cert-orangecyberdefense/mintsloader

github.com/cert-orangecyberdefense/mintsloader

cert-orangecyberdefense

cert-orangecyberdefense/
mintsloader

MintsLoader IOCs

MintsLoader is a little-known, multi-stage malware loader that has been used since at least February 2023. We detected this loader in widespread distribution campaigns between July and October 2024. The name comes from a very characteristic use of an URL parameter “1.php?s=mintsXX" (with XX being numbers). Other campaigns used "s=boicn" pattern, as mentioned here: https://www.huntress.com/blog/fake-browser-updates-lead-to-boinc-volunteer-computing-software

MintsLoader primarily delivers malicious RAT or infostealing payloads such as AsyncRAT and Vidar through phishing emails, targeting organizations in Europe (Spain, Italy, Poland, etc.). Written in JavaScript and PowerShell, MintsLoader operates through a multi-step infection process involving several URLs and domains, most of which use a domain generation algorithm (DGA) with .top TLD.

Additional information on this threat is available for our World Watch customers in our dedicated advisory from August 10 here: https://portal.cert.orangecyberdefense.com/worldwatch/advisory/1837 and here: https://portal.orangecyberdefense.com/updates/worldwatch/viewSignal/1837.

IOCs and Yara rules are available in this repository.