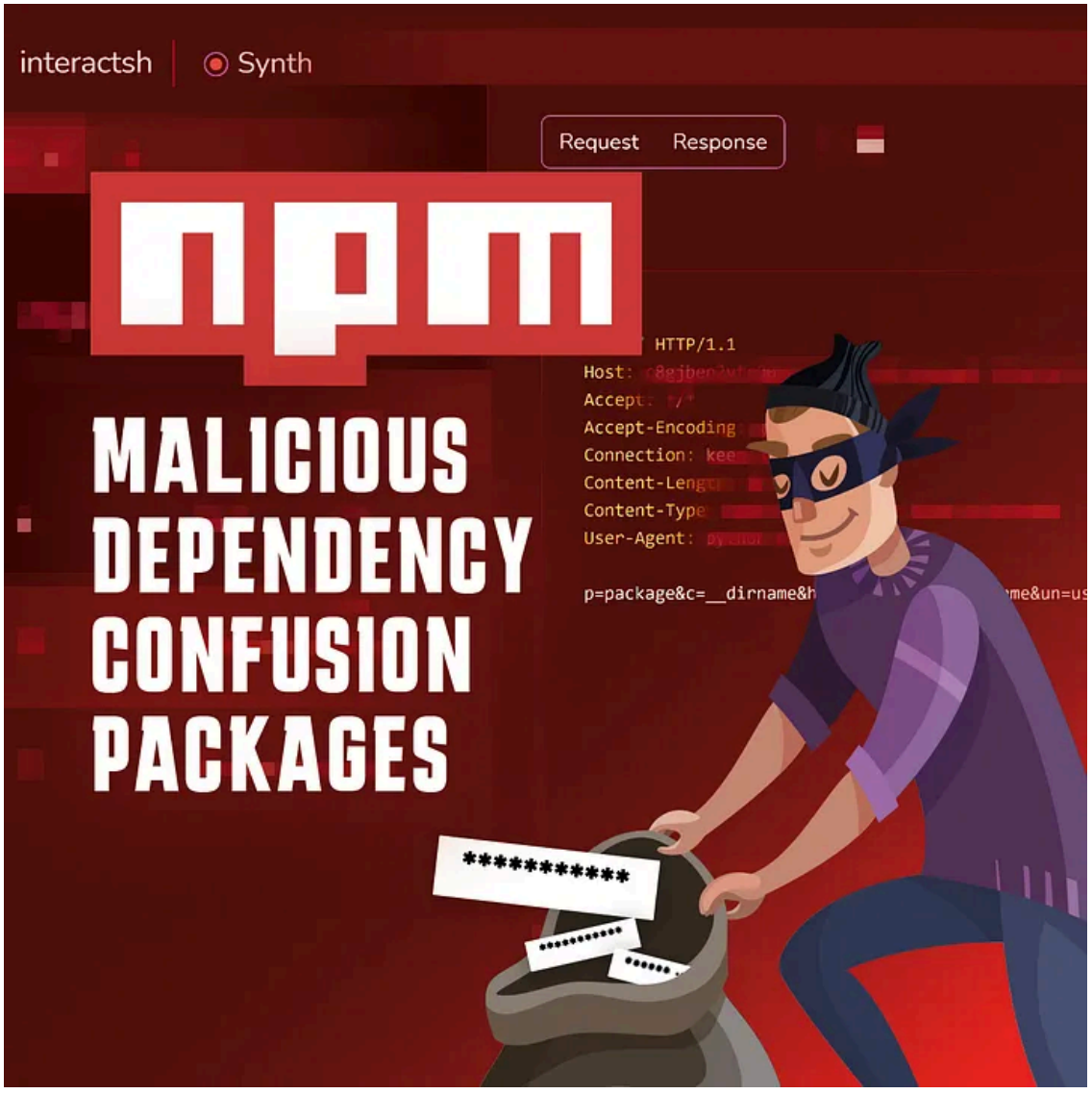
Webhook Party — Malicious packages caught exfiltrating data via legit webhook services

