CENTRAL RESERVE POLICE FORCE

CYBER BYTE

- NPM Trojan Bypasses UAC, Installs AnyDesk with "Oscompatible" Package.
- Threat group using youTube channels to distribute Lumma Stealer.

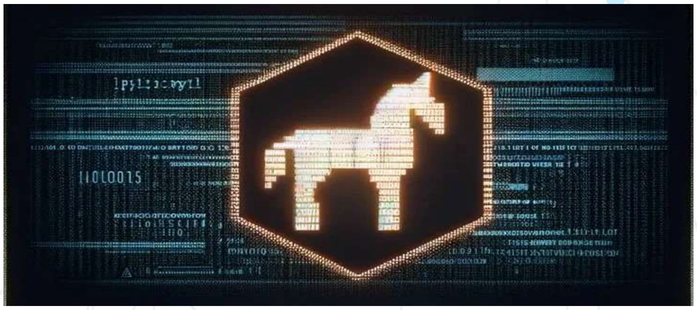
CYBER BYTE
FEBRUARY-2024
EDITION

Cyber frauds updates

Secure Social Media Accounts.

1.CYBER GEEKS NEWS

A) NPM Trojan Bypasses UAC, Installs AnyDesk with "Oscompatible" Package



A malicious package uploaded to the NPM (Node package manager) registry has been found deploying a sophisticated remote access trojan on compromised Windows machines. The package is named as "oscompatible".

Oscompatible included a "few strange binaries," according to software supply chain security firm Phylum, including a single executable file, a dynamic-link library (DLL) and an encrypted DAT file, alongside a JavaScript file.

This JavaScript file ("index.js") executes an "autorun.bat" batch script but only after running a compatibility check to determine if the target machine runs on Microsoft Windows.

If the platform is not Windows, it displays an error message to the user, stating the script is running on Linux or an unrecognized operating system, urging them to run it on "Windows Server OS." The batch script, for its part, verifies if it has admin privileges, and if not, runs a legitimate Microsoft Edge component called "cookie_exporter.exe" via a PowerShell command.

Attempting to run the binary code will trigger a User Account Control (UAC) prompt asking the target to execute it with administrator credentials.

In doing so, the threat actor carries out the next stage of the attack by running the DLL ("msedge.dll") by taking advantage of a technique called DLL search order hijacking.

The trojan zed version of the library is designed to decrypt the DAT file ("msedge.dat") and launch another DLL called "msedgedat.dll," which, in turn, establishes connections with an actor-controlled domain named "kdark1[.]com" to retrieve a ZIP archive.

The ZIP file comes fitted with the AnyDesk remote desktop software as well as a remote access trojan ("verify.dll") that's capable of fetching instructions from a command-and-control (C2) server via WebSocket's and gathering sensitive information from the host.

It also "installs Chrome extensions to Secure Preferences, configures AnyDesk, hides the screen, and disables shutting down Windows, captures keyboard and mouse events,".

Suggestions:

- Keep autoplay settings disabled.
- Set up and use firewalls to keep the internet connections secure.
- Use a non-administrator account whenever possible.
- Think twice before clicking links or downloading anything from untrusted side.
- Limit your file-sharing.
- Keep your computer and software updated.
- Avoid third-Party software Downloads.
- Use Hardware-based firewall and deploy DNS.

B) Threat group using YouTube channels to distribute Lumma Stealer.

SOC PRIME
LUMMA STEALER
Hackers Abuse YouTube Videos
to Spread Malware & Steal Sensitive Data

A threat group is using YouTube channels to distribute a Lumma Stealer variant. The attackers compromise YouTube accounts, upload videos featuring cracked software, and embed malicious URLs in the video descriptions. These URLs leads users to download a ZIP file containing a private .NET loader responsible for fetching the Lumma Stealer malware. The Lumma Stealer variant employs various evasion techniques, such as decoding strings using the "BygoLarchen" method and conducting extensive environment checks to avoid detection. The final payload is injected using the "Suspend Thread" function. Lumma Stealer establishes communication with a command and control (C2) server, exchanging instructions and transmitting stolen data.

Suggestions:

- Update system, applications and software to the latest version and download the latest security patches.
- Install anti-virus/anti-malware software and keep the software (and its definition files) updated.
- Perform a scan of the system and networks regularly and scan all received files.
- Use complex passwords and strong methods of authentication.
- Be careful while clicking on links from untrusted sources.
- Don't trust pop-up windows that ask you to download software.
- Regularly monitor all user accounts and disable inactive accounts.
- Enforce password updates for account owners that may have their credentials leaked.

