FinFisher RAT (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 21:06:28 UTC

FinFisher is a commercial software used to steal information and spy on affected victims. It began with few functionalities which included password harvesting and information leakage, but now it is mostly known for its full Remote Access Trojan (RAT) capabilities. It is mostly known for being used in governmental targeted and lawful criminal investigations. It is well known for its anti-detection capabilities and use of VMProtect.

2022-03-28 · Netzpolitik.org · Andre Meister
Staatstrojaner-Hersteller FinFisher „ist geschlossen und bleibt es auch“
FinFisher RAT 2021-11-15 · binarly · Binarly Team
Design issues of modern EDRs: bypassing ETW-based solutions
ESPecter FinFisher RAT 2021-09-28 · Kaspersky Labs · GReAT
FinSpy: unseen findings
FinFisher FinFisher FinFisher FinFisher RAT 2021-03-21 · Blackberry · Blackberry Research
2021 Threat Report
Bashlite FritzFrog IPStorm Mirai Tsunami elf.wellmess AppleJeus Dacls EvilQuest Manuscrypt Astaroth BazarBackdoor Cerber Cobalt Strike Emotet FinFisher RAT Kwampirs MimiKatz NjRAT Ryuk SmokeLoader TrickBot 2020-10-14 · Netzpolitik.org · Andre Meister
German Made State Malware Company FinFisher Raided
FinFisher FinFisher FinFisher FinFisher RAT 2020-09-25 · Amnesty International · Amnesty International
German-made FinSpy spyware found in Egypt, and Mac and Linux versions revealed
FinFisher FinFisher FinFisher FinFisher RAT 2019-08-01 · Kaspersky Labs · GReAT
APT trends report Q2 2019
ZooPark magecart POWERSTATS Chaperone COMpfun EternalPetya FinFisher RAT HawkEye Keylogger HOPLIGHT Microcin NjRAT Olympic Destroyer PLEAD RokRAT Triton Zebrocy 2018-03-01 · Microsoft · Microsoft Defender ATP Research Team, Office 365 Threat Research Team
FinFisher exposed: A researcher’s tale of defeating traps, tricks, and complex virtual machines
FinFisher RAT 2018-02-21 · Möbius Strip Reverse Engineering · Rolf Rolles
FinSpy VM Unpacking Tutorial Part 3: Devirtualization. Phase #3: Fixing The Function-Related Issues
FinFisher RAT 2018-02-21 · Möbius Strip Reverse Engineering · Rolf Rolles
FinSpy VM Unpacking Tutorial Part 3: Devirtualization. Phase #2: First Attempt At Devirtualization
FinFisher RAT 2018-02-21 · Möbius Strip Reverse Engineering · Rolf Rolles
FinSpy VM Unpacking Tutorial Part 3: Devirtualization. Phase #1: Deobfuscating FinSpy VM Bytecode Programs
FinFisher RAT 2018-02-21 · Möbius Strip Reverse Engineering · Rolf Rolles
FinSpy VM Unpacking Tutorial Part 3: Devirtualization. Phase #4: Second Attempt At Devirtualization
FinFisher RAT 2018-02-21 · Möbius Strip Reverse Engineering · Rolf Rolles
FinSpy VM Unpacking Tutorial Part 3: Devirtualization

FinFisher RAT 2018-02-21 · GitHub (RolfRolles) · Rolf Rolles

FinSpyVM (Static Unpacker for FinSpyVM)

FinFisher RAT 2018-01-24 · ESET Research · Filip Kafka

ESET'S GUIDE TODEOBFUSCATING AND DEVIRTUALIZING FINFISHER

FinFisher RAT 2018-01-23 · Möbius Strip Reverse Engineering · Rolf Rolles

A Walk-Through Tutorial, with Code, on Statically Unpacking the FinSpy VM: Part One, x86 Deobfuscation

FinFisher RAT 2017-10-16 · Kaspersky Labs · GReAT

BlackOasis APT and new targeted attacks leveraging zero-day exploit

FinFisher RAT BlackOasis 2017-09-21 · ESET Research · Filip Kafka

New FinFisher surveillance campaigns: Internet providers involved?

FinFisher RAT 2017-09-12 · FireEye · Ben Read, Genwei Jiang, James T. Bennett

FireEye Uncovers CVE-2017-8759: Zero-Day Used in the Wild to Distribute FINSPY,FireEye Uncovers CVE-2017-8759: Zero-Day Used in the Wild to Distribute FINSPY

FinFisher RAT BlackOasis 2017-07-18 · Elastic · Ashkan Hosseini

Ten process injection techniques: A technical survey of common and trending process injection techniques

Cryakl CyberGate Dridex FinFisher RAT Locky 2017-01-13 · Artem Baranov

Finfisher rootkit analysis

FinFisher RAT 2014-10-02 · CodeAndSec · CodeAndSec

FinFisher Malware Analysis - Part 2

FinFisher RAT

- [TLP:WHITE] win_finfisher_auto (20251219 | Detects win.finfisher.)
- [TLP:WHITE] win_finfisher_w0 (20170517 | FinFisher FinSpy)
- [TLP:WHITE] win_finfisher_w1 (20170517 | FinFisher FinSpy)
