Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

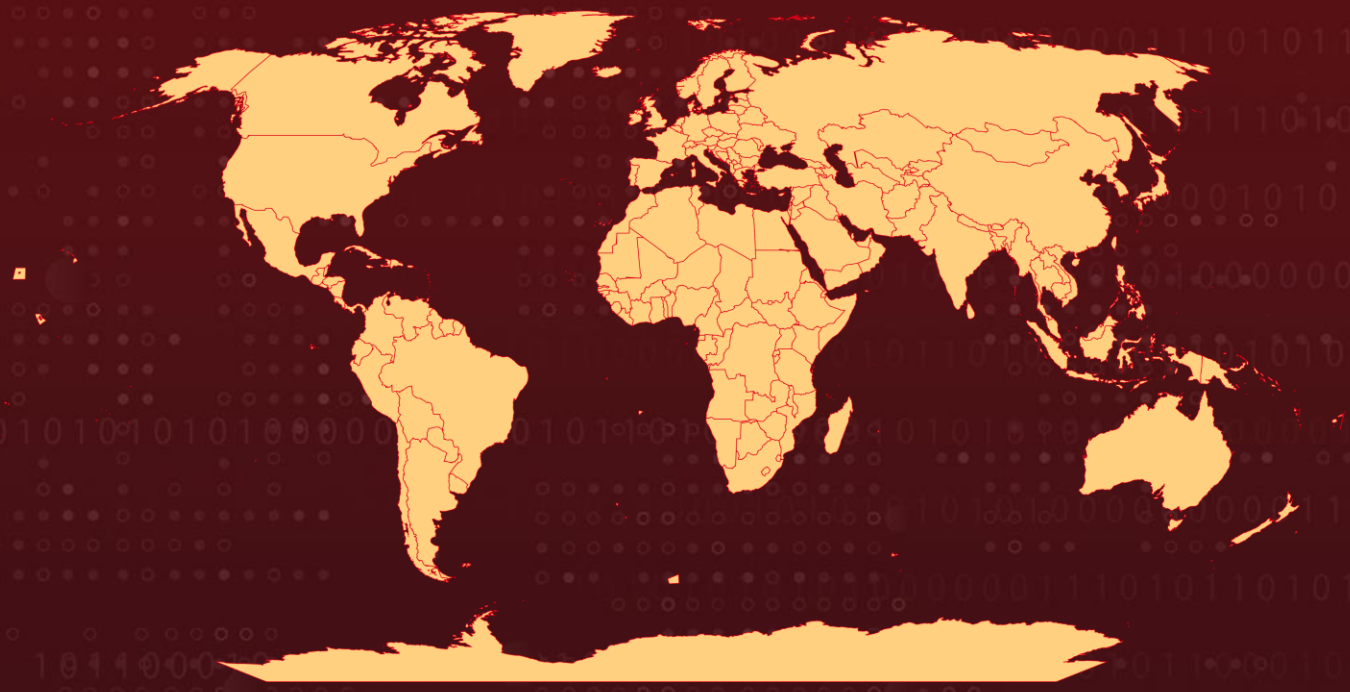
Over 2 Million Malicious Repositories Planted on Docker Hub

Date of Publication	Admiralty Code	TA Number
May 2, 2024	A1	TA2024169

Summary

Attack Began: Early 2021
Attack Region: Worldwide
Attack: Since the start of 2021, Docker Hub users have faced three significant campaigns, each disseminating millions of repositories containing malware and phishing sites. These campaigns utilized distinct strategies for creating and distributing the malicious repositories. The "Website SEO" campaign focused on establishing a few fake repositories daily, with each repository associated with a single user. In contrast, the "Downloader" and "eBook Phishing" initiatives opted for bulk creation of false repositories.

Attack Regions



Attack Details

#1 The discovery of millions of empty repositories on Docker Hub has raised concerns about the platform's vulnerability to exploitation by malicious actors. These repositories, devoid of images and content, serve as fertile ground for various fraudulent activities, including phishing scams and malware distribution. Despite efforts to moderate the platform, Docker Hub remains a target for cybercriminals seeking to exploit its community-oriented nature and large user base.

#2 Several malicious campaigns have been identified targeting Docker Hub users, with the most notable being the "Downloader," "eBook Phishing," and "Website SEO" initiatives. These campaigns employ different tactics to deceive users and lure them into visiting fraudulent websites or downloading malicious software.

#3 The "Downloader" campaign operates in two phases, utilizing URL shorteners and legitimate resources as redirects to malicious sources. It aims to evade detection by constantly changing its tactics and leveraging widely used platforms such as Google and Blogger. The malware distributed by this campaign prompts users to download and install advertised software, but instead, it clandestinely downloads multiple malicious programs onto the infected machine.

