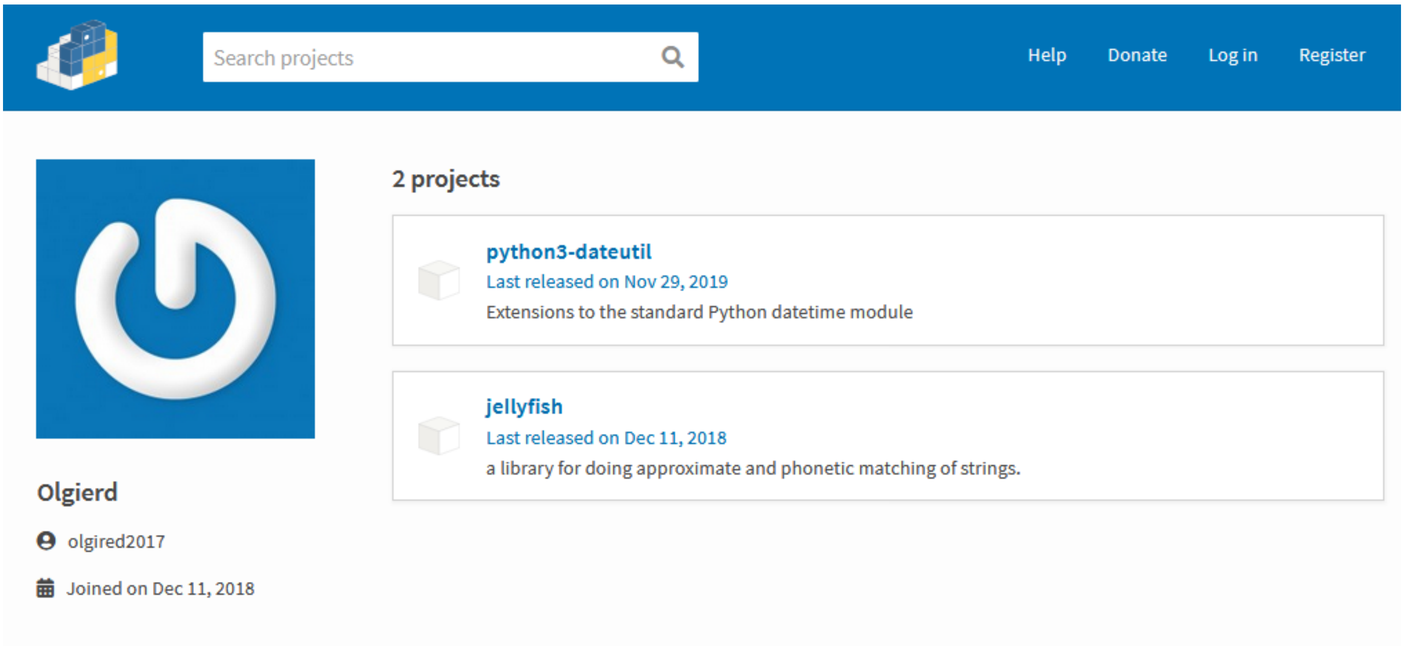
MUST READ: FBI recommends that you keep your IoT devices on a separate network

Two malicious Python libraries caught stealing SSH and GPG keys

One library was available for only two days, but the second was live for nearly a year.

By Catalin Cimpanu for Zero Day | December 4, 2019 -- 00:52 GMT (16:52 PST) | Topic: Security



2 projects

python3-dateutil
Last released on Nov 29, 2019
Extensions to the standard Python datetime module

jellyfish
Last released on Dec 11, 2018
a library for doing approximate and phonetic matching of strings.

Olgierd
olgired2017
Joined on Dec 11, 2018

Image: ZDNet

The Python security team removed two trojanized Python libraries from PyPI (Python Package Index) that were caught stealing SSH and GPG keys from the projects of infected developers.

The two libraries were created by the same developer and mimicked other more popular libraries -- using a technique called typosquatting to register similarly-looking names.

The first is "python3-dateutil," which imitated the popular "dateutil" library. The second is "jeIlyfish" (the first L is an I), which mimicked the "jellyfish" library.

The two malicious clones were discovered on Sunday, December 1, by German software developer Lukas Martini. Both libraries were removed on the same day after Martini notified dateutil developers and the PyPI security team.

While the python3-dateutil was created and uploaded on PyPI two days before, on November 29, the jeIlyfish library had been available for nearly a year, since December 11, 2018.

STEALING SSH AND GPG KEYS

According to Martini, the malicious code was present only in the jeIlyfish library. The python3-dateutil package didn't contain malicious code of its own, but it did import the jeIlyfish library, meaning it was malicious by association.

