The JinxLoader - Malware

Date: 03rd January 2024 | Severity: High

Summary

JinxLoader is a new Go-based loader that was spotted delivering next-stage malware such as Formbook and XLoader.

Attack Vectors

Palo Alto Networks' Unit 42 first observed the malware in November 2023 reporting that it has been advertised on the hacking forum Hackforums since April 30, 2023.

The attack spotted by the researchers used phishing messages posing as Abu Dhabi National Oil Company (ADNOC).

The content of the messages attempted to trick the recipients into opening a password protected RAR archive. Once the archive is opened, the infection chain starts leading to the deploys a secondary malware, such as Formbook or its successor, XLoader

Indicator of Compromise

INDICATOR TYPE	INDICATORS
File Hash	b7c66440c975bed86efe68c47c95bd1460ab8cf21bccacfc1e80c145e7be0f8b 08bf78e0c3c6250a295664c3fb4be7d05b90592260f979f87bb476638dd4a0a9 5c11e9204d181a28fb6ba97d0f26febe409e2151ae71c5aa63ea34ffb14ed383 9b1090ff32a441a89294739884b9a0330e75497573dde39b6b79ac4dd0a9effd c1d3ad3f518cf02925d304f1912860d01e8cfd8d2ed6f76bd200c7d25370206f edf824f5152829ef7be198c97a42e4ecd5ae9be37ef57051deda0435cc302063
Domains	219855[.]xn--80aswg 1214888[.]com Austintrafficlawyer[.]com Worldlife[.]casino Terranovaservices[.]top Ofupakoshi[.]com Julieannmirabel[.]online Zkrbma[.]store Ncdanmark[.]org ldhqi4[.]fun cjjmobbbshhhu[.]shop infinite-7[.]com autrevalevale[.]click overthemoonphoto[.]com taxhwangeub[.]com e3iaibr[.]icu http://loremipsum[.]network/login http://essentialdrivers[.]org/login http://91[.]92.246[.]52:8585/login https://www[.]wgs.com[.]pk/js/Qvaloe.vdf http://5.188.159[.]44/login
IPs	46.183.221[.]59 5.188.159[.]44

Recommendation

Submit the File Hash to the Antivirus team to update their database with the file hashes.

Submit the IPs to Network team to block in the firewall.

Block the Domain in the Proxy.

Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.

Run Regularly Scheduled Scans with Your Anti-Virus Software.

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://securityaffairs.com/156760/malware/jinxloader-loader.html

https://thehackernews.com/2024/01/new-jinxloader-targeting-users-with.html