

malware-indicators/202006_DarkBasin at master · citizenlab/malware-indicators · GitHub

github.com/citizenlab/malware-indicators/tree/master/202006_DarkBasin

citizenlab

citizenlab/malware-indicators



Citizen Lab Malware Reports

5 Contributors 1 Issue 219 Stars 62 Forks



Dark Basin Indicators of Compromise

This list of IOCs is being jointly released by Citizen Lab and NortonLifeLock, further to reports released on June 9, 2020.

Citizen Lab Report: [Dark Basin: Uncovering a Massive Hack-For-Hire Operation](#)

NortonLifeLock Report: [Mercenary.Amanda](#)

Note: *NortonLifeLock tracks Dark Basin as Mercenary.Amanda*

Files included in this directory:

- openioc.ioc : IOCs in OpenIOC format
- stix.xml : IOCs in STIX XML format
- iocs.csv : IOCs in csv format
- misp.json : IOCs in MISP format
- snort.rules: IOCs as a Snort ruleset.