

Dacls (Malware Family)

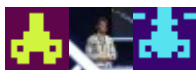
By Fraunhofer FKIE

Archived: 2026-04-05 18:47:11 UTC

Dacls

aka: MATA

Actor(s): [Lazarus Group](#)



According to PCrisk, Dacls is the name of a remote access Trojan (RAT), a malicious program that allows cyber criminals to control infected computers remotely.

Research shows that this malware is tied to Lazarus Group (a group of cyber criminals) and targets Linux and the Windows Operating System. Typically, cyber criminals use RATs to steal sensitive, confidential information, infect systems with other malware, and so on. In any case, no RAT is harmless and should be uninstalled immediately.

References

2023-10-18 · [Kaspersky Labs](#) ·

Updated MATA attacks industrial companies in Eastern Europe

[Dacls Unidentified 106](#)

2023-09-27 · [Positive Technologies](#) · [Denis Kuvshinov](#), [Maxim Andreev](#)

Dark River. You can't see them, but they're there

[Dacls Unidentified 106](#)

2022-11-21 · [vmware](#) · [Takahiro Haruyama](#), [Threat Analysis Unit](#)

Threat Analysis: Active C2 Discovery Using Protocol Emulation Part4 (Dacls, aka MATA)

[Dacls](#)

2021-10-08 · [Virus Bulletin](#) · [Seongsu Park](#)

Multi-universe of adversary: multiple campaigns of the Lazarus group and their connections

[Dacls](#) [AppleJeus](#) [AppleJeus](#) [Bankshot](#) [BookCodes](#) [RAT](#) [Dacls](#) [DRAT](#) [Zarus](#) [LCPDot](#) [LPEClient](#)

2021-08-22 · [Malware and Stuff](#) · [Andreas Klopsch](#)

PEB: Where Magic Is Stored

[Dacls](#)

2021-03-03 · [SYGNIA](#) · [Amitai Ben Shushan](#), [Amnon Kushnir](#), [Boaz Wasserman](#), [Martin Korman](#), [Noam Lifshitz](#)
Lazarus Group's MATA Framework Leveraged to Deploy TFlower Ransomware
[Dacls Dacls Dacls TFlower](#)

2020-09-22 · [vmware](#) · [Omar Elgebaly](#), [Takahiro Haruyama](#)
Detecting Threats in Real-time With Active C2 Information
[Agent.BTZ Cobalt Strike Dacls NetWire RC PoshC2 Winnti](#)

2020-07-29 · [Kaspersky Labs](#) · [GReAT](#)
APT trends report Q2 2020
[PhantomLance Dacls Penguin Turla elf.wellmess AppleJeus Dacls AcidBox Cobalt Strike Dacls EternalPetya Godlike12 Olympic Destroyer PlugX shadowhammer ShadowPad Sinowal VHD Ransomware Volgmer WellMess X-Agent XTunnel](#)

2020-07-28 · [Kaspersky Labs](#) · [Félix Aime](#), [Ivan Kwiatkowski](#), [Pierre Delcher](#)
Lazarus on the hunt for big game
[Dacls Dacls Dacls VHD Ransomware](#)

2020-07-22 · [Kaspersky Labs](#) · [GReAT](#)
MATA: Multi-platform targeted malware framework
[Dacls Dacls Dacls](#)

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.](#)

2019-12-17 · [Netlab](#) · [GenShen Ye](#), [Jinye](#)
Lazarus Group uses Dacls RAT to attack Linux platform
[Dacls Log_Collector Dacls](#)

There is no Yara-Signature yet.