#4 The "eBook Phishing" campaign floods Docker Hub with spam repositories masquerading as a "pirated eBook library." These repositories offer free eBook downloads but redirect users to phishing websites soliciting credit card information. Despite featuring barely-legible subscription costs in the footer, these deceptive sites aim to trick users into divulging sensitive financial information.

#5 In contrast, the "Website SEO" campaign focuses on generating innocuous content with a random username pattern. Although these repositories lack malicious content, they serve as a potential testing ground for more nefarious campaigns in the future. By exploiting Docker Hub's platform credibility, attackers aim to evade detection and distribute malicious content under the guise of harmless repositories.

#6 The prevalence of malicious activities on Docker Hub underscores the importance of ongoing moderation and vigilance. Despite the platform's efforts to mitigate abuse, the sheer volume of malicious repositories highlights the persistent challenges faced in maintaining platform security. As Docker Hub remains a popular platform for developers and organizations, it is crucial to remain vigilant and implement robust security measures to mitigate the risks posed by malicious actors.

Recommendations

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0011 Command and Control
T1566 Phishing	T1071 Application Layer Protocol	T1053 Scheduled Task/Job	T1195 Supply Chain Compromise
T1036 Masquerading	T1059 Command and Scripting Interpreter	T1102 Web Service	T1190 Exploit Public-Facing Application
T1525 Implant Internal Image	T1027 Obfuscated Files or Information	T1189 Drive-by Compromise	T1057 Process Discovery
T1608 Stage Capabilities	T1608.006 SEO Poisoning	T1555 Credentials from Password Stores	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	failhostingpolp[.]ru, gts794[.]com, blltly[.]com, ltlly[.]com, byltly[.]com, bytlly[.]com, cinurl[.]com, fancli[.]com, geags[.]com, gohhs[.]com, imgfil[.]com, jinyurl[.]com, miimms[.]com, picfs[.]com, shoxet[.]com, shurll[.]com, ssurll[.]com, tinourl[.]com, tinurli[.]com, tinurll[.]com, tiurll[.]com, tlniurl[.]com, tweeat[.]com, urlca[.]com, urlcod[.]com, urlgoal[.]com, urllie[.]com, urllio[.]com, urloso[.]com, urluso[.]com, urluss[.]com, vittuv[.]com, rd[.]lesac[.]ru, soneservice[.]shop

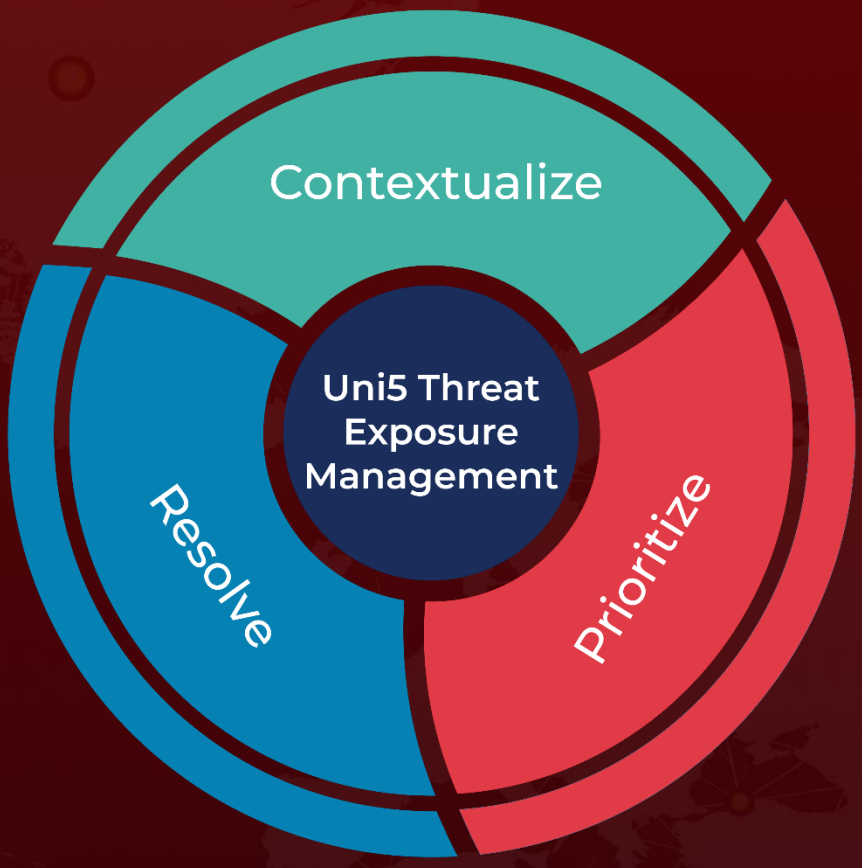
References

https://jfrog.com/blog/attacks-on-docker-with-millions-of-malicious-repositories-spread-malware-and-phishing-scams/

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

May 2, 2024 • 5:30 AM

More at www.hivepro.com