By Jossef Harush Kadouri

Published: 2022-03-07 · Archived: 2026-04-05 18:12:09 UTC

Press enter or click to view image in full size

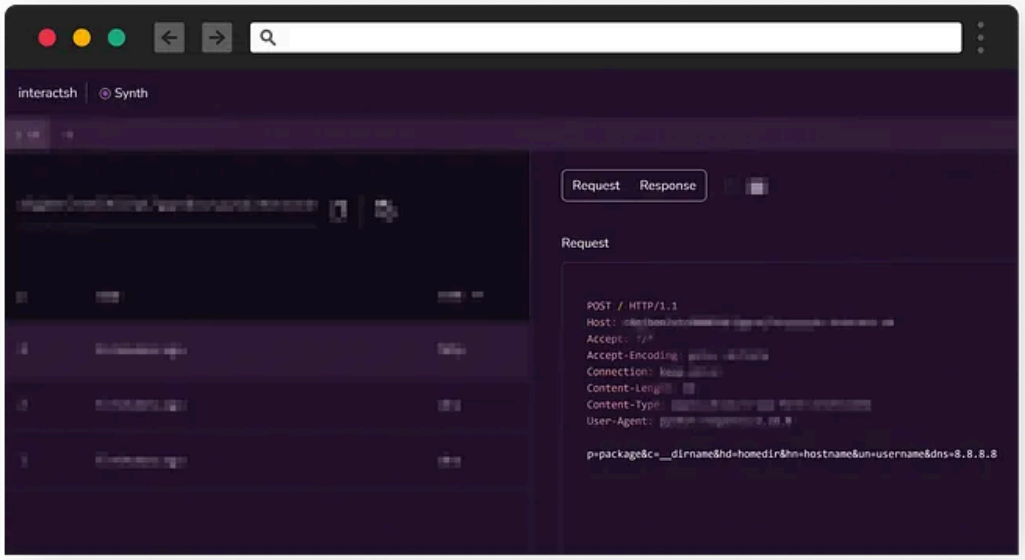


Checkmarx Supply Chain Security (SCS) team (previously Dustico) has found several malicious packages attempting to use a dependency confusion attack. Those packages were detected by the team's malicious package detection system. Findings show all packages caught contained malicious payload which is using legitimate SaaS services for data exfiltration. This behavior is part of an alarming trend we are seeing in recent attacks.

Details

Let us start with the NPM packages ‘azureazure’ and ‘azure-sdk-v4’. Those two packages both include the description “azure whitehat package” but still collect sensitive system information and exfiltrate it to address “425a2.rt11[.]ml”. After some digging, we linked this address to the webhook service https://interactsh.com/ which provides a simple and free way to implement endpoint to this kind of attack.

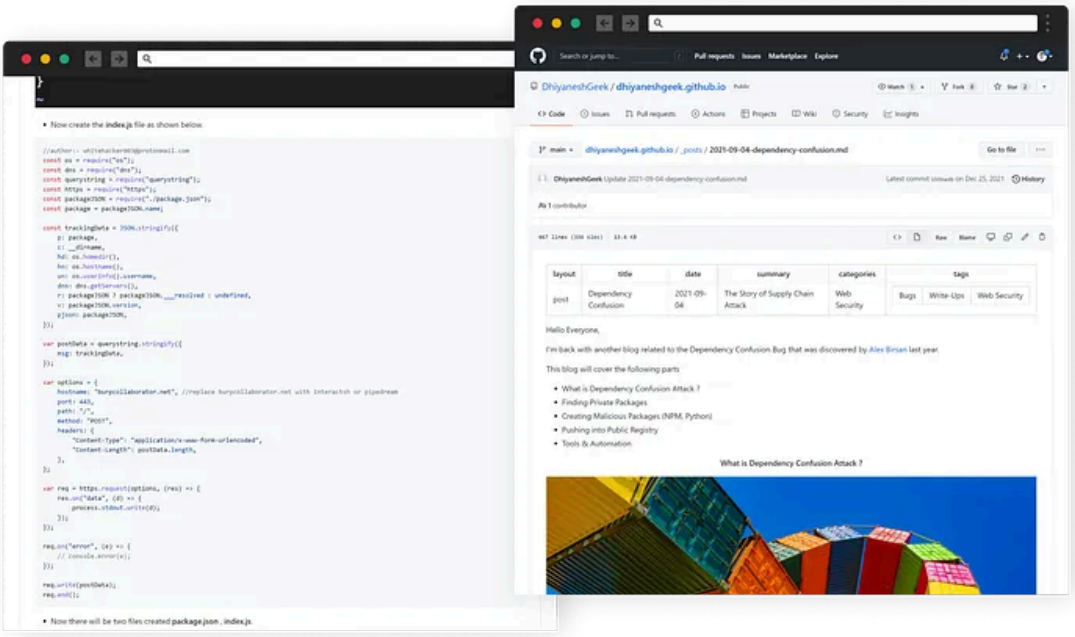
Press enter or click to view image in full size



User interface of the ‘interactsh’ service — this is how the collected data is displayed to the attacker

Looking more closely at the code, we encountered a few revealing comments that were enough to link the code in this package to a tutorial explaining dependency confusion attacks and providing code snippets that can be used while implementing this technique.

Press enter or click to view image in full size



a tutorial explaining dependency confusion attacks and providing code snippets

The code in the packages we found closely resembled the code snippets in the tutorial other than the fact that the uploader decides to add two more functionalities to it:

- enumerate the files in a list of interesting paths [C:\, D:\, /, /home]
- retrieving the external IP address

Code Obfuscation

Other than the additional features, it seems like the person behind these packages is testing further concepts and so we found the next two NPM packages that were likely to come from them: ‘glints-sdk’ and ‘azure-sdk-v3’.

Get Jossef Harush Kadouri’s stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

These two packages deliver a similar code to the victim only in an obfuscated form:

As a part of the automatic malware detection system developed by Checkmarx SCS team, the packages are being dynamically analyzed in several sub-engines, and in these cases, the results of the analysis for all four packages mentioned above included network communicates with the address (hxxps://425a2.rt11[.]ml). This implies that ‘glints-sdk’ and ‘azure-sdk-v3’ are made by the same attacker.

