HIGHNOON (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 13:18:51 UTC

win.highnoon (Back to overview)

HIGHNOON

Actor(s): APT41, Aurora Panda

According to FireEye, HIGHNOON is a backdoor that may consist of multiple components. The components may include a loader, a DLL, and a rootkit. Both the loader and the DLL may be dropped together, but the rootkit may be embedded in the DLL. The HIGHNOON loader may be designed to run as a Windows service.

References

2021-12-16 · TEAMT5 · Aragorn Tseng, Charles Li, Peter Syu, Tom Lai
Winnti is Coming - Evolution after Prosecution
Cobalt Strike FishMaster FunnySwitch HIGHNOON ShadowPad Spyder

2019-11-19 · FireEye · Kelli Vanderlee, Nalani Fraser
Achievement Unlocked: Chinese Cyber Espionage Evolves to Support Higher Level Missions
MESSAGETAP TSCookie ACEHASH CHINACHOPPER Cobalt Strike Derusbi Empire Downloader Ghost RAT HIGHNOON HTran MimiKatz NetWire RC POISONPLUG Poison Ivy pupy Quasar RAT ZXShell

2019-08-19 · FireEye · Alex Pennino, Matt Bromiley
GAME OVER: Detecting and Stopping an APT41 Operation
ACEHASH CHINACHOPPER HIGHNOON

2019-08-09 · FireEye · FireEye
Double Dragon APT41, a dual espionage and cyber crime operation
CLASSFON crackshot CROSSWALK GEARSHIFT HIGHNOON HIGHNOON.BIN JUMPALL POISONPLUG Winnti

2019-08-08 · Twitter (@MrDanPerez) · Dan Perez
Tweet on Winnti and HIGHNOON
HIGHNOON

There is no Yara-Signature yet.

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.highnoon