

# Beware: Fake Facebook Job Ads Spreading 'Ov3r\_Stealer' to Steal Crypto and Credentials

 [thehackernews.com/2024/02/beware-fake-facebook-job-ads-spreading.html](https://thehackernews.com/2024/02/beware-fake-facebook-job-ads-spreading.html)

February 6, 2024

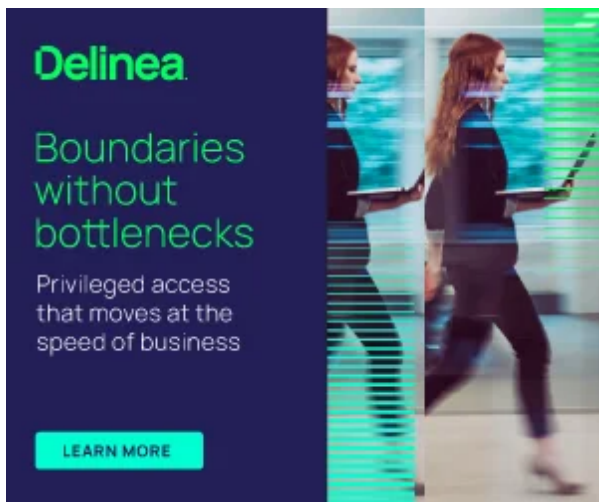


Threat actors are leveraging bogus Facebook job advertisements as a lure to trick prospective targets into installing a new Windows-based stealer malware codenamed **Ov3r\_Stealer**.

"This malware is designed to steal credentials and crypto wallets and send those to a Telegram channel that the threat actor monitors," Trustwave SpiderLabs said in a report shared with The Hacker News.

Ov3r\_Stealer is capable of siphoning IP address-based location, hardware info, passwords, cookies, credit card information, auto-fills, browser extensions, crypto wallets, Microsoft Office documents, and a list of antivirus products installed on the compromised host.

While the exact end goal of the campaign is unknown, it's likely that the stolen information is offered for sale to other threat actors. Another possibility is that Ov3r\_Stealer could be updated over time to act as a QakBot-like loader for additional payloads, including ransomware.



The starting point of the attack is a weaponized PDF file that purports to be a file hosted on OneDrive, urging users to click on an "Access Document" button embedded into it.

Trustwave said it identified the PDF file being shared on a fake Facebook account impersonating Amazon CEO Andy Jassy as well as via Facebook ads for digital advertising jobs.

Users who end up clicking on the button are served an internet shortcut (.URL) file that masquerades as a DocuSign document hosted on Discord's content delivery network (CDN). The shortcut file then acts as a conduit to deliver a control panel item (.CPL) file, which is then executed using the Windows Control Panel process binary ("control.exe").

The execution of the CPL file leads to the retrieval of a PowerShell loader ("DATA1.txt") from a GitHub repository to ultimately launch Ov3r\_Stealer.

Library ID: 267052542987870

Inactive

Nov 7, 2023 - Nov 7, 2023

Platforms

**pink women's magazine - අම්මටයි උවටයි**

Sponsored

Library ID: 267052542987870

**We are Hiring**

We have exciting opportunities available for a Digital Marketing Specialist and a Paid B2C Ad Account Manager. These positions offer freelance work with the flexibility to work remotely.


Here are the details:

- Required time commitment: 16 hours per week.
- Average salary: \$14,000 USD per month.
- Working environment: India
- Job description in detail : <https://shorturl.at/dKOR6>

Join us and enjoy:

- 🔥 Industry leading salary packages
- 🏡 A healthy work environment
- 📈 Opportunities to learn & grow.
- 🧘 Health and wellness benefits.

Ready to make your next big career move? 🤖



### European Union transparency

---

#### About the advertiser

**pink women's magazine - අම්මටයි උවටයි**

@pinkpaper.lk

19.6K followers • Yoga Studio

---

#### Beneficiary and payer

When targeting certain locations, advertisers are required to disclose who will benefit from an ad and who is paying for it.

Current

<b>Beneficiary</b>	Betsopen
<b>Payer</b>	Betsopen

---

[About ads and data use](#)

It's worth noting at this stage that a near-identical infection chain was recently disclosed by Trend Micro as having put to use by threat actors to drop another stealer called Phemedrone Stealer by exploiting the Microsoft Windows Defender SmartScreen bypass flaw (CVE-2023-36025, CVSS score: 8.8).

The similarities extend to the GitHub repository used (nateeintanan2527) and the fact that Ov3r\_Stea1er shares code-level overlaps with Phemedrone.

"This malware has recently been reported, and it may be that Phemedrone was re-purposed and renamed to Ov3r\_Stea1er," Trustwave said. "The main difference between the two is that Phemedrone is written in C#."



**CIS Hardened Images®**

**Work more securely in the cloud**

Microsoft Windows 10 & 11 in Azure Marketplace

**LAUNCH NOW**

CIS

Further solidifying the connections between the two stealer malware, the threat actor has been observed sharing news reports published about the Phemedrone Stealer on their Telegram channels in an effort to build "street cred" for their malware-as-a-service (MaaS) business.

"My custom stealer is on the new[s], showing how evasive it is, im [sic] the developer of it, so happy now," the threat actor, who goes by the online alias Liu Kong said, while also expressing frustration at the fact that threat hunters managed to "reverse the whole exploit chain" despite everything being "on memory."



The findings come as Hudson Rock revealed that threat actors are advertising their access to law enforcement request portals of major organizations like Binance, Google, Meta, and TikTok by exploiting credentials obtained from infostealer infections.

They also follow the emergence of a category of infections called CrackedCantil that leverage cracked software as an initial access vector to drop loaders like PrivateLoader and SmokeLoader, when subsequently act as a delivery mechanism for information stealers, crypto miners, proxy botnets, and ransomware.

Found this article interesting? Follow us on Twitter and LinkedIn to read more exclusive content we post.

SHARE \_ \_ \_ \_ \_

SHARE