May 25, 2020

# INFOSEC WEEKLY

## #MADE4SECURITY

- Discord client used to steal password
- Cisco patched RCE in Unified CCX
- Microsoft Confirms Security problems for Windows 10 users
- Bluetooth Vulnerability Exposed millions of devices to hackers
- Ransomware deploying virtual machine to evade antivirus
- New DNS Vulnerability Let Attackers Launch Large-Scale DDoS Attack
- Phishing campaign using Excel macros to hack PCs

## 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. Discord client used to steal password

| Description | |
|---|---|
| A trojan dubbed AnarchyGrabber3 is released targeting discord client to steal passwords, user tokens, disable 2FA, and spread malware to victim's friends. The trojan modifies the Discord's JavaScript file to convert it to malware to steal sensitive information. The malicious script injected into Discord's JS file logs user out of the application and prompts to log back in. Once logged in, the malicious discord client attempts to disable 2FA, use webhook to forward victim's email, plain text password, IP Address. The script also forwards the malware attached message to friends of victim to distribute the malware. | |
| Source | https://www.bleepingcomputer.com/news/security/discord-client-turned-into-a-password-stealer-by-updated-malware/ |
| Infected Technology | Discord |
| Recommendation | • Do not open attachments from untrusted source<br>• Scan for malwares for attachment downloaded from internet<br>• Verify if your discord client is affected from the source above |

## 2. Cisco patched RCE in Unified CCX

| Description | |
|---|---|
| Cisco has fixed a critical remote code execution bug in its customer center express platform. The vulnerability was present due to insecure deserialization which allowed hacker to execute arbitrary code as root user by sending malicious serialized object to specific listener in affected system. The vulnerability was present in Cisco Unified CCX version 12.0 or before. Cisco has urged users to update the version to the fixed release. Cisco has also fixed various other vulnerability including SQL injection, memory overflow and DOS flaw in previous patches last week. | |
| Source | https://www.csoonline.com/article/3543838/cisco-and-palo-alto-networks-appliances-impacted-by-kerberos-authentication-bypass.html?&web_view=true |
| Infected Technology | CISCO Unified CCX |
| CVE | CVE-2020-3280 |
| Recommendation | Update to CCX to fixed release, 12.0(1) ES03 |

### 3. Microsoft Confirms Security problems for Windows 10 users

| Description | |
|---|---|
| Microsoft Confirms new security vulnerability with Thunderbolt ports, that enables an attacker with physical access to a PC to modify the port's controller firmware, disabling its security. A physical compromise such as this is nicknamed an "evil maid" attack—the idea being that your machine is targeted when you're staying in a hotel and away from your room, or when the overnight cleaning crew come to blitz your office. An attacker needs a few undisturbed minutes with no eyes-on. | |
| Source | https://www.forbes.com/sites/zakdoffman/2020/05/17/microsoft-confirms-serious-new-windows-10-security-problem-says-go-buy-a-new-pc/amp/?__twitter_impression=true |
| Infected Technology | Windows 10 |
| Recommendation | Enable Kernel DMA Protection |

### 4. Bluetooth Vulnerability Exposed millions of devices to hackers

| Description | |
|---|---|
| "BlueBorne," a set of vulnerabilities in the implementation of Bluetooth in various operating systems (OS): Android, Linux, iOS, and Windows. If successfully exploited, they can enable attackers to remotely hijack the device. The security flaws can also let attackers jump from one Bluetooth-enabled device to another. Exploiting BlueBorne could allow an attacker to execute malicious code, steal data, and carry out Man-in-the-Middle attacks. | |
| Source | https://www.trendmicro.com/vinfo/pl/security/news/internet-of-things/blueborne-bluetooth-vulnerabilities-expose-billions-of-devices-to-hacking |
| Infected Technology | Android, Linux, iOS, Windows |
| CVE_ID | CVE-2017-8628, CVE-2017-14315<br>CVE-2017-0781, CVE-2017-0782,<br>CVE-2017-0783, and CVE-2017-0785 |
| Recommendation | Patching and keeping the OS updated help mitigate attacks |

## 5. Ransomware deploying virtual machine to evade antivirus

| Description | |
|---|---|
| Ragnar Locker, a ransomware targeting corporate network since 2019, is deploying a Windows XP virtual machine to evade detection from security appliances. Sophos has released a report where it disclosed the method used by the ransomware to bypass security appliance. The attack is initiated by creating mini XP vdi file with various executable script. The script than identifies the attached disk and shares the drives to the virtual machine. The ransomware than encrypts the files via shared folder in virtual machine based in Windows XP. | |
| Source | https://www.bleepingcomputer.com/news/security/ransomware-encrypts-from-virtual-machines-to-evade-antivirus/ |
| Infected Medium | Microsoft Windows |
| Recommendation | • Enable Controlled Folder Access in Windows 10<br>• Use endpoint protections with behavior analysis |

## 6. New DNS Vulnerability Let Attackers Launch Large-Scale DDoS Attack

| Description | |
|---|---|
| NXNSAttack, a vulnerability in DNS servers that can be abused to launch DDoS attacks of massive proportions. NXNSAttack impacts recursive DNS servers and the process of DNS delegation. Recursive DNS servers are DNS systems that pass DNS queries upstream in order to be resolved and converted from a domain name into an IP address. | |
| Source | https://thehackernews.com/2020/05/dns-server-ddos-attack.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.2232.qx0a00e50w.1eew |
| Infected Technology | DNS Server |
| Recommendation | Update the DNS resolver Software |

## 7. Phishing campaign using Excel macros to hack PCs

| Description | |
|---|---|
| Microsoft Security Intelligence Team has warned about phishing campaign that installs remote access tool onto PCs using Excel 4.0 macros. The excel file is sent via E-mail with name "WHO COVID-19 Situation report". When recipient open the attached excel file, a security warning regarding editing option is displayed with a graph of corona virus cases in US. When allowed to run, the macro download NetSupport Manager that connects to Command and Control (C&C) server. | |
| Source | https://www.zdnet.com/article/microsoft-beware-this-massive-phishing-campaign-using-malicious-excel-macros-to-hack-pcs/ |
| Infected Technology | Microsoft Excel |
| Recommendation | Do not open attachments from unknown sources<br>Scan files before enabling macros/editing options |

For any queries/recommendations:

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