

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

SL securelist.com/lofy-life-malicious-npm-packages/107014



[Incidents](#)



[Incidents](#)

28 Jul 2022

minute read



Authors

-  Igor Kuznetsov
-  Leonid Bezvershenko

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:

```
pio 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](#).

- [Data theft](#)
- [JavaScript](#)
- [Malware Descriptions](#)
- [Node.js](#)
- [Open source](#)

Authors

-  [Igor Kuznetsov](#)
-  [Leonid Bezvershenko](#)

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

Your email address will not be published. Required fields are marked *

GReAT webinars

13 May 2021, 1:00pm

GReAT Ideas. Balalaika Edition

26 Feb 2021, 12:00pm

GReAT Ideas. Green Tea Edition

17 Jun 2020, 1:00pm

GReAT Ideas. Powered by SAS: malware attribution and next-gen IoT honeypots

From the same authors



Two more malicious Python packages in the PyPI



OpenTIP, command line edition



BloodyStealer and gaming assets for sale



Sunburst: connecting the dots in the DNS requests

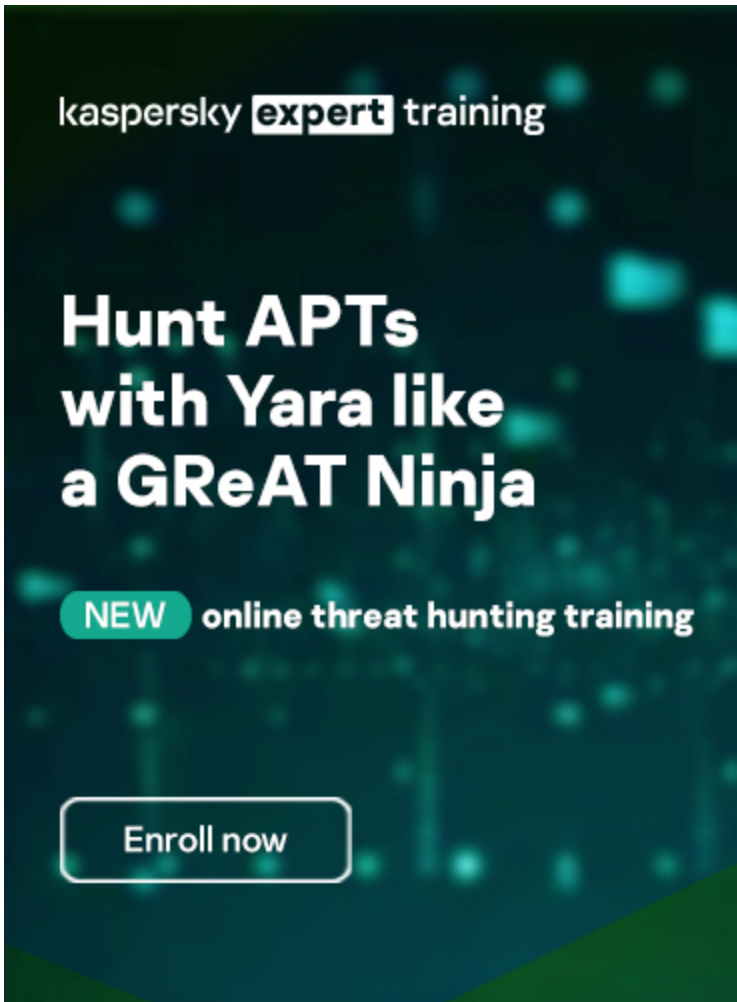


What does it take to become a good reverse engineer?

Subscribe to our weekly e-mails

The hottest research right in your inbox

-
-
-



Reports

Kimস্যuky's GoldDragon cluster and its C2 operations

Kimস্যuky (also known as Thallium, Black Banshee and Velvet Chollima) is a prolific and active threat actor primarily targeting Korea-related entities. In early 2022, we observed this group was attacking the media and a think-tank in South Korea.

VileRAT: DeathStalker's continuous strike at foreign and cryptocurrency exchanges

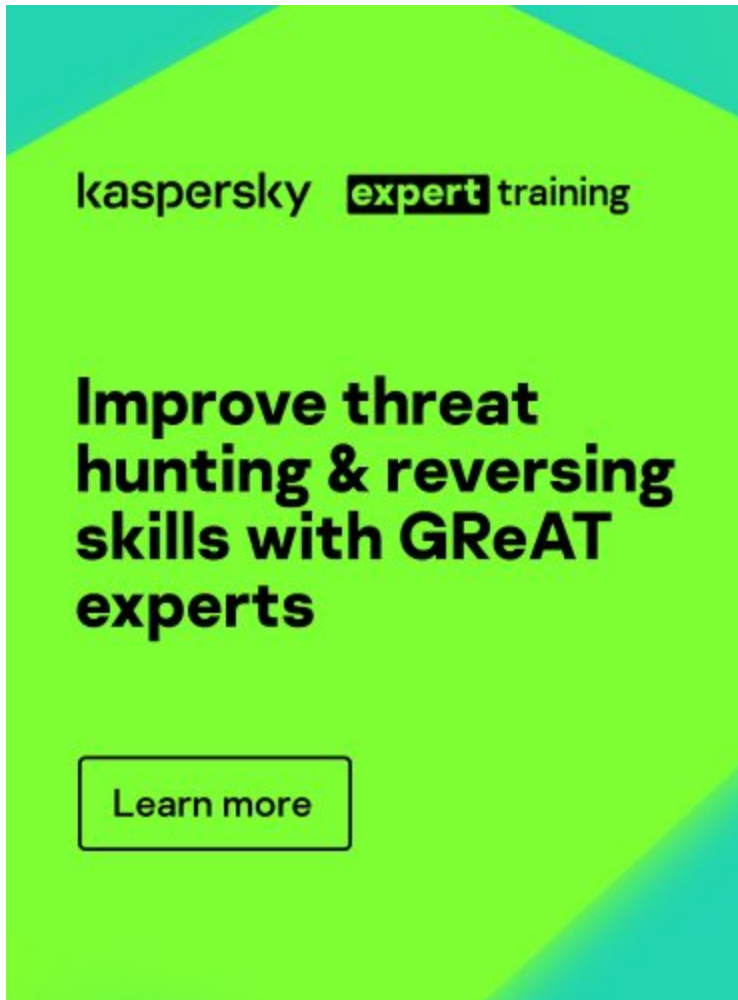
VileRAT is a Python implant, part of an evasive and highly intricate attack campaign against foreign exchange and cryptocurrency trading companies.

Andariel deploys DTrack and Maui ransomware

Earlier, the CISA published an alert related to a Stairwell report, "Maui Ransomware." Our data should openly help solidify the attribution of the Maui ransomware incident to the Korean-speaking APT Andariel, also known as Silent Chollima and Stonefly.

Targeted attack on industrial enterprises and public institutions

Kaspersky ICS CERT experts detected a wave of targeted attacks in several East European countries, as well as Afghanistan. Of the six backdoors identified on infected systems, five have been used earlier in attacks attributed to APT TA428.

A promotional banner for Kaspersky expert training. The background is a vibrant green with teal accents in the corners. At the top left, the text 'kaspersky expert training' is displayed, with 'expert' in a black box. The main headline reads 'Improve threat hunting & reversing skills with GReAT experts'. At the bottom, there is a white button with a black border that says 'Learn more'.

Subscribe to our weekly e-mails

The hottest research right in your inbox

-
-
-

kaspersky **expert** training

Improve threat hunting & reversing skills with GReAT experts

[Learn more](#)