Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

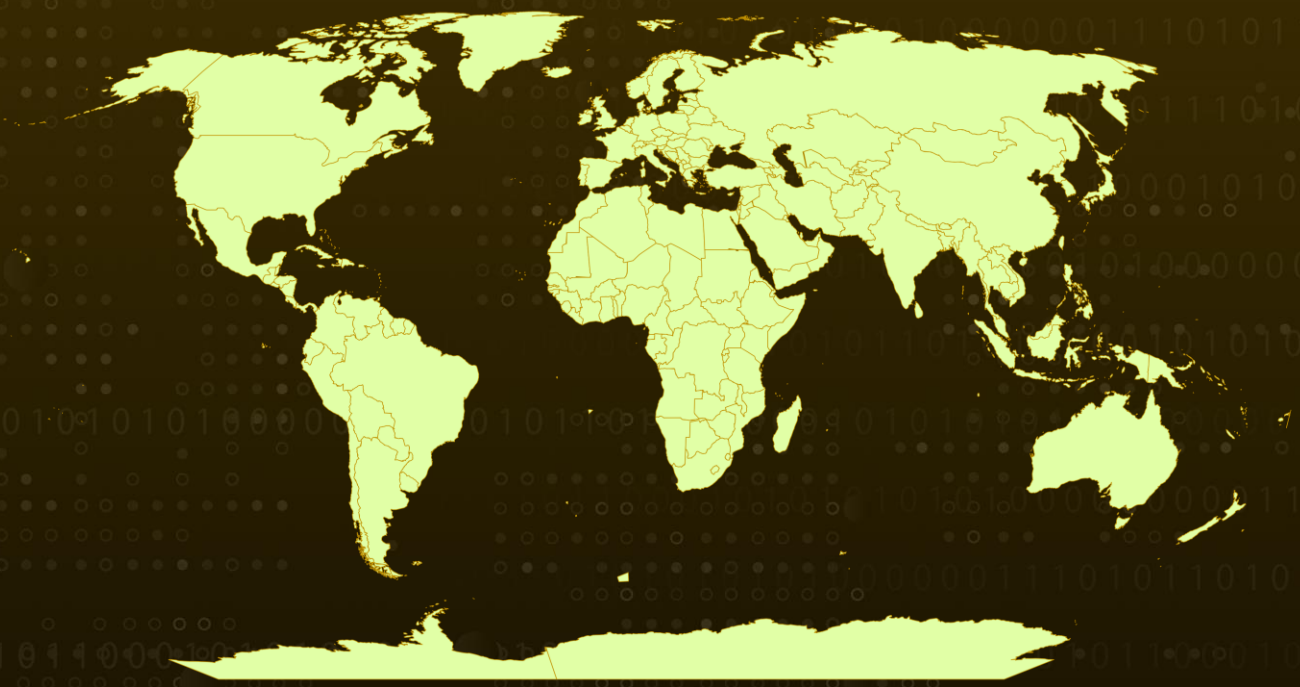
Millions of Github Repositories susceptible to Repojacking

Date of Publication	Admiralty Code	TA Number
June 26, 2023	A1	TA2023279

Summary

First appeared: October, 2020
Attack Region: Worldwide
Targeted Industries: Technology Companies
Attack: Millions of GitHub repositories may be vulnerable to Repojacking, which could lead to large-scale supply chain attacks.

Attack Regions



Attack Details

#1 Github permits users and organizations to change their name, establishing a static link that automatically redirects resource requests from the old name to the new name. However, Github allows individuals to register using the old name, subject to certain limitations, which may lead to a scenario of dependency hijacking.

#2 Repojacking, also known as repository hijacking, is an attack method where hackers take control of GitHub projects to execute malicious code. In this scenario, the attacker registers using an old name and hosts malicious code. Consequently, dependent projects unwittingly incorporate the malicious code into their own products, enabling adversaries to scale their attacks and infect numerous applications.

