cti/green_nailao at main · cert-orangecyberdefense/cti · GitHub

github.com/cert-orangecyberdefense/cti/tree/main/green_nailao

cert-orangecyberdefense

1. cti

/

green_nailao

/

Copy path

Name	Last commit message	Last commit date
..		

Name	Last commit message	Last commit date
iocs	iocs	
readme	readme	
yara	yara	

readme

Green Nailao is a malicious campaign that has been targeting at least between June and October 2024 European organizations, in particular in the healthcare sector. Tracked as Green Nailao (“Nailao” meaning “cheese” in Chinese – a topic our World Watch team holds in high regard), this campaign involves the ShadowPad malware as well as a previously undocumented ransomware payload dubbed NailaoLocker.
Orange Cyberdefense does not associate this campaign with a known threat group. Nevertheless, we assess with medium confidence that the threat actors do align with typical Chinese intrusion sets.

Full research article:
https://www.orangecyberdefense.com/global/blog/cert-news/meet-nailaolocker-a-ransomware-distributed-in-europe-by-shadowpad-and-plugx-backdoors#c137080