Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

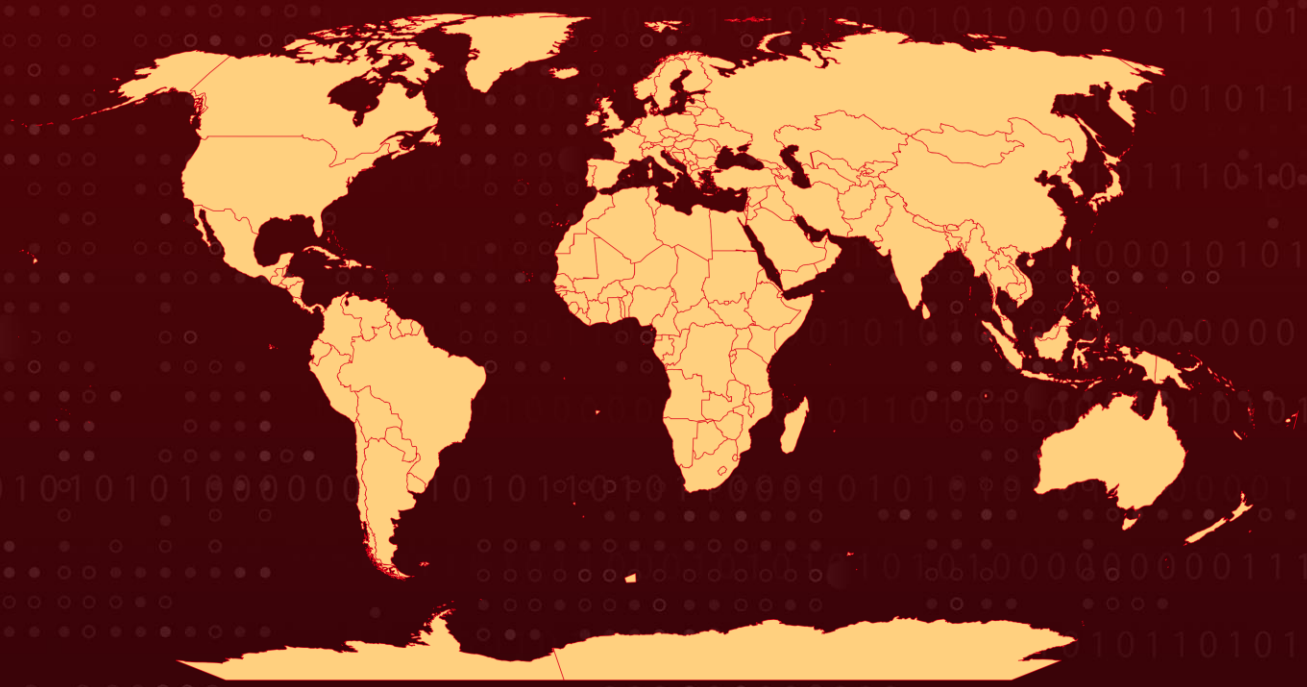
Over 170K Users Hit by Fake Python Infrastructure

Date of Publication	Admiralty Code	TA Number
April 5, 2024	A1	TA2024130

Summary

Attack Commenced: 2024
Attack Region: Worldwide
Attack: An unidentified group of threat actors orchestrated a supply chain attack, aiming at members of the Top[.]gg GitHub organization and individual developers. Their main goal was to inject malicious code into the code ecosystem. As a result, the attackers successfully impacted over 170,000 users by introducing malicious dependencies through a fabricated Python infrastructure linked to GitHub projects.

Attack Regions



Attack Details

#1 An unidentified group of threat actors orchestrated a sophisticated supply chain cyberattack targeting members of the Top[.]gg GitHub organization and individual developers. They aimed to inject malicious code into the code ecosystem, specifically focusing on the software supply chain.

#2 This focus is evidenced by the successful exploitation of numerous victims, impacting over 170,000 users through the introduction of malicious dependencies via a fabricated Python infrastructure associated with GitHub projects.

#3 The threat actors employed a variety of techniques in their attacks, including account takeover via pilfered browser cookies, establishment of a customized Python mirror, and distribution of malicious packages through the PyPi registry.

#4 To deceive victims, the threat actors plotted multiple malicious open-source tools with enticing descriptions, likely to lure unsuspecting users through search engine results. The malicious payload was executed in stages, extracting credentials, and other valuable data from infected systems, which were then sent to the attackers' infrastructure.

#5 They also established a counterfeit Python package mirror, successfully deploying a tainted version of the popular "Colorama" package, which is used by over 150 million users to streamline text formatting processes. By concealing malicious code within seemingly legitimate software, the attackers broadened their impact beyond GitHub repositories.

#6 In the final phase of the attack, the malware pilfered sensitive information on prominent user platforms such as web browsers with a focus on acquiring cookies, autofill data, and credentials. Additionally, the malware targeted Discord accounts, exploiting decrypted tokens to gain unauthorized access.

#7 The malware was also capable of stealing victims' cryptocurrency wallets, Telegram session data, and Instagram profile information. The data extracted from these attacks was subsequently transferred to the attacker's server using various methods, including anonymous file-sharing services and HTTP requests.

Recommendations

Static and Dynamic Code Analysis: Conduct regular static and dynamic code analysis to identify and remediate security vulnerabilities, including potential backdoors, injection flaws, and insecure dependencies.

