LoJax (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 17:20:00 UTC

win.lojax (Back to overview)

LoJax

Actor(s): APT28

There is no description at this point.

References

2022-05-27 · · PTSecurity · Aleksey Vishnyakov, Anton Belousov

How bootkits are implemented in modern firmware and how UEFI differs from Legacy BIOS

LoJax MoonBounce

2022-01-11 · ESET Research · Michal Poslušný

Signed kernel drivers – Unguarded gateway to Windows' core

InvisiMole LoJax RobinHood Slingshot

2021-06-15 · vmware · Takahiro Haruyama

Detecting UEFI Bootkits in the Wild (Part 1)

LoJax MosaicRegressor TrickBot

2020-02-13 · Qianxin · Qi Anxin Threat Intelligence Center

APT Report 2019

Chrysaor Exodus Dacls VPNFilter DNSRat Griffon KopiLuwak More_eggs SQLRat AppleJeus BONDUPDATER Agent.BTZ Anchor AndroMut AppleJeus BOOSTWRITE Brambul Carbanak Cobalt Strike Dacls DistTrack DNSpionage Dtrack ELECTRICFISH FlawedAmmyy FlawedGrace Get2 Grateful POS HOPLIGHT Imminent Monitor RAT jason Joanap KerrDown KEYMARBLE Lambert LightNeuron LoJax MiniDuke PolyglotDuke PowerRatankba Rising Sun SDBbot ServHelper Snatch Stuxnet TinyMet tRat TrickBot Volgmer X-Agent Zebrocy

2018-11-05 · Youtube (MSRC) · Frédéric Vachon, Jean-Ian Boutin

BlueHat v18 || First STRONTIUM UEFI Rootkit Unveiled

LoJax

2018-10-04 · Symantec · Critical Attack Discovery and Intelligence Team

APT28: New Espionage Operations Target Military and Government Organizations

LoJax Seduploader X-Agent XTunnel Zebrocy APT28

2018-09-01 · ESET Research

LoJax: First UEFI rootkit found in the wild, courtesy of the Sednit group

LoJax

There is no Yara-Signature yet.
