CastleLoader: Malware Overview

By ANY.RUN

Published: 2026-02-02 · Archived: 2026-04-05 21:48:48 UTC

9 min read

Feb 2, 2026

CastleLoader is a modern malware loader designed to quietly