CamuBot (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 02:01:58 UTC

There is no lot of IOCs in this article so we take one sample and try to extract some interesting IOCs, our findings below :

CamuBot sample : 37ca2e37e1dc26d6b66ba041ed653dc8ee43e1db71a705df4546449dd7591479

C:\Users\user~1\AppData\Local\Temp\protecao.exe : 0af612461174eedec813ce670ba35e74a9433361eacb3ceab6d79232a6fe13c1

C:\Users\user~1\AppData\Local\Temp\Renci.SshNet.dll : 3E3CD9E8D94FC45F811720F5E911B892A17EE00F971E498EAA8B5CAE44A6A8D8

C:\ProgramData\m.msi : AD90D4ADFED0BDCB2E56871B13CC7E857F64C906E2CF3283D30D6CFD24CD2190

Protecao.exe try to download hxxp://www.usb-over-network.com/usb-over-network-64bit.msi

A new driver is installed : C:\Windows\system32\drivers\ftusbload2.sys : 9255E8B64FB278BC5FFE5B8F70D68AF8

ftusbload2.sys set 28 IRP handlers.

▶ [TLP:WHITE] win_camubot_auto (20201014 | autogenerated rule brought to you by yara-signator)