Network Segmentation: Implement network segmentation to minimize the lateral movement of attackers within the network, limiting their ability to access critical systems and data.

Zero Trust Architecture: Adopt a Zero Trust security architecture, where trust is never assumed and continuous authentication and authorization mechanisms are implemented, reducing the risk of unauthorized access.

Code Signing: Implement code signing mechanisms to verify the authenticity and integrity of software components and dependencies, ensuring that only trusted code is executed within the environment.

Software Composition Analysis (SCA): Utilize SCA tools to scan and analyze third-party dependencies and libraries for known vulnerabilities and security flaws before integration into the codebase.

Enhancing Code Integrity: Implementing a strict code merge policy is crucial for maintaining code clarity and preventing the integration of obfuscated code into the master branch. Additionally, it's important to avoid merging pre-compiled unknown objects to maintain transparency and ensure that only trusted code components are integrated, thereby reducing the risk of vulnerabilities or malicious code.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0007 Discovery	TA0040 Impact	TA0011 Command and Control
TA0010 Exfiltration	T1195 Supply Chain Compromise	T1190 Exploit Public-Facing Application	T1212 Exploitation for Credential Access

T1059 Command and Scripting Interpreter	T1059.006 Python	T1036 Masquerading	T1027 Obfuscated Files or Information
T1027.002 Software Packing	T1005 Data from Local System	T1105 Ingress Tool Transfer	T1056.001 Keylogging
T1056 Input Capture	T1082 System Information Discovery	T1555.003 Credentials from Web Browsers	T1555.005 Password Managers

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps[:]//files[dot]pythanhosted[dot]org/packages/d8/53/6f443c9a4a8358a93a6792e2acffb9d9d5cb0a5cfd8802644b7b1c9a02e4/colorama-0.4.5[dot]tar[dot]gz, hxxps[:]//files[dot]pypihosted[dot]org/packages/d8/53/6f443c9a4a8358a93a6792e2acffb9d9d5cb0a5cfd8802644b7b1c9a02e4/coloramа-0.4.6[dot]tar[dot]gz, hxxps[:]//files[dot]pypihosted[dot]org/packages/d8/53/6f443c9a4a8358a93a6792e2acffb9d9d5cb0a5cfd8802644b7b1c9a02e4/coloramа-0.4.3[dot]tar[dot]gz
IPv4	162[.]248[.]101[.]215, 162[.]248[.]100[.]217, 162[.]248[.]100[.]117
Domain	pypihosted[.]org/version
SHA256	0c1873196dbd88280f4d5cf409b7b53674b3ed85f8a1a28ece9caf2f98a71207, 35ac61c83b85f6ddcf8ec8747f44400399ce3a9986d355834b68630270e669fb, c53b93be72e700f7e0c8d5333acd68f9dc5505fb5b71773ca9a8668b98a17ba8

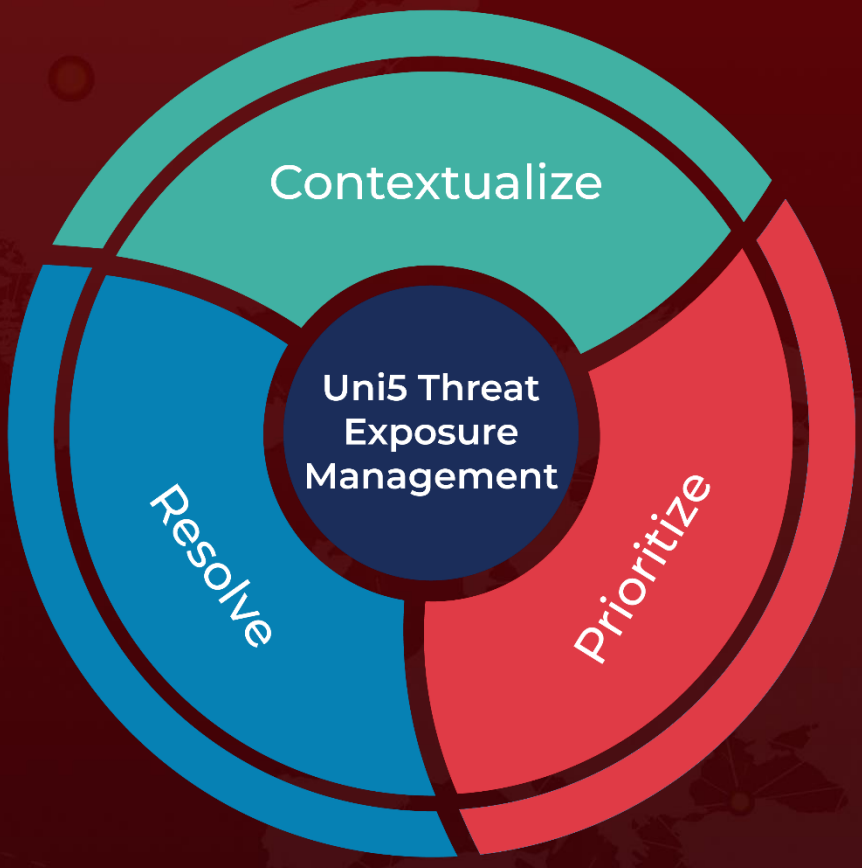
References

https://checkmarx.com/blog/over-170k-users-affected-by-attack-using-fake-python-infrastructure/

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

April 5, 2024 • 4:30 AM

More at www.hivepro.com