LofyLife: malicious npm packages steal Discord tokens and bank card data

By Igor Kuznetsov

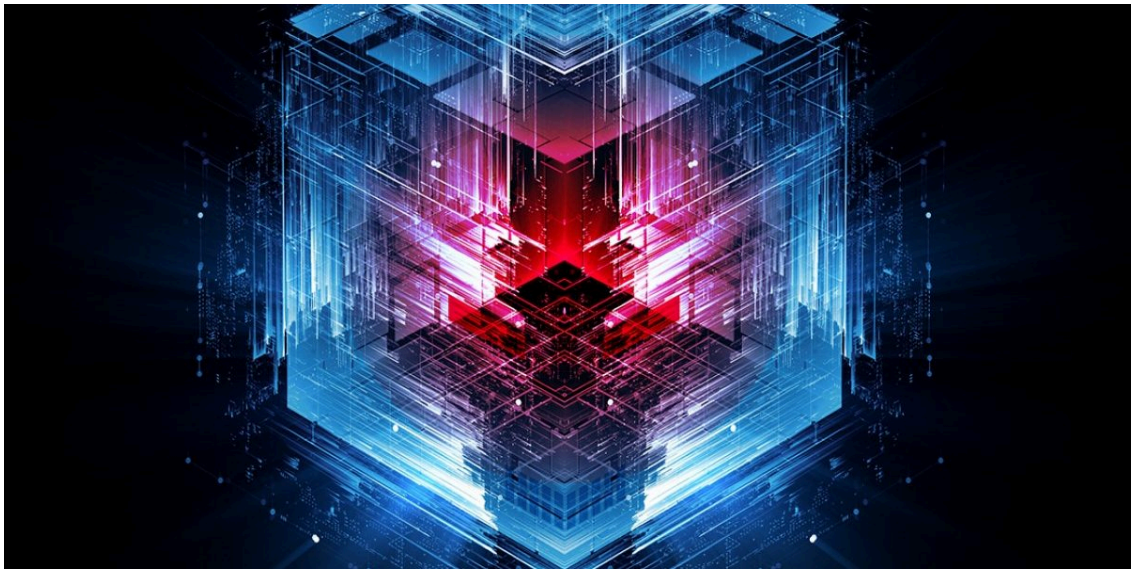
Published: 2022-07-28 · Archived: 2026-04-05 18:46:59 UTC

Incidents

Incidents

28 Jul 2022

1 minute read



On July 26, using the internal automated system for monitoring open-source repositories, we identified four suspicious packages in the Node Package Manager (npm) repository. All these packages contained highly obfuscated malicious Python and JavaScript code. We dubbed this malicious campaign “LofyLife”.

Título

Este pacote capitaliza corretamente seus títulos conforme O Manual de Estilo de Chicago. Além disso, todos os Os nomes dos produtos da Vercel também são capitalizados corretamente.

Uso

Primeiramente, instale o pacote:

```
fio adicionar título
```

Em seguida, carregue-o e converta qualquer entrada:

```
const title = require('proc-title')

title('tHe cHicaGo maNual oF StyLe')

// Vai resultar em:
// "O Manual de Estilo de Chicago"
```

Description of the proc-title package (Translation: This package correctly capitalizes your titles as per the Chicago manual of style)

The Python malware is a modified version of an open-source token logger called Volt Stealer. It is intended to steal Discord tokens from infected machines, along with the victim’s IP address, and upload them via HTTP. The JavaScript malware we dubbed “Lofy Stealer” was created to infect Discord client files in order to monitor the victim’s actions. It detects when a user logs in, changes email or password, enables/disables multi-factor authentication (MFA) and adds new payment methods, including complete bank card details. Collected information is also uploaded to the remote endpoint whose address is hard-coded.

Data is exfiltrated to Replit-hosted instances:

- life.polarlabs.repl[.]co
- Sock.polarlabs.repl[.]co

- idk.polarlabs.repl[.]co

Kaspersky solutions detect the threat with the following verdicts:

- HEUR:Trojan.Script.Lofy.gen
- Trojan.Python.Lofy.a

We are constantly monitoring the updates to repositories to ensure that all new malicious packages are detected.

Timeline of uploaded packages

Package name	Version	Timestamp (UTC)
small-sm	8.2.0	2022-07-17 20:28:29
small-sm	4.2.0	2022-07-17 19:47:56
small-sm	4.0.0	2022-07-17 19:43:57
small-sm	1.1.0	2022-06-18 16:19:47
small-sm	1.0.9	2022-06-17 12:23:33
small-sm	1.0.8	2022-06-17 12:22:31
small-sm	1.0.7	2022-06-17 03:36:45
small-sm	1.0.5	2022-06-17 03:31:40
pern-valids	1.0.3	2022-06-17 03:19:45
pern-valids	1.0.2	2022-06-17 03:12:03
lifeculer	0.0.1	2022-06-17 02:50:34
proc-title	1.0.3	2022-03-04 05:43:31
proc-title	1.0.2	2022-03-04 05:29:58

We covered the incident in more detail in a private report delivered to customers of our Threat Intelligence Portal.

Latest Posts

Latest Webinars

Reports

Kaspersky researchers analyze updated CoolClient backdoor and new tools and scripts used in HoneyMyte (aka Mustang Panda or Bronze President) APT campaigns, including three variants of a browser data stealer.

Kaspersky discloses a 2025 HoneyMyte (aka Mustang Panda or Bronze President) APT campaign, which uses a kernel-mode rootkit to deliver and protect a ToneShell backdoor.

Kaspersky GReAT experts analyze the Evasive Panda APT's infection chain, including shellcode encrypted with DPAPI and RC5, as well as the MgBot implant.

Kaspersky expert describes new malicious tools employed by the Cloud Atlas APT, including implants of their signature backdoors VBShower, VBCloud, PowerShower, and CloudAtlas.