#3 This easily exploitable vulnerability allows for remote code injection and impacts significant projects from prominent companies such as Google, GitHub, Facebook, Kubernetes, NodeJS, Amazon, and more. It affects everything, from web frameworks to cryptocurrencies.

#4 Github does not allow name changing for projects having more than 100 clones. However, it still leaves millions of repo and other popular repos which use small repos, susceptible to Repojacking.

Recommendations

Avoid Direct Dependency Public Link: Download all project dependencies and make it available with local package manager or other with local resource library.

Keep Watch on Project dependencies: List all dependencies, verify their source and ensure they are referred from well-known and trusted sources.

Own the Old Name: If you change the organization name, ensure that you still own the previous name to avoid attackers from misusing it.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0040 Impact
T1593 Search Open Websites and Domains	T1593.003 Code Repositories	T1608 Stage Capabilities	T1608.004 Drive-by Target
T1195 Supply Chain Compromise	T1195.001 Compromise Software Dependencies and Development Tools		

References

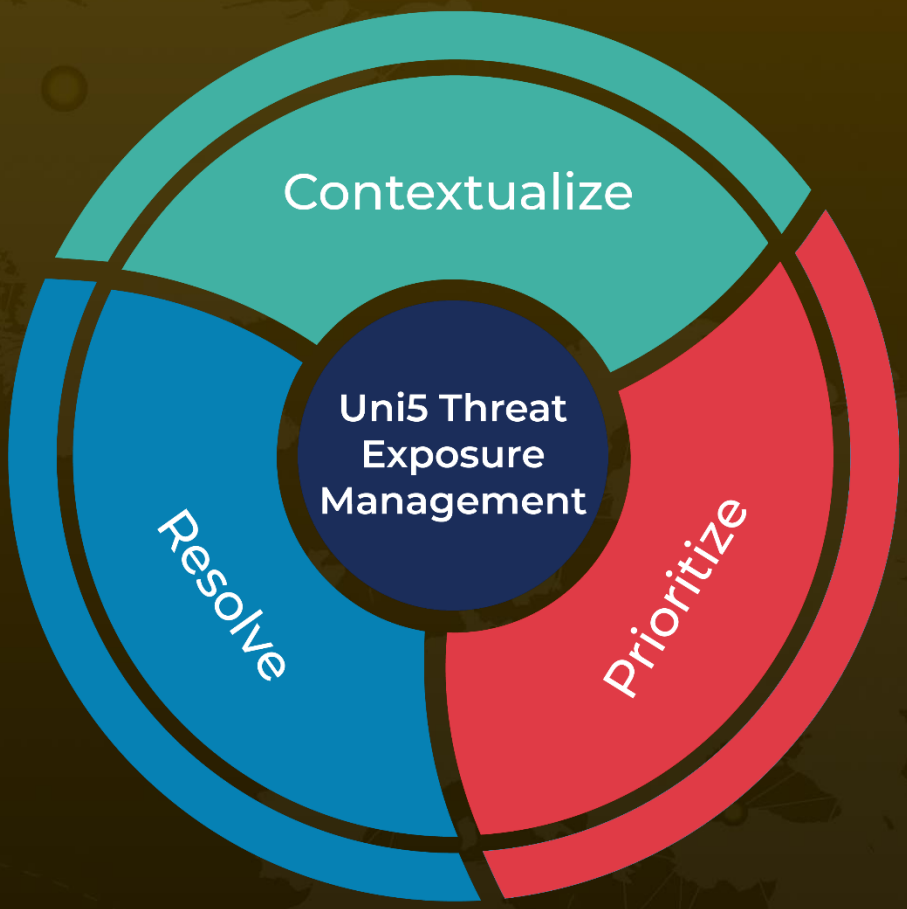
https://blog.aquasec.com/github-dataset-research-reveals-millions-potentially-vulnerable-to-repojacking

https://github.blog/2018-04-18-new-tools-for-open-source-maintainers/#popular-repository-namespace-retirement

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

June 26, 2023 • 06:30 AM

More at www.hivepro.com