CENTRAL RESERVE POLICE FORCE

CYBER BYTE

- New Wi-Fi Vulnerability Enables Network Eavesdropping via Downgrade Attacks.
- Ransomware crooks now SIM swap executives' kids to pressure their parents.
- Cybercriminals Exploit Cloud Storage for SMS Phishing Scams.
- Fake Av Websites Used To Distribute Info-Stealer Malware.

CYBER BYTE
JUNE-2024
EDITION

- **Cyber frauds updates**

1.CYBER GEEKS NEWS

A) New Wi-Fi Vulnerability Enables Network Eavesdropping via Downgrade Attacks.

A new security vulnerability stemming from a design flaw in the **IEEE 802.11 Wi-Fi** standard that tricks victims into connecting to a less secure wireless network and eavesdrop on their network traffic.

The SSID Confusion attack, tracked as CVE-2023-52424, impacts all operating systems and Wi-Fi clients, including home and mesh networks that are based on WEP, WPA3, 802.11X/EAP, and AMPE protocols. The method "involves downgrading victims to a less secure network by spoofing a trusted network name (SSID) so they can intercept their traffic or carry out further attacks. A successful SSID Confusion attack also causes any VPN functionality to auto-disable on trusted networks to turn itself off, leaving the victim's traffic exposed.

Suggestion

- Keep your devices and firmware updated.
- Enable WPA3 encryption.
- Use strong, unique passwords.
- Implement network segmentation.
- Monitor network traffic.
- Employ strong encryption for sensitive data.
- Disable outdated protocols.
- Regularly review security settings.
- Educates users who uses your Wi-Fi network about security best practices.
- Report vulnerabilities in your Wi-Fi router or any other network device, report it to the manufacturer or relevant security authorities promptly.

B) Ransomware crooks now SIM swap executives' kids to pressure their parents.

RSAC Ransomware infections have morphed into "a psychological attack against the victim organization," as criminals use increasingly personal and aggressive tactics to force victims to pay up, according to Google-owned Mandiant. We saw situations where threat actors essentially SIM swap the phones of children of executives, and start making phone calls to executives, from the phone numbers of their children. The psychological dilemma that the executive goes through – seeing a phone call from the children, picking up the phone and hearing that it's somebody else's voice? Sometimes, **it's caller ID spoofing.** Other times, we see demonstrated SIM swapping family members." Either way, it's horrifying. Seeing a phone call from the children, picking up the phone, and hearing that it's somebody else's voice.

Suggestion

- Enable SIM card locks:
- Use strong, unique passwords.
- Implement multi-factor authentication (MFA).
- Educate executives and their families.
- Regularly review and update security settings.
- Monitor accounts for suspicious activity.
- Limit exposure of personal information.
- Secure devices with up-to-date software.
- Establish communication protocols.
- Report suspicious activity.

C) Cybercriminals Exploit Cloud Storage for SMS Phishing Scams.

A series of criminal campaigns that exploit cloud storage services such as **Amazon S3, Google Cloud Storage, Backblaze B2 and IBM Cloud Object Storage.** These campaigns, driven by unnamed threat actors, aim to redirect users to malicious websites to steal their information using SMS messages. **The attackers have two primary goals.**

First, they want to ensure that scam text messages are delivered to mobile handsets without detection by network firewalls. **Second,** they seek to convince end users that the messages or links they receive are trustworthy. By leveraging cloud storage platforms to host static websites with embedded spam URLs, attackers make their messages appear legitimate and avoid common security measures. Cloud storage services allow organizations to store and manage files and host static websites by storing website assets in a storage bucket. Cybercriminals have exploited this capability by embedding spam URLs in static websites stored on these platforms.

Suggestion

- Implement SMS filtering.
- Use reputable cloud storage providers.
- Encrypt sensitive data.
- Enable multi-factor authentication (MFA).
- Monitor for suspicious activity.
- Regularly review access controls.
- Implement mobile device management (MDM).
- Deploy anti-phishing solutions.
- Report phishing attempts.

D) Fake Av Websites Used To Distribute Info-Stealer Malware.

Threat actors used fake AV websites masquerading as legitimate antivirus products from Avast, Bitdefender, and Malwarebytes to distribute malware. In mid-April 2024, researchers at Trellix Advanced Research Center team spotted multiple fake AV sites used to distribute info-stealers. The malicious websites hosted sophisticated malicious files such as APK, EXE and Inno setup installer, including Spy and Stealer capabilities. The fake websites were masquerading as legitimate antivirus products from Avast, Bitdefender, and Malwarebytes. The sites hosting malware are avast-securedownload.com (Avast.apk), bitdefender-app.com(setup-win-x86-x64.exe.zip), malwarebytes.pro (MBSetup.rar).