The code downloaded and read a list of hashes stored in a GitLab repository. The nature and purpose of these hashes was initially unknown, as neither Martini or the PyPI team detailed the behavior in great depth before the library was promptly removed from PyPI.

ZDNet asked today Paul Ganssle, a member of the dateutil dev team, to take a closer look at the malicious code and put it in perspective for our readers.

"The code directly in the `jeIlyfish` library downloads a file called 'hashsum' that looks like nonsense from a gitlab repo, then decodes that into a Python file and executes it," Ganssle told *ZDNet*.

"It looks like [this file] tries to exfiltrate SSH and GPG keys from a user's computer and send them to this IP address: **http://68.183.212.246:32258**."

"It also lists a bunch of directories, home directory, PyCharm Projects directory," Ganssle added. "If I had to guess what the purpose of that is, I would say it's to figure out what projects the credentials work for so that the attacker can compromise that person's projects."

DEVELOPERS ADVISED TO REVIEW PROJECTS

Both of the malicious libraries were uploaded on PyPI by the same developer, who used the username of olgired2017 -- also used for the GitLab account.

It is believed that olgired2017 created the dateutil clone in an attempt to capitalize on the original's library popularity and increase the reach of the malicious code; however, this also brought more attention from more developers and eventually ended up in exposing his entire operation.

Excluding the malicious code, both typosquatted packages were identical copies of the original libraries, meaning they would have worked as the originals.

Developers who didn't pay attention to the libraries they downloaded or imported into their projects should check to see if they've used the correct package names and did not accidentally use the typosquatted versions.

If they accidentally used any of the two, developers are advised to change the all SSH and GPG keys they've used over the past year.

This is the third time the PyPI team intervenes to remove typo-squatted malicious Python libraries from the official repository. Similar incidents have happened in September 2017 (ten libraries), October 2018 (12 libraries), and July 2019 (three libraries).

Article updated one hour after publication with Ganssle's analysis.

What's in a name? These DevOps tools come...

SEE FULL GALLERY

1 - 4 of 23

NEXT >

DEVELOPER

Good news for developers: The CLI is back

Windows 10 1909: What do developers need to know? Not much, says Microsoft

Qualtrics extends developer platform, adds integration partners

Introducing STEAM to kids through sports (ZDNet YouTube)

The Best Web Hosting Providers for 2019 (CNET)

How to get a developer job (TechRepublic)

RELATED TOPICS: OPEN SOURCE SECURITY TV DATA MANAGEMENT CXO DATA CENTERS

By Catalin Cimpanu for Zero Day | December 4, 2019 -- 00:52 GMT (16:52 PST) | Topic: Security

TECHREPUBLIC PREMIUM

Special report: Blockchain in business: Where are we now, and predictions for the next decade

Microsoft Ignite 2019: Azure Arc, HoloLens 2, Edge, Quantum and Teams

Year-round IT budget template

Digital Transformation ebook: Guide to becoming a digital transformation champion

TechRepublic Premium: Network documentation checklist

Quick Glossary: Storage area network (SAN)

Technical documentation policy

Quick glossary: Network attached storage

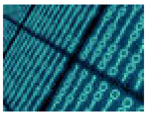
SHOW COMMENTS

MORE FROM CATALIN CIMPANU

Security
Reddit links leak of US-UK trade documents to Russian influence campaign

Security
BMW and Hyundai hacked by Vietnamese hackers, report claims

Security
FBI recommends that you keep your IoT devices on a separate network


Security
New vulnerability lets attackers sniff or hijack VPN connections

NEWSLETTERS

ZDNet Security

Your weekly update on security around the globe, featuring research, threats, and more.

Your email address

SUBSCRIBE

SEE ALL

MORE RESOURCES

IBM: Visually Build AI and Machine Learning Models

White Papers from IBM

READ NOW

IBM: Scaling Data Science: How Best in Class Companies Innovate with Machine Learning

White Papers from IBM

READ NOW

8x8's Enterprise Engagement Management Platform: Moving Toward an Integrated Approach

White Papers from 8x8, Inc.

READ NOW

RELATED STORIES

1 of 3

Reddit links leak of US-UK trade documents to Russian influence campaign

Reddit bans 61 accounts and one subreddit for "misuse of the platform."

BMW and Hyundai hacked by Vietnamese hackers, report claims

Hacks linked to Ocean Lotus (APT32), a group believed to operate with orders from the Vietnamese government.

These are the worst hacks, cyberattacks, and data breaches of 2019

A slew of hacks, data breaches, and attacks tainted the cybersecurity landscape in 2019.