Cross Platform Attack

Around the same time, Checkmarx’s system has detected another package, this time it was published on PyPi. The user ‘azureazure’ (with the display name ‘Kareem’) published a Python package ‘azureazure’. Looking at the code

we found similar functionalities to its JavaScript counterpart, including gathering system information and exfiltrating it to the same address (hxxps://425a2.rt11[.]ml). in addition to these, the Python code also included data exfiltration through DNS tunneling.

We believe those packages published by the same actor, we found more NPM packages all contain similar malicious payload which exfiltrate host information to the free SaaS services ‘burpcollaborator.net’ and ‘pipedream.net’.

Webhook as a C&C Server

The usage of these legitimate free services by all those malicious packages corresponds with an interesting trend — we are witnessing in which actor are utilizing “out of the box” solutions for the backend infrastructure of their attacks. Free SaaS services such as the examples listed below provide an effortless way to get up and running, with an endpoint ready to go in a matter of seconds, to which the exfiltrated data will be collected:

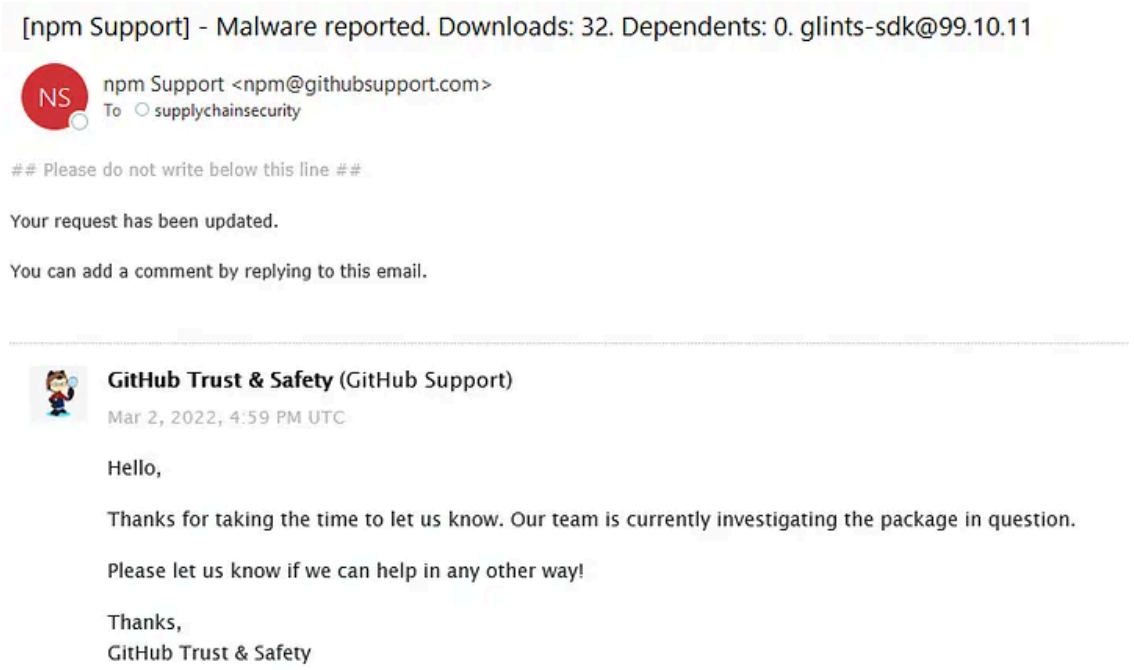
- https://pipedream.com/
- https://burpcollaborator.net/
- https://app.interactsh.com/
- https://webhook.site/
- Messaging services such as Discord, Telegram, etc.

Aside from the ease of using these services instead of building and deploying a dedicated server, this technique has one more important outcome. In case of a successful infection, network traffic to these services will not raise red flags to defenders for they are legitimate and can be used for legitimate purposes. The combination of TLS encrypted traffic with the usage of known and legitimate sites makes it even harder for defenders to identify sensitive information being exfiltrated from their networks.

Press enter or click to view image in full size

While few packages did state a “whitehat” disclaimer, they still send data from the victim’s machine into the attacker’s endpoint. We reported all malicious packages to NPM and PyPi security teams, and most of the packages were rapidly removed from the registry.

Press enter or click to view image in full size



an example of one of the reports sent to npm

IOCs

- 425a2.rt11[.]ml
- gxh1p4cmhshj6na8ds6zue6s6jcb00.burpcollaborator[.]net
- hxxps://grabify[.]link/YXP9CJ
- enjg65nwg4r8o28.m.pipedream[.]net

Conclusion

This is one of several types of malicious packages that the Checkmarx Supply Chain Security (SCS) team (previously Dustico) is discovering in the wild. We'll continue to report on our findings here in this blog, so stay tuned.

Read the full story on Checkmarx Blog
