

WellMail (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 18:38:57 UTC

elf.wellmail ([Back to overview](#))

WellMail

Actor(s): APT 29

There is no description at this point.

References

2021-02-25 · [Intezer](#) · [Intezer](#)

Year of the Gopher A 2020 Go Malware Round-Up

[NiuB WellMail elf.wellmess ArdaMax AsyncRAT CyberGate DarkComet Glupteba Nanocore RAT Nefilim NjRAT Quasar RAT WellMess Zebrocy](#)

2020-12-21 · [Intezer](#) · [Intezer](#)

Top Linux Cloud Threats of 2020

[AgeLocker AnchorDNS Blackrota Cloud Snooper Dacls Doki FritzFrog IPStorm Kaiji Kinsing NOTROBIN Penquin Turla PLEAD Prometei RansomEXX Stantinko TeamTNT TSCookie WellMail elf.wellmess TeamTNT](#)

2020-12-21 · [IronNet](#) · [Adam Hlavec](#), [Kimberly Ortiz](#)

Russian cyber attack campaigns and actors

[WellMail elf.wellmess Agent.BTZ BlackEnergy EternalPetya Havex RAT Industroyer Ryuk Triton WellMess](#)

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](#)

2020-09-17 · [PWC UK](#) · [PWC UK](#)

Analysis of WellMail malware's Command and Control (C2) server

[WellMail](#)

2020-08-13 · [Talos Intelligence](#) · [Martin Lee](#), [Paul Rascagnères](#), [Vitor Ventura](#)

Attribution: A Puzzle

[WellMail elf.wellmess AcidBox WellMess](#)

2020-07-16 · [CISA](#) · [US-CERT](#)

Malware Analysis Report (AR20-198C)

[WellMail](#)

2020-07-16 · [NCSC UK](#) · [NCSC UK](#)

Advisory: APT29 targets COVID-19 vaccine development

[WellMail](#) [elf.wellmess](#) [SoreFang](#) [WellMess](#)

There is no Yara-Signature yet.

Source: <https://malpedia.caad.fkie.fraunhofer.de/details/elf.wellmail>