Vitali Kremez on X: "2020-04-21:🆕🔥 #GuLoader Loader | #Signed Cert:🇷🇺[OOO MEDUZA SERVICE GROUP] #Sectigo 💉 Process Hollowing #YARA 1 HeavensGate 2 shellcode_get_eip Default URL Download & Execute (http://myurl/myfile.bin) via "Wininet.dll" h/t @malwrhunterteam MD5:8F56B7FB84C9688568426525D8D0E785 https://t.co/DUFuoZsLIt" / X

Published: 2020-04-21 · Archived: 2026-04-05 14:19:32 UTC

Source: https://twitter.com/VK_Intel/status/1252678206852907011