Okrum (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 22:48:33 UTC

win.okrum (Back to overview)

Okrum

Actor(s): Mirage

---

a new, previously unknown backdoor that we named Okrum. The malicious actors behind the Okrum malware were focused on the same targets in Slovakia that were previously targeted by Ketrican 2015 backdoors.

References

2021-02-18 · PTSecurity · PTSecurity
https://www.ptsecurity.com/ww-en/analytics/antisandbox-techniques/
Poet RAT Gravity RAT Ketrican Okrum OopsIE Remcos RogueRobinNET RokRAT SmokeLoader

2020-11-03 · Kaspersky Labs · GReAT
APT trends report Q3 2020
WellMail EVILNUM Janicab Poet RAT AsyncRAT Ave Maria Cobalt Strike Crimson RAT CROSSWALK Dtrack LODEINFO MoriAgent Okrum PlugX POISONPLUG Rover ShadowPad SoreFang Winnti

2020-05-21 · Intezer · Paul Litvak
The Evolution of APT15’s Codebase 2020
Ketrican Ketrum Okrum

2019-07-18 · ESET Research · Zuzana Hromcová
Okrum: Ke3chang group targets diplomatic missions
Ketrican Okrum

There is no Yara-Signature yet.
