مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Malware Campaign: StrelaStealer

Tracking #:432315729

Date:26-03-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed an ongoing campaign targeting organizations with StrelaStealer, a malware program designed to steal email credentials.

TECHNICAL DETAILS:

StrelaStealer has been active since 2022 and is known for large-scale email phishing campaigns. The malware, first documented in November 2022, has evolved through various large-scale campaigns, with the most recent one in late January 2024. StrelaStealer targets Windows machines and aims to steal email login credentials from popular email clients.

Delivery Method: The primary delivery method is phishing emails.

The infection chain of StrelaStealer involves phishing emails with attachments that execute the malware payload. In earlier versions, the malware was spread via .iso files containing .lnk and HTML files, utilizing polyglot files to evade detection. However, the latest variant uses ZIP attachments to drop JScript files, which then deploy a DLL payload through rundll32.exe. This new version employs control flow obfuscation and removes PDB strings to complicate analysis and avoid detection by security tools relying on static signatures.

If a user clicks on a malicious link or attachment in a phishing email, StrelaStealer can be installed on their device. Once installed, the malware steals email login credentials, granting attackers access to victims' email accounts. This compromised access can be used for further attacks, including:

- Sending spam emails from the victim's account.
- Launching spear phishing attacks against the victim's contacts.
- Exfiltrating sensitive information

INDICATORS OF COMPROMISE(IoCs):

SHA256 Hash	**Filetype**
0d2d0588a3a7cff3e69206be3d75401de6c69bcff30aa1db59d34ce58d5f799a e6991b12e86629b38e178fef129dfda1d454391ffbb236703f8c026d6d55b9a1	DLL
f95c6817086dc49b6485093bfd370c5e3fc3056a5378d519fd1f5619b30f3a2e aea9989e70ffa6b1d9ce50dd3af5b7a6a57b97b7401e9eb2404435a8777be054 b8e65479f8e790ba627d0deb29a3631d1b043160281fe362f111b0e080558680	EML
3189efaf2330177d2817cfb69a8bfa3b846c24ec534aa3e6b66c8a28f3b18d4b	ZIP

544887bc3f0dccb610dd7ba35b498a03ea32fca047e133a0639d5bca61cc6f45	JS
193[.]109[.]85[.]231	C2 server

RECOMMENDATIONS:

- Block the attached IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- Regular Backups: Implement a robust backup routine with backups stored offline and regularly tested for recoverability.
- Increase awareness: Train users to identify phishing emails. Educate them on best practices for email security, such as not clicking on suspicious links or attachments.
- Enable multi-factor authentication (MFA): MFA adds an extra layer of security to email accounts, making it more difficult for attackers to gain access even if they steal login credentials.
- Update email clients: Regularly update email clients to ensure they have the latest security patches.
- Implement email security solutions: Consider deploying solutions that can detect and block phishing emails.
- Monitor systems for suspicious activity: Regularly monitor systems for signs of malware infection.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings (e.g. IOCs, TTPs...etc).

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

REFERENCES:

1. https://unit42.paloaltonetworks.com/strelastealer-campaign/