Mapping and Pivoting from Cobalt Strike C2 Infrastructure Attributed to CVE-2021-40444

By Michael Koczwara

Published: 2021-09-15 · Archived: 2026-04-10 03:13:29 UTC

Member-only story

Michael Koczwara

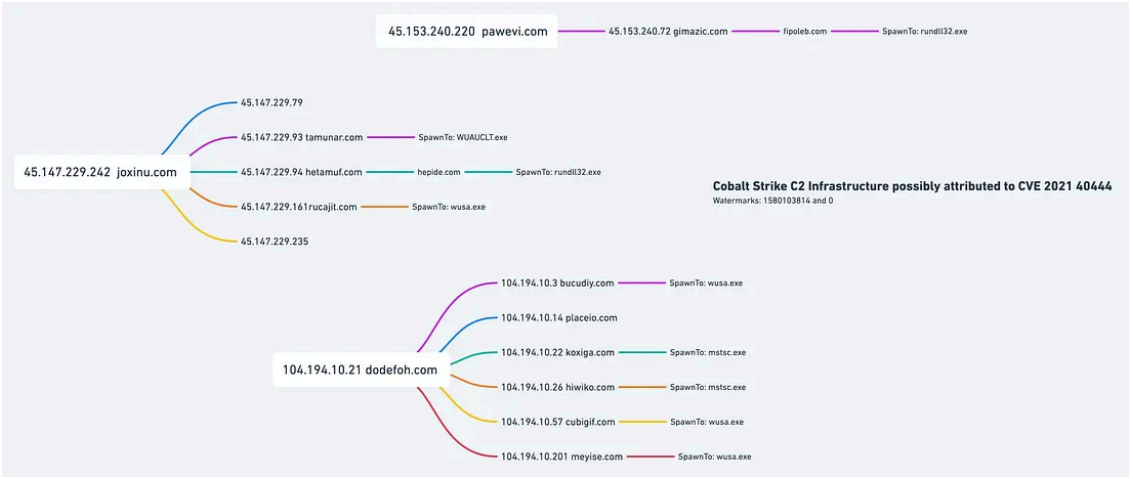
11 min read

Sep 12, 2021

Press enter or click to view image in full size

- **Threat Actors Infrastructure (VT Analysis).**
- **Pivoting from 45.147.229[.]242**
- **Pivoting from 104.194.10[.]21**
- **Pivoting from 45.153.240[.]220**
- **Short summary and IOC’s.**

Press enter or click to view image in full size



Threat Actors Cobalt Strike C2 Infrastructure

Cobalt Strike C2 Infrastructure possibly attributed to CVE-2021-40444

Edit description

drive.google.com

Threat Actors Infrastructure (VT Analysis)

The starting point is from the TrendMicro blog. I will take a look at joxinu[.]com, dodefoh[.]com, and pawevi[.]com, and I will try to find out if the Threat Actor deployed additional C2's on the same hosting provider, subnets, and IP range.

Press enter or click to view image in full size

hxxps://joxinu[.]com	C&C Server
hxxps://joxinu[.]com/hr[.]html	
hxxps://dodefoh[.]com	
hxxps://dodefoh[.]com/ml[.]html	
hxxp://pawevi[.]com/e32c8df2cf6b7a16/specify.html	

https://www.trendmicro.com/en_us/research/21/i/remote-code-execution-zero-day--cve-2021-40444--hits-windows--tr.ht…

Source: https://michaelkoczwara.medium.com/mapping-and-pivoting-cobalt-strike-c2-infrastructure-attributed-to-cve-2021-40444-438786fcd68a