# Saitama Backdoor (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 18:05:32 UTC

win.saitama (Back to overview)

## Saitama Backdoor

aka: AMATIAS, Saitama

Actor(s): OilRig

---

This in .Net witten backdoor abuses the DNS protocoll for its C2 communication. Also other techniques (e.g. long random sleeps, compression) are used to become more stealthy.

#### References

2023-02-02 · Trend Micro · Mahmoud Zohdy, Mohamed Fahmy, Sherif Magdy
New APT34 Malware Targets The Middle East
Karkoff RedCap Saitama Backdoor

2022-06-24 · XJunior · Mohamed Ashraf
APT34 - Saitama Agent
Saitama Backdoor

2022-06-13 · SANS ISC · Renato Marinho
Translating Saitama's DNS tunneling messages
Saitama Backdoor

2022-05-11 · Fortinet · Fred Gutierrez
Please Confirm You Received Our APT
Saitama Backdoor

2022-05-10 · Malwarebytes Labs · Threat Intelligence Team
APT34 targets Jordan Government using new Saitama backdoor
Saitama Backdoor

There is no Yara-Signature yet.

---

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.saitama