Janicab (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 17:23:31 UTC

osx.janicab (Back to overview)

Janicab

Actor(s): Evilnum

According to Patrick Wardle, this malware persists a python script as a cron job.
Steps:
1. Python installer first saves any existing cron jobs into a temporary file named '/tmp/dump'.
2. Appends its new job to this file.
3. Once the new cron job has been added 'python (~/.t/runner.pyc)' runs every minute.

References

2022-12-08 · Kaspersky · GReAT
DeathStalker targets legal entities with new Janicab variant
Janicab Janicab Stormwind

2022-05-31 · Malwarology · Gaetano Pellegrino
Janicab Series: Attibution and IoCs
Janicab

2022-05-27 · Malwarology · Gaetano Pellegrino
Janicab Series: The Core Artifact
Janicab

2022-05-26 · Malwarology · Gaetano Pellegrino
Janicab Series: Further Steps in the Infection Chain
Janicab

2022-05-24 · Malwarology · Gaetano Pellegrino
Janicab Series: First Steps in the Infection Chain
Janicab

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

2020-08-24 · Kaspersky Labs · Ivan Kwiatkowski, Maher Yamout, Pierre Delcher

Lifting the veil on DeathStalker, a mercenary triumvirate

EVILNUM Janicab Evilnum

2018-12-13 · Security 0wnage · Mo Bustami

POWERSING - From LNK Files To Janicab Through YouTube & Twitter

Janicab

2015-09-11 · · MacMark · Markus Möller

CSI MacMark: Janicab

Janicab

2013-07-22 · Avast · Peter Kálnai

Multisystem Trojan Janicab attacks Windows and MacOSX via scripts

Janicab

2013-07-15 · F-Secure · Broderick Aquilino

Signed Mac Malware Using Right-to-Left Override Trick

Janicab

There is no Yara-Signature yet.

Source: https://malpedia.caad.fkie.fraunhofer.de/details/osx.janicab