MiniDuke (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 19:11:19 UTC

win.miniduke (Back to overview)

MiniDuke

Actor(s): APT29

The MiniDuke toolset consists of multiple downloader and backdoor components

References

2022-09-21 · Check Point · Jiří Vinopal
Native function and Assembly Code Invocation
MiniDuke

2021-09-29 · CYBER GEEKS All Things Infosec · CyberMasterV
How to defeat the Russian Dukes: A step-by-step analysis of MiniDuke used by APT29/Cozy Bear
MiniDuke

2020-03-26 · VMWare Carbon Black · Scott Knight
The Dukes of Moscow
Cobalt Strike LiteDuke MiniDuke OnionDuke PolyglotDuke PowerDuke

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

2020-01-01 · Secureworks · SecureWorks
IRON HEMLOCK
FatDuke MiniDuke OnionDuke PolyglotDuke APT29

2019-08-12 · Kindred Security · Kindred Security

An Overview of Public Platform C2’s

HTML5 Encoding LOWBALL Makadocs MiniDuke RogueRobinNET RokRAT

2013-05-30 · CIRCL · CIRCL

Analysis of a stage 3 Miniduke sample

MiniDuke

2013-02-28 · FireEye · James T. Bennett

It's a Kind of Magic

MiniDuke

There is no Yara-Signature yet.
