مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Malware Campaign- New Cheana Stealer

Tracking #:432316193

Date:28-08-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a sophisticated phishing campaign that utilizes the "Cheana Stealer" malware. This malware is designed to target users across Windows, Linux, and macOS operating systems.

TECHNICAL DETAILS:

The Cheana Stealer is a sophisticated malware that targets users downloading Virtual Private Network (VPN) applications on Windows, Linux, and macOS. This malware is distributed through a phishing site that impersonates a legitimate VPN service (WarpVPN) to lure users into downloading malicious applications. This malware is specifically targeting cryptocurrency-related services and collects sensitive data such as stored browser passwords, SSH keys, and cryptocurrency wallet information.

- **Targeted Distribution**: Cheana Stealer is delivered through distinct methods for each OS:
  - **Windows**: Uses a PowerShell script linked to a malicious Python package that steals sensitive information from cryptocurrency wallets and browser extensions.
  - **Linux**: Distributes via a curl command that collects various types of sensitive data.
  - **macOS**: Employs deceptive prompts to gather credentials and sensitive information through the system's Keychain.
- **Phishing Site and User Trust**: The phishing site is linked to a Telegram channel with over 54,000 subscribers, which previously offered "free" VPN services to build credibility before promoting the malicious site.
- **Data Exfiltration**: The stolen data is securely sent to the attackers' command and control (C&C) server over HTTPS, making detection challenging.

INDICATORS OF COMPROMISE(IOCs):

Indicators	Type	Description
70f08497d7a9e6a8e5f2dd3683a20563d20668e1c78df636ff1e36a014c9d493	SHA-256	install-linux.sh
acf807def82c4b56752a9fa9b081dbb37ba9cc9f6e1c522568ff502b6b49b6db	SHA-256	install.bat
48964c11fcbefd6508164239866c94b55ca2798e9745671c37447ad0a6f3e1c4	SHA-256	install.sh
d3ece8616d0dd8244666af574cc2475d947180ed240f49b1a6e61443a896f65d	SHA-256	main.zip
3ef838502663c167f5c502585e810ffae3e03152b3f82544b813389c19a33dce	SHA-256	main.py
ac4aeab3952f6ca960cbd48c3123f09a68f50818f9bdf35c9d811570893fa102	SHA-256	fflg.py
6a68e95ae67aa8c61bd74ecf5f57f98fbdc0bbe0489ae71b7c8732edf49ac3a9	SHA-256	helperwd.py
c044b1a36249f6fe7219e6c48270d9927bf359110ff3583129dcbdff809f2d2d	SHA-256	utils.py
ba8058b704a55e50c24383a765fd74b38d7dbbf8546c4f179266c265403174b8	SHA-256	Warpvpn.zip
warpvpn[.]net	Domain	Phishing site
hxxps://ganache[.]live	Domain	C&C

RECOMMENDATIONS:

- Review the Indicators of Compromise (IOCs) and implement the necessary security measures.
- **Download Software Only from Reputable Sources**: Always verify the legitimacy of any VPN or software prior to downloading.
- **Recognize Phishing Attempts**: Stay informed about common phishing tactics. Awareness campaigns can help users identify potential scams.
- **Advanced Endpoint Protection**: Employ advanced security solutions to detect and block malicious scripts. Ensure these tools are updated frequently.
- **Monitor Network Traffic**: Use security tools to monitor and prevent communication with known malicious C&C servers.
- **Enable Multi-Factor Authentication (MFA)**: Implement MFA to add an additional layer of security, reducing the impact of compromised credentials.
- **Incident Response Plan**: Develop and regularly update an incident response plan to ensure swift action against potential malware infections.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://cyble.com/blog/new-cheana-stealer-targets-vpn-user/?__hstc=202258190.a25d22137b745cd14ecf20f735f0e4b9.1724825568337.1724825568337.1724825568337.1&__hssc=202258190.2.1724825568338&__hsfp=797865114