Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 232 **22-02-2024**

Name: Ov3r_Stealer Malware Targets Facebook Ads for Password Theft – Active IoCs

Threat Classification: Malware

Affected Software / Services:

- Facebook, Discord, Windows Operating System

Summary:

Ov3r_Stealer, a newly emerged malware, spreads through deceptive job advertisements on Facebook, targeting users seeking management positions. The malware is distributed via a Discord URL, where a PowerShell script downloads the Ov3r_Stealer payload from a GitHub repository. The infection chain begins with fake job ads on Facebook, redirecting users to a Discord CDN to download a malicious file disguised as a DocuSign document. Ov3r_Stealer employs various loading methods and establishes persistence by creating a scheduled task, compromising a range of applications and exfiltrating data to a Telegram bot.

Severity	**High**
Attack Vector	Social Engineering

Active IOCs

MD5
58c966c06d908017264506dbe2dd7e45

© Copyright 2023, Pakistan Telecommunication Authority. All Rights Reserved.
Unauthorized use, dissemination or modification of this document is strictly prohibited.

5d39a9e99b58faf99cae275723c9168e
a8fd240af0ab05e5496afb0d6df0223c
48a2fca4599cd29531cb62cfb5534478
477c0ed261ad6db5eb250b0efccf963a
1210c904bb5986a63605a29cc54c47d9
SHA-1
6d0820a24a78d4f5699f9c25c02f1de3ac834fb6
41d186163cd74d39e89cf06fa4f3a06d7fa88f6b
da9003182528580b7104458c75f561f39d04d101
ff5e2b1a310c19e278496900b7dd2b2689103f4c
6149acf6575b7230710d111c9c46d61d6b62cad5
334430f26a460035e8b9634c800dee623402da7f
SHA-256
69941417f26c207f7cbbbe36ce8b4d976640a3d7f407d316932428e427f1980b
7c0a1e11610805bd187ef6e395c8fa31c1ae756962e26cdbff704ce54b9e678a
70c23213096457df852b66443d9a632e66816e023fdf05a93b9087ffb753d916
6bd8449de1e1bdd62a86284ed17266949654f758e00e10d8cd59ec4d233c32e5
a841cd16062702462fdffdd7eef9fc3d88cde65d19c8d5a384e33066d65f9424
22236e50b5f700f5606788dcd5ab1fb69ee092e8dffdd783ac3cab47f1f445ab

Recommendations:

- Block all threat indicators and search for IOCs using your security controls.
- Exercise caution with email attachments from unknown sources, avoiding enabling macros.
- Keep systems updated with the latest patches to mitigate known vulnerabilities.
- Educate staff on identifying phishing emails and safe online practices.
- Regularly backup critical data and enforce MFA for sensitive accounts.
- Develop and test an incident response plan for efficient security incident handling.
- Deploy robust endpoint protection and email filtering solutions.
- Conduct regular security assessments and penetration testing.
- Vet third-party vendors and software for strong security practices before integration.

© Copyright 2023, Pakistan Telecommunication Authority. All Rights Reserved.
Unauthorized use, dissemination or modification of this document is strictly prohibited.

- In case of any incident, please report to this office, through PTA CERT Portal and email.

© Copyright 2023, Pakistan Telecommunication Authority. All Rights Reserved.
Unauthorized use, dissemination or modification of this document is strictly prohibited.