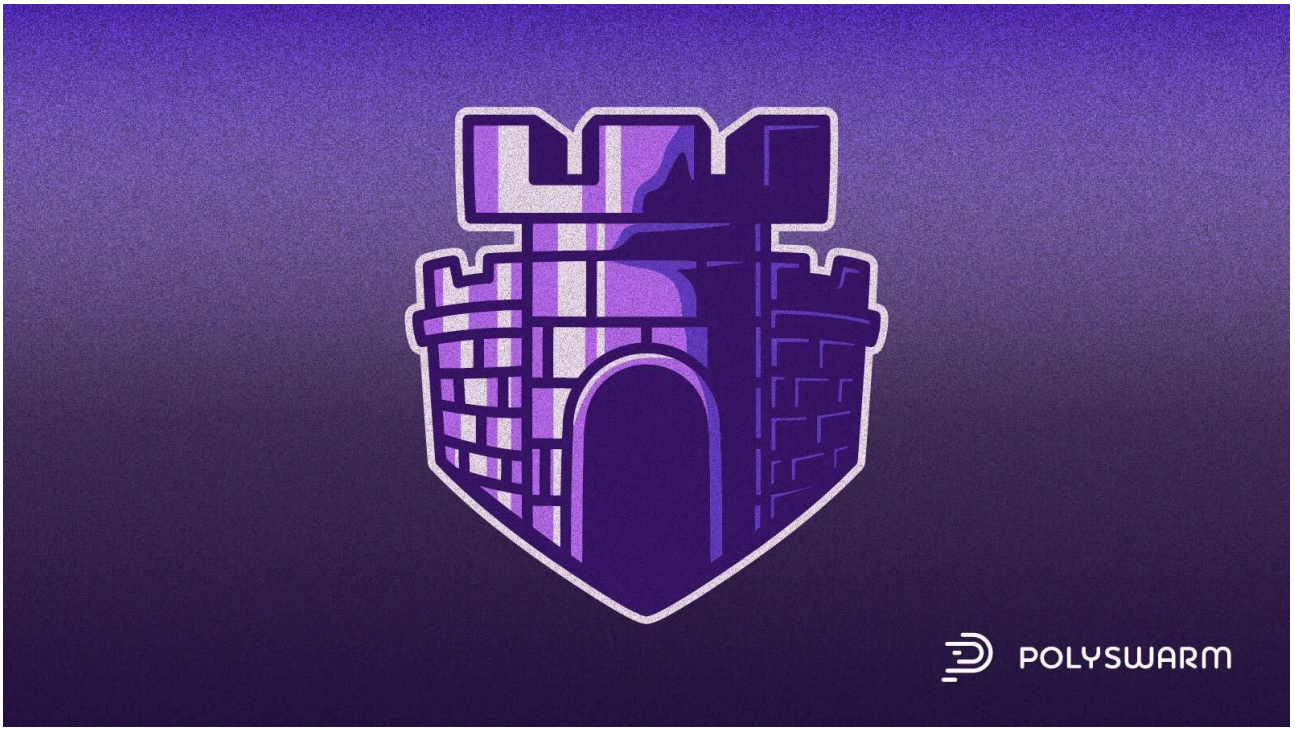
# CastleLoader

By The Hivemind

Archived: 2026-04-05 21:44:17 UTC




**Verticals Targeted:** Government
**Regions Targeted:** US
**Related Families:** StealC, RedLine, NetSupport RAT, DeerStealer, HijackLoader, SectopRAT

---

## Executive Summary

CastleLoader, a versatile malware loader, has infected 469 devices since May 2025, leveraging Cloudflare-themed ClickFix phishing and fake GitHub repositories to deliver information stealers and RATs. Its sophisticated attack chain, high infection rate, and modular design make it a significant threat to organizations, particularly U.S. government entities.**Key Takeaways**

- CastleLoader employs ClickFix phishing and fake GitHub repositories to trick users into executing malicious PowerShell commands.
- The malware has a 28.7% infection rate, compromising 469 devices out of 1,634 attempts since May 2025.
- It delivers multiple payloads, including StealC, RedLine, NetSupport RAT, DeerStealer, HijackLoader, and SectopRAT.
- U.S. government entities are among the critical victims targeted by CastleLoader campaigns.

## What is CastleLoader?

Since its emergence in early 2025, CastleLoader has established itself as a formidable malware loader, orchestrating the delivery of information stealers and remote access trojans (RATs) through advanced phishing tactics and deceptive GitHub repositories. Cybersecurity researchers at PRODAFT have tracked its campaigns, which have infected 469 devices out of 1,634 attempts since May 2025, yielding a 28.7% infection rate. This high success rate underscores the malware's effectiveness in exploiting human behavior and trusted platforms, with a notable impact on U.S. government entities.

CastleLoader's primary infection vector is the ClickFix phishing technique, often themed around Cloudflare services. Victims are lured to fraudulent domains mimicking software development libraries, online meeting platforms like Google Meet, or browser update notifications. These pages display fake error messages or CAPTCHA prompts, tricking users into copying and executing malicious PowerShell commands via the Windows Run prompt. This method bypasses traditional email-based security by exploiting user-initiated actions.

Alternatively, CastleLoader leverages fake GitHub repositories, such as one disguised as SQL Server Management Studio (SSMS-lib), to distribute malicious installers. These repositories exploit developers' trust in GitHub, prompting them to run seemingly legitimate software that connects to a command-and-control (C2) server. The loader's modular design allows it to deploy a range of secondary payloads, including StealC, RedLine, DeerStealer, NetSupport RAT, SectopRAT, and HijackLoader, depending on the campaign's objectives. StealC, RedLine, and DeerStealer focus on harvesting credentials, browser data, and cryptocurrency wallets, while NetSupport RAT and SectopRAT provide backdoor access for persistent control. HijackLoader, another loader, further extends the attack chain, amplifying CastleLoader's versatility.

The malware's technical sophistication is evident in its use of PowerShell and AutoIT scripts. After initial execution, the AutoIT script loads shellcode into memory as a DLL, resolving hashed DLL names and APIs to connect to one of seven distinct C2 servers. These servers, managed via a web-based panel, provide operators with detailed telemetry, including victim identifiers, IP addresses, and system details. The panel's Delivery module stores payloads with metadata, while the Tasks module enables precise control over distribution, supporting geographic targeting and encrypted Docker containers. Campaigns can enforce administrative privileges, anti-VM detection, and fake error displays to evade detection.

CastleLoader's overlap with DeerStealer campaigns, where both distribute HijackLoader, suggests coordinated efforts among threat actors. Network communications further complicate attribution, as payloads are retrieved from legitimate file-sharing services and compromised websites. This distributed approach enhances resilience against takedowns. With over 400 critical victims, including government entities, CastleLoader's impact is significant. PolySwarm analysts consider CastleLoader to be an emerging threat.

## IOCs

PolySwarm has a sample of CastleLoader.

05ecf871c7382b0c74e5bac267bb5d12446f52368bb1bfe5d2a4200d0f43c1d8

You can use the following CLI command to search for all CastleLoader samples in our portal:

***$ polyswarm link list -f CastleLoader***

***Don’t have a PolySwarm account? Go [here](#) to sign up for a free Community plan or subscribe.***

***Contact us at* hivemind@polyswarm.io | *Check out our [blog](#) | [Subscribe](#) to our reports.***

Topics: Threat Bulletin, Phishing, Redline, Emerging Threat, PowerShell, StealC, ClickFix, CastleLoader, GitHub, DeerStealer, malware loader, NetSupport RAT

---

Source: https://blog.polyswarm.io/castleloader