List of the malicious websites.

avast-securedownload[.]com: Distributes the SpyNote trojan as an Android package file ("Avast.apk"), which, once installed, requests intrusive permissions such as reading SMS messages and call logs, installing and deleting apps, taking screenshots, tracking location, and mining cryptocurrency.

bitdefender-app[.]com: Distributes a ZIP archive file ("setup-win-x86-x64.exe.zip") that was used to deploy the Lumma information stealer.

malwarebytes[.]pro: Distributes a RAR archive file ("MBSetup.rar") that was used to deploy the StealC information stealer malware. The experts also discovered a malicious Trellix binary that pretends to be Legit **(AMCoreDat.exe).**

Suggestion

- Use reputable antivirus software.
- Implement web filtering.
- Enable browser security features.
- Deploy endpoint protection.
- Monitor network traffic.
- Conduct regular security audits.
- Patch and update software.
- Enforce least privilege access.
- Establish incident response procedures.

2.CYBER FRAUDS

i) Delhi Police arrested a cyber-fraudster who duped people via fake ads in Jamtara.

An 18-year-old man who ran fake advertisements online and phished money from unsuspecting victims has been arrested by Delhi Police in Jharkhand's Jamtara. The accused used **remote desktop apps** to take control of his victims' computers. Police found that the accused had siphoned over Rs 1 crore so far. Scammer started putting up fake advertisements on search engine websites in such a way that if a user searched for the official customer

care helpline of a particular service provider, web links would redirect to his website. In this way, an unsuspecting airline ticket holder, a professor of Jawaharlal Nehru University, searched the name of the carrier to avail himself of a cancellation refund. The user dialed a number given on the website, and the accused represented himself as a customer care representative of the airline. The victim was then asked to download a remote desktop control application to lodge a complaint, but a phishing link was provided to him. The link resembled a bank account details form, similar to those used by banks. Once the victim entered his bank details, the fraudster logged into his net banking and siphoned off more than Rs 7 lakh. A complaint was registered with the police. Investigation into the money trail revealed that the money was sent to four accounts in different locations across the country, such as Kolkata, Mumbai, Ludhiana and Varanasi. Police traced the mobile number advertised, and it was traced to Jharkhand's Jamtara. A police raid in the wee hours of the morning resulted in the apprehension of Ansari, and the discovery of his brother and accomplice in the cyber fraud.

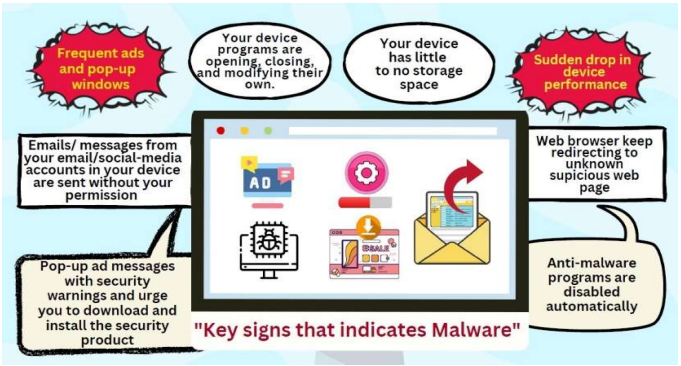
ii) Cyber fraudsters target emotional side of parents.

Chennai: Cybercriminals who extort money by masquerading as officers from cybercrime wings or the Enforcement Directorate (ED) have now changed tack and threaten the potential victims by claiming to detain or arrest their adult children on serious charges. In a recent incident, a businessman received a call from an individual who introduced himself as a police officer and demanded 1 lakh to release his daughter from a case involving her and her friends in a cheating scam. In their statement, the cybercrime police said the scammer usually initiates contact with the victim through a phone call, claiming to be a law enforcement or govt official. They assert that the victim's family members, usually son or daughter, have been involved in a serious crime and could be arrested. They also fabricate details such as case numbers to make the story seem believable and threaten with legal consequences.

"The scamster may employ techniques such as spoofing phone numbers or using distressing background noises like crying or shouting. The victim is pressured to act quickly and comply with the scammer's demands, usually involving transfer of money or sensitive information. The scammer isolates the victim from external communication or verification by instructing them to stay. on the phone and not contact anyone, particularly the family member in question," the release said. The fraudster then demands immediate payment or other forms of compliance from the victim to resolve the fabricated crisis or to prevent further consequences. Fearing the worst, the victim makes payment to the cyber fraudster. Recently, a Chennai resident received a call wherein the caller claimed that his daughter had been arrested for money laundering and that her identity would be released to the media. The caller demanded online transfer of 40,000. When the victim said he did not have that much money, the caller asked him to pay 5,000. He attempted to pay the money but made a mistake with the PIN. However, the victim managed to reach his family through his friend's phone and confirmed that his daughter was at home, leading him to disconnect the call.

3.TIP OF THE MONTH

Malware key signs & protective measures.



- Avoid clicking on suspicious emails, links, and sites from unknown source.
- As soon as you click on any malicious link, your mobile can be hacked or your data can be stolen.
- Browse only secure and authorized websites.
- Always keep your computer software/browser up to date.
- Maintain backup of your data regularly.
- Install software like pop-up/ ad-blocker to block the malicious advertisements appearing on websites.
- Install antivirus and antimalware solutions in your devices and keep them updated.
- Hover over the images/links to find the actual link.
- Do not install any apps through links received on chats or social media posts.


9 अप्रैल 202


Celebrating Moments


PPT ON GRIEVANCE REDRESSAL OF MARTYRS' NOKs


DIRECTORATE GENERAL
SERVICE AND LOYALTY