September 7, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- Attackers Steal Outlook Credentials Via Overlay screens on legitimate site
- Cisco jabber Bug Could let hacker target windows system remotely
- Cisco issues warning over IOS XR
- SonicWall fixed vulnerability affecting 10 million managed devices
- Web skimmer steals credit card data via telegram
- Visa warns about new JavaScript skimmer in e-commerce sites
- Evilnum targeting financial firm with new Python-based RAT

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. Attackers Steal Outlook Credentials Via Overlay screens on legitimate site

Description	
Researcher Discovered a phishing campaign that uses overlay screens and email 'quarantine' policies to steal Microsoft Outlook Credentials from the targets. The overlay screens are displayed on the top of legitimate webpages to trick victims into providing their credentials. The experts observed the new technique in an attack aimed at an unnamed company, the messages were posing as the technical support team of employee's company. The email claimed that the company's email-security service had quarantined three valid email messages and ask the victims to review them by accessing their inbox. To put pressure on the victims and trick them into interacting with the targeted site the messages states that two of the messages were considered valid and are being held for deletion.	
Source	https://cofense.com/message-quarantine-campaign-overlying-potential/
Infected Technology	Outlook
Recommendation	• User should learn to recognize phishing attacks to avoid clicking on malicious link • Avoid giving sensitive information via email or link followed by email

2. Cisco jabber Bug Could let hacker target windows system remotely

Description	
Networking equipment leader Cisco has released a new version of its Jabber Video conferencing and messaging app for windows that includes patches for multiple vulnerabilities which, if exploited, could allow an authentication, remote attacker to execute arbitrary code. Two of the four flaw can be exploited to gain remote code execution on target system by sending specially crafted chat message in groups or specific individuals. A successful exploit could allow the attacker to cause the application to execute arbitrary programs on the targeted system with privileges of user account that is running the cisco jabber Client software.	
Source	https://watchcom.no/nyheter/nyhetsarkiv/uncovers-cisco-jabber-vulnerabilities/
Infected Technology	Cisco jabber
Recommendation	Update latest version of the software
CVE_ID	CVE-2020-3495

3. Cisco issues warning over IOS XR

Description	
Cisco has confirmed the flaws in IOS XR, which is a version of its Internetworking Operating System used in multiple Cisco Network Converging System carrier-grade routers, including the CRS, 12000 and ASR9000 series. The vulnerabilities are present in every Cisco device that runs any release of the IOS XR software if the software has been configured to use multicast routing. Multicast routing helps save bandwidth by sending some types of data - such as video - in one stream to multiple recipients. The flaws exist in the distance vector multicast routing protocol, or DVMRP. An unauthenticated, remote attacker could exhaust the process memory of a device by sending crafted internet group management protocol - aka IGMP - packets to a device. A successful exploit could allow the attacker to cause memory exhaustion, resulting in instability of other processes. A successful exploit could allow the attacker to cause memory exhaustion, resulting in instability of other processes. The Vulnerabilities score a relatively serious 8.6 CVSS score	
Source	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-dvmrp-memexh-dSmpdvfz
Infected Technology	Cisco IOS XR
Recommendation	• Rate limit the IGMP traffic • Implement the access control entry to an existing interface access control list, to block attackers
CVE_ID	CVE-2020-3566 CVE-2020-3569

4. SonicWall fixed vulnerability affecting 10 million managed devices

Description	
SonicWall has fixed an Insecure Direct Object Reference (IDOR) vulnerability in its cloud service effecting 50,000 organization with 1.9 user groups. The vulnerability is found due to improper validation of authorization which allowed attacker to add itself to any organization's user group resulting in full access of the victim's resource. According to the researchers, the team took 14 days after the issue was reported, exposing the userbase to the flaw while SonicWall has responded that the vulnerability has not been exploited and the fix has been deployed in its cloud service with no intervention by end user.	
Source	https://www.pentestpartners.com/security-blog/cloud-firewall-management-api-snafu-put-500k-sonicwall-customers-at-risk/
Infected Technology	SonicWall Cloud Management Platform

5. Web skimmer steals credit card data via telegram

Description	
Cybercriminal groups are constantly evolving to find new ways to pilfer financial information, and the latest trick in their arsenal is to leverage the messaging app Telegram to their benefit. The encrypted messaging service is being used to send stolen payment details from compromised websites back to the attackers. This data exfiltration mechanism is efficient and doesn't require them to keep up infrastructure that could be taken down or blocked by defenders. The fraudulent data exchange is conducted via Telegram's API, which posts payment details into a chat channel. hat data was previously encrypted to make identification more difficult.	
Source	https://blog.malwarebytes.com/web-threats/2020/09/web-skimmer-steals-credit-card-data-via-telegram/
Infected Areas	Telegram
Recommendation	Use browser protections to prevent from malicious payloads in sites

6. Visa warns about new JavaScript skimmer in e-commerce sites

Description	
Visa has issued a warning about a new JavaScript based skimmers found in various e-commerce sites. The new skimmer dubbed as Baka is added to merchant's checkout pages via a script that is used to download the skimming code from C2 server which decrypts the payload to JavaScript to load dynamically to evade malware detection. The skimmer remove itself from the memory when the data has been successfully exfiltrated making it difficult to identify and analyze.	
Source	https://usa.visa.com/content/dam/VCOM/global/support-legal/documents/visa-security-alert-baka-javascript-skimmer.pdf
Infected Technology	E-commerce site
Recommendation	For e-commerce platforms: • Regularly scan for communication with known C2 • Periodic vulnerability assessment of the platform For users: • Only use trusted platform for purchasing • Use browser protections to detect known threats in visited websites

7. Evilnum targeting financial firm with new Python-based RAT

Description	
Evilnum group, known for targeting financial firms since 2018, has changed its infection chain and added a RAT called "PyVil RAT" with abilities to harvest information, take screenshot, capture keystroke, open SSH shell and deploy new tools. The group has been linked to several malware campaigns across UK and EU involving backdoors. The attacker group uses spear phishing campaigns and JavaScript based Trojan to deliver the payload which download the RAT via multi-process delivery procedure. The group uses IPs instead of domain to communicate with its C2 server and keeps adding IPs to its list.	
Source	https://www.cybereason.com/blog/no-rest-for-the-wicked-evilnum-unleashes-pyvil-rat
Infected Technology	Windows
Recommendation	• Do not open attachments from unknown sources • Use End Point protection to avoid delivery of malicious tools • Scan your network for communication with known IOCs and communication with malicious IPs

For any queries/recommendations:

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