do not open any links in the mail if it looks suspicious

5. Canonical Ubuntu's github get hacked

Description	
An attacker used a Canonical owned GitHub account compromising its credentials to access the account. It could have created repositories and created other issues. Fortunately, it was just a defacement attempt, so no malicious activity occurred unlike last year's attack on Gentoo Linux distribution's GitHub account, which was hacked using password-guessing and the repositories' content was replaced with malware.	
Source	https://thenextweb.com/security/2019/07/08/ubuntu-makers-github-account-hacked-but-the-source-code-is-safe/

6. Android Apps Collecting Data Even When Denying Permissions

Description	
More than 1300 android apps are collecting users' geolocation data even when denying permissions using various shady techniques. Apps were found using metadata of photos and Wi-Fi connections to figure out the location of devices. Apps were also found to be using phone's IMEI number stored on phone's SD card by other apps.	
Source	https://www.techworm.net/2019/07/android-apps-user-data-permission.html
Infected Technology	Android
Recommendation	Do not download applications from third-party sites

For any queries/recommendations:

Contact us: whois@cryptogennepal.com