GitHub's search functionality to distribute Malware

Date: 13th April 2024 | Severity: High

Summary

Threat actors are exploiting GitHub's search functionality to distribute malware by creating malicious repositories disguised as popular projects. They manipulate search rankings and use fake stars to deceive users into downloading their repositories.

Malicious code is concealed within Microsoft Visual Code project files to download malware from remote URLs. Some repositories download encrypted files containing large executables to evade detection, ultimately launching malware capable of diverting cryptocurrency transactions.

Checkmarx highlights the need for developers to exercise caution when downloading from open-source repositories, as relying solely on reputation is insufficient. Additionally, there's been an uptick in spam packages on the npm registry, suggesting a broader trend of exploiting open-source ecosystems for malicious purposes.

Attack Vectors

- Manipulation of GitHub Search Rankings: Threat actors manipulate GitHub's search functionalityto ensure their malicious repositories appear at the top of search results, enticing unsuspecting users looking for popular projects.
- Creation of Malicious Repositories: Attackers create repositories with names and topics like popular projects, adding a veneer of legitimacy to their malicious activities.
- Fake Stars: By using automated techniques or fake accounts, attackers artificially inflate the star ratings of their malicious repositories, further enhancing their perceived legitimacy and visibility.
- Concealment of Malicious Code: Malicious code is hidden within Microsoft Visual Code project files, making it difficult for users to detect the presence of malware upon downloading the repository.
- Download of Next-Stage Payloads: The concealed malicious code within the repositories is designed to download additional malware payloads from remote URLs, potentially executing harmful actions on the victim's system.
- Large File Sizes to Evade Detection: Some repositories download encrypted files containing large executables, such as "feedbackAPI.exe" inflated to 750 MB. This tactic aims to evade antivirus scanning and increase the chances of successful malware execution.

- Distribution through Popular Topics: Malicious repositories are disguised as legitimate projects related to popular games, cheats, and tools, exploiting users' interest in these topics to increase the likelihood of repository downloads.
- Exploitation of Open-Source Ecosystems: The attackers exploit the open-source ecosystem, leveraging platforms like GitHub and npm registry to distribute malware and conduct malicious activities.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• cc9d54b78688ef6f41e4f4d0c8bced3e04bfcedc • 5f4ea58b58997f01f8001d790d970e12 • 95712a831f3694f4388d12f0149e675f • 9f45e1c9f94bdd9dfee166709ec1a465
Domain/URL	• hxxps[:]//paste[.]fo/raw/dd6cd76eb5a0 • hxxps[:]//paste[.]fo/raw/efda79f59c55 • hxxps[:]//rentry[.]co/4543t/raw • hxxps[:]//rentry[.]co/a2edp • hxxps[:]//textbin[.]net/raw/gr2vzmwcvt • hxxps[:]//rentry[.]co/q3i7zp/raw • hxxps[:]//rentry[.]co/tvfwh/raw • https[:]//rentry.co/MuckCompanyMMC/raw • hxxps[:]//cdn.discordapp[.]com/attachments/1192526919577649306/1211404800575537304/VisualStudioEN.7z?ex=6612fda3&is=660088a3&hm=5ae3b1b5d2c7dc91a9c07a65dbf8c61d3822b1f16a2d7c70eb37a039979e8290& • hxxps[:]//cdn.discordapp[.]com/attachments/1192526919577649306/1211403074799804476/VisualStudioRU.7z?ex=6612fc07&is=66008707&hm=0a7fc9432f5ef58960b1f9a215c3feceb4e7704afd7179753faa93438d7e8f54&

Recommendation

- To prevent falling victim to similar attacks, it is recommended to keep an eye on the following suspicious properties of a repo:

  Commit frequency: Does the repo have an extraordinary number of commits relative to its age?

  Are these commits changing the same file with very minor changes?

  Stargazers: Who is starring this repo? Do most of the stargazers appear to have had accounts created around the same time?
- By being aware of these red flags, users can better protect themselves from inadvertently downloading and executing malware.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre- Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://thehackernews.com/2024/04/beware-githubs-fake-popularity-scam.html
- https://www.bleepingcomputer.com/news/security/malicious-visual-studio-projects-ongithub- push-keyzetsu-malware/
- https://checkmarx.com/blog/new-technique-to-trick-developers-detected-in-an-open-sourcesupply chain-attack/