



**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

Did someone say ... cookies?

X and its partners use cookies to provide you with a better, safer and faster service and to support our business. Some cookies are necessary to use our services, improve our services, and make sure they work properly.

---

Source: [https://twitter.com/VK\\_Intel/status/1252678206852907011](https://twitter.com/VK_Intel/status/1252678206852907011)