New Technique to Trick Developers Detected in an Open Source Supply Chain Attack

Date: 04th April 2024 | Severity: High

Summary

- In a recent attack campaign, cybercriminals were discovered cleverly manipulating GitHub's search functionality, and using meticulously crafted repositories to distribute malware.
- GitHub search manipulation: Attackers create malicious repositories with popular names and topics, using techniques like automated updates and fake stars to boost search rankings and deceive users.
- Malicious code is often hidden within Visual Studio project files (.csproj or .vcxproj) to evade detection, automatically executing when the project is built.
- The malware establishes persistence on infected Windows machines by creating a scheduled task that runs the malicious executable daily at 4AM without user confirmation.
- The recent malware campaign involves a large, padded executable file that shares similarities with the "Keyzetsu clipper" malware, targeting cryptocurrency wallets.

Attack Vectors

- Exploiting GitHub's Search Functionality:
  - Our recent findings reveal a threat actor creating GitHub repositories with names and topics that are likely to be searched by unsuspecting users. These repositories are cleverly disguised as legitimate projects, often related to popular games, cheats, or tools, making it difficult for users to distinguish them from benign code.
  - To ensure maximum visibility, the attackers employ a couple of clever techniques that consistently place their malicious repositories at the top of GitHub search results.
- Automatic Updates:
  - The attackers automatically update the repositories at a very high frequency by modifying a file, usually called "log", with the current date and time or just some random small change. This continuous activity artificially boosts the repositories' visibility, especially for instances where users filter their results by "most recently updated," increasing the likelihood of unsuspecting users finding and accessing them.

- Faking Popularity:
  - While automatic updates help, the attackers combine another technique to amplify the effectiveness of their repo making it to the top results.
  - This social engineering technique is designed to manipulate users into believing that the repository.
- Hidden Malware in Project Files:
  - The attackers conceal their malware primarily as obfuscated code deep within the .csproj or .vcxproj files of the repository (files commonly used in Visual Studio projects) to decrease the chances of the average user detecting it unless they proactively search for suspicious elements.

Indicator of compromise

INDICATOR TYPE	INDICATORS
URLs	• 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=0a7fc9432f5ef58960b1f9a215c3feceb4e7704afd 7179753faa93438d7e8f54& • hxxps[:]//rentry[.]co/q3i7zp/raw • hxxps[:]//rentry[.]co/tvfwh/raw • hxxps[:]//cdn[.]discordapp.com/attachments/1193658583947149322/1218876343232630844/main.exe?ex=6609420d&is=65f6cd0d&hm=f5a0af7499e892637935c3e4071f2dc59d48214f56a1c1d7aedc3392f58176db& • hxxps[:]//paste[.]fo/raw/dd6cd76eb5a0 • hxxps[:]//paste[.]fo/raw/efda79f59c55 • hxxps[:]//rentry[.]co/4543t/raw • hxxps[:]//rentry[.]co/a2edp • hxxps[:]//textbin[.]net/raw/gr2vzmwcvt • https://rentry.co/MuckCompanyMMC/raw • hxxps[:]//rentry[.]co/hwqfx/raw

Recommendation

- Employee Training and Awareness.
- Stay up to date with known vulnerabilities.
- While good access control, risk management, and design will limit the impact of a known vulnerability, it's better to just ensure you have few known vulnerabilities and mitigate them as needed.

Reference Links

- https://checkmarx.com/blog/new-technique-to-trick-developers-detected-in-an-open-source-supply-chain-attack/?web_view=true
- https://otx.alienvault.com/pulse/6616fc06e73afd06071b73e5