GitHub abused to distribute payloads on behalf of malware-as-a-service

Researchers from Cisco's Talos security team have uncovered a malware-as-a-service operator that used public GitHub accounts as a channel for distributing an assortment of malicious software to targets.

The use of GitHub gave the malware-as-a-service (MaaS) a reliable and easy-to-use platform that's greenlit in many enterprise networks that rely on the code repository for the software they develop. GitHub removed the three accounts that hosted the malicious payloads shortly after being notified by Talos.

"In addition to being an easy means of file hosting, downloading files from a GitHub repository may bypass Web filtering that is not configured to block the GitHub domain," Talos researchers Chris Neal and Craig Jackson wrote Thursday. "While some organizations can block GitHub in their environment to curb the use of open-source offensive tooling and other malware, many organizations with software development teams require GitHub access in some capacity. In these environments, a malicious GitHub download may be difficult to differentiate from regular web traffic."

Emmenhtal, meet Amadey

The campaign, which Talos said had been ongoing since February, used a previously known malware loader tracked under names including Emmenhtal and PeakLight. Researchers from

security firm Palo Alto Networks and Ukraine’s major state cyber agency SSSCIP had already documented the use of Emmenhtal in a separate campaign that embedded the loader into malicious emails to distribute malware to Ukrainian entities. Talos found the same Emmenhtal variant in the MaaS operation, only this time the loader was distributed through GitHub.

The campaign using GitHub was different from one targeting Ukrainian entities in another key way. Whereas the final payload in the one targeting the Ukrainian entities was a malicious backdoor known as SmokeLoader, the GitHub one installed Amadey, a separate malware platform known. Amadey was first seen in 2018 and was initially used to assemble botnets. Talos said the primary function of Amadey is to collect system information from infected devices and download a set of secondary payloads that are customized to their individual characteristics, based on the specific purpose in different campaigns.

https://arstechnica.com/security/2025/07/malware-as-a-service-caught-using-github-to-distribute-its-payloads/