

TROJAN MOBILE

GodLoader

17+ mentions in the last 2 weeks

35 articles in the last 12 months



 Using open-source data collected by Feedly AI.

Overview

GodLoader is a malware strain that exploits the Godot game engine, a popular open-source platform for game development, to deliver malicious payloads across multiple operating systems, including Windows, macOS, Linux, Android, and iOS. It has been active since at least June 2024 and has infected over 17,000 systems. The malware utilizes Godot's scripting capabilities to embed harmful code within g... [See More](#)

Aliases

- God Loader

Source: Feedly AI

Article count



No article counts found. Try changing the time period.

Top targeted industries and organizations

INDUSTRIES	ORGANIZATIONS	ARTICLES	ATTACK REPORTED
------------	---------------	----------	-----------------





No attack has been detected in the time frame selected

Top threat actors using this malware

No threat actors have been linked to this malware at the moment

Tactics, Techniques, and Procedures

Last mentioned 

TECHNIQUE	MITRE ID	PROCEDURES	MITIGATION	ARTICLES
Virtualization/Sandbox Evasion 	T1497	<u>12</u>	0	<u>11</u>
Private Keys	T1552.004	<u>1</u>	<u>4</u>	<u>1</u>
Ingress Tool Transfer 	T1105	<u>17</u>	<u>1</u>	<u>11</u>
Software Packing	T1027.002	<u>2</u>	<u>1</u>	<u>2</u>
System Language Discovery	T1614.001	<u>1</u>	0	<u>1</u>

Command and Scripting Interpreter ↑	T1059	<u>15</u>	<u>7</u>	<u>11</u>
Data from Local System	T1005	<u>1</u>	<u>1</u>	<u>1</u>
Match Legitimate Name or Location	T1036.005	<u>4</u>	<u>3</u>	<u>4</u>
Process Injection	T1055	<u>2</u>	<u>2</u>	<u>2</u>

Exploited vulnerabilities

CVE ID	CVSS SCORE ⬇	EPSS SCORE ⬇	VENDOR	PRODUCT	TREND
<div><div></div><div>No exploited vulnerabilities at the moment</div></div>					

News



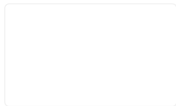
Godot Game Engine Targeted in Widespread Malware Attack

🔗 5 TTPs • CySecurity News - Latest Information Sec... by Trapti Rajput / 7d

- ↗ GodLoader malware exploits gaming engines

A newly identified malware threat, GodLoader, is targeting gamers globally by exploiting the Godot game development engine, according to a report from Check Point Research.

Also in The Hacker News | #1..., #malware, +101 feeds



2nd December – Threat Intelligence Report

🔗 6 CVEs • Check Point Research by tomersp@checkpoint.com / 7d •

🔗 10 TTPs

Malicious loader, dubbed “GodLoader”, which is using this technique has been active since at least June 2024, and is believed to have already infected over 17,000 machines.



Hackers use Godot game engine scripting to deliver malware

Security News by invalid@example.com (Victor M) / 8d

A popular open-source game engine called Godot Engine is being misused as part of a new GodLoader malware campaign, infecting over 17,000 systems since at least June 2024.



CTO at NCSC Summary: week ending December 1st

🔗 Threat Actors • by Ollie Whitehouse / 9d • 📄 Threat Intelligence Reports

- 🔗 3 CVEs • 🔗 29 TTPs

submitted by /u/digicat [link] [comments]



Godot Engine Exploited to Spread Malware on Windows, macOS, Linux

🔗 12 TTPs •

Hackread – Latest Cybersecurity, Tech, C... by Deeba Ahmed / 10d • Original source: Check Point Research / 12d •

↗ GodLoader malware exploits gaming engines

Check Point Research (CPR) has published its latest research on a novel multi-platform technique employed by cybercriminals to exploit the popular open-source game engine, Godot to deliver a newly discovered malicious payload dubbed...

Also in The Hacker News | #1..., #malware, +101 feeds



Popular game script spoofed to infect thousands of game developers

🔗 4 TTPs • Popular game script spoofed to infect th... / 10d • Original source: Check Point Research / 12d • ↗ Godot engine infected with malware

A malware loader, now named GodLoader, has been observed to be using Godot, a free and open-source game engine, as its runtime to execute malicious codes and has dropped known malware on at least 17,000 machines.

Also in TechRadar, Patrick C Miller, +115 feeds

[See 11 more articles and social media posts](#)

Made with  feedly