2.CYBER FRAUDS

A) Google Search; two held in Jharkhand google Search.

Alongside deepfake calls and videos, scammers are using Google Ads to steal money from people online sitting miles away from them. In a recent case, a Delhi woman, searched for the customer care number of **Punjab National Bank** on Google and called the mobile number that appeared on the website. The person on the other side of the line asked her to download an app that helped him steal over Rs 5 lakh from her account.

As per an official statement by Deputy Commissioner of Police, "The alleged person advised her to download **Rust Desk App** and took access of her phone and account related information. Later, a total amount of Rs 5,45,000 was debited from her Canara Bank account."

B) A 45-year-old doctor loses Rs 1.8 crore.

A 45-year-old doctor from Dharwad has fallen prey to cyber criminals, losing a whopping Rs 1.79 crore. The cybercrime police are investigating the fraud which took place when the doctor received a call from an unknown individual two months ago. The fraudster, posing as a financial advisor, duped the doctor by promising lucrative returns on her investments in the stock market. The caller suggested investing in the IPO of Planet Image International Company for substantial profits. The doctor willingly joined a social media site at the caller's behest.

The interaction took a sinister turn as the cyber criminals successfully extracted sensitive data related to the doctor's bank accounts. Subsequently, a sum of Rs 1.79 crore was transferred from various bank accounts linked to the victim. The manner in which the criminals obtained such personal information remains unclear, prompting the police to take up further investigation. A case has been registered with the police who are calling.

3.TIP OF THE MONTH

Secure Social Media Accounts.

1. Strong Password Policies: Implement and enforce strong password policies, including regular changes and avoidance of password reuse across different platforms.

2. Multi-Factor Authentication (MFA): Enable MFA for all social media accounts wherever possible.

3. Access Control: Limit access to official social media accounts to designated officials and systems.

4. Dedicated Secure Devices: Allocate dedicated and secured devices specifically for managing official social media accounts. These devices should have enhanced security features and should only be used for this purpose to reduce the risk of compromise.

5. Dedicated Email Accounts: Use a dedicated and separate email account for operating official social media accounts. Ensure that the credentials for this email and the social media accounts are distinct and comply with the organization's password policy.

6. Avoid Personal Email for Operating Official Accounts: Refrain from using personal email accounts for managing official social media accounts to prevent potential security breaches.

7. Single Active Session: Ensure that only a single session is active at any given time. Regularly check and terminate any other sessions that are active under the account settings to prevent unauthorized access.

8. Content Approval: Ensure that content posted on official social media handles is pre-approved by the appropriate authority within the organization.

9. Controlled Access to Social Media Management Tools: If using social media management tools, ensure controlled and secured access to these tools, with regular reviews of who has access.

10. Avoid Public Devices: Do not use public or unauthorized devices to access official social media accounts.

11. Disable Geolocation: Turn off GPS access for official social media platforms to prevent location tracking.

12. Software Updates: Regularly update social media applications and devices with the latest security patches.

13. Access Revocation: Promptly revoke access to social media accounts if an employee's role changes or they leave the organization.

14. Monitor Associated Email Accounts: Regularly check the email account linked with the social media accounts for any unusual activity alerts.

15. Login Alerts: Activate alerts for unrecognized login attempts in the security settings of the social media platform.

16. Caution with Third-Party Apps: Exercise caution when using third-party applications for social media management.

17. Stay Informed: Keep abreast of updates from social media companies regarding security and privacy settings and implement them appropriately.

18. Beware of Phishing and Malware: Do not click and submit credentials on phishing links and scan your system regularly with antivirus for the presence of any malware.

19. Be careful when clicking on a link: Someone might take over one of your connection's accounts and try to trick you into clicking. It could start with an innocent-sounding question, like "what do you think?" that entices you to click and doesn't give you enough context to suspect anything. The link might send you to a page that infects your device. Or, it might look exactly like a legitimate website (such as the platform's login page), but it's not.

19. Don't share your personal information: A "friend" or fake account might try to trick you into sharing your personal information. Be cautious of messages related to making money, starting a romantic relationship or helping the person with their account because these are common starting points that scammers use to build trust.

20. Never tell someone your password or authentication codes: Don't share it, even if your known is asking you to share a code that's sent to your phone. If their account is compromised, the scammer is probably trying to get into one of your accounts and asking you to share the MFA code that will give them access.

NATIONAL CYBER FORENSIC LAB

BASIC COURSE IN CYBER FORENSIC INVESTIGATION TRAINING PROGRAMME

01.01.2024 TO 12.01.2024