LaZagne (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 23:08:42 UTC

LaZagne

The author described LaZagne as an open source project used to retrieve lots of passwords stored on a local computer. It has been developed for the purpose of finding these passwords for the most commonly-used software. It is written in Python and provided as compiled standalone binaries for Linux, Mac, and Windows.

References

2025-03-20 · Cisco Talos · Asheer Malhotra, Brandon White, Jungsoo An, Vitor Ventura
UAT-5918 targets critical infrastructure entities in Taiwan
ShortLeash LaZagne JuicyPotato Meterpreter MimiKatz ShortLeash UAT-5918

2023-10-26 · Fourcore · parth gol
Threat Hunting: Detecting Browser Credential Stealing [T1555.003]
LaZagne RedLine Stealer

2023-04-03 · Mandiant · Eduardo Mattos, JASON DEYALSINGH, Nick Richard, NICK SMITH, Tyler McLellan
ALPHV Ransomware Affiliate Targets Vulnerable Backup Installations to Gain Initial Access
LaZagne BlackCat MimiKatz

2022-10-03 · Kaspersky Labs · GReAT
DeftTorero: tactics, techniques and procedures of intrusions revealed
Nightrunner Tunna ASPXSpy LaZagne ExplosiveRAT reGeorg Volatile Cedar

2022-06-20 · · Infinitum IT · infinitum IT
Charming Kitten (APT35)
LaZagne DownPaper MimiKatz pupy

2022-05-17 · Trend Micro · Trend Micro Research
Ransomware Spotlight: RansomEXX
LaZagne Cobalt Strike IcedID MimiKatz PyXie RansomEXX TrickBot

2022-05-09 · The DFIR Report · The DFIR Report
SEO Poisoning – A Gootloader Story
GootLoader LaZagne Cobalt Strike GootKit

2021-01-09 · Marco Ramilli's Blog · Marco Ramilli
Command and Control Traffic Patterns

ostap LaZagne Agent Tesla Azorult Buer Cobalt Strike DanaBot DarkComet Dridex Emotet Formbook IcedID ISFB NetWire RC PlugX Quasar RAT SmokeLoader TrickBot

2020-12-09 · Avast Decoded · Igor Morgenstern, Luigino Camastra

APT Group Targeting Governmental Agencies in East Asia

LaZagne Albaniiutas HyperBro MimiKatz PolPo Tmanger TaskMasters

2020-11-30 · Yoroi · Antonio Pirozzi, Luca Mella, Luigi Martire

Shadows From The Past Threaten Italian Enterprises

Rekoobe LaZagne Responder MimiKatz win.rekoobe

2020-11-20 · Trend Micro · Abraham Camba, Bren Matthew Ebriega, Gilbert Sison

Weaponizing Open Source Software for Targeted Attacks

LaZagne Defray PlugX

2020-09-14 · Github (AlessandroZ) · AlessandroZ

The LaZagne Project !!!

LaZagne

2020-08-01 · Group-IB · Group-IB

RedCurl: The pentest you didn’t know about

LaZagne

2020-05-08 · MITRE · MITRE ATT&CK

Inception

PowerShower LaZagne

2020-05-08 · MITRE · MITRE ATT&CK

Inception

PowerShower LaZagne Inception Framework

There is no Yara-Signature yet.

Source: https://malpedia.caad.fkie.fraunhofer.de/details/py.lazagne