

BIOPASS (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 00:24:30 UTC

win.biopass ([Back to overview](#))

BIOPASS

Actor(s): [APT41](#)

BIOPASS RAT is a malware family which targets online gambling companies in China by leveraging a watering hole attack. This Remote Access Trojan (RAT) is unique in that it leverages the Open Broadcaster Software (OBS) framework to monitor the user's screen.

References

2022-01-17 · [Trend Micro](#) · [Cedric Pernet](#), [Daniel Lunghi](#), [Gloria Chen](#), [Jaromír Hořejší](#), [Joseph Chen](#), [Kenney Lu](#)

Delving Deep: An Analysis of Earth Lusca's Operations

[BIOPASS Cobalt Strike FunnySwitch JuicyPotato ShadowPad Winnti Earth Lusca](#)

2021-07-07 · [Trend Micro](#) · [Gloria Chen](#), [Jaromír Hořejší](#), [Joseph C. Chen](#), [Kenney Lu](#)

BIOPASS RAT: New Malware Sniffs Victims via Live Streaming

[BIOPASS Cobalt Strike Derusbi](#)

There is no Yara-Signature yet.

Source: <https://malpedia.caad.fkie.fraunhofer.de/details/win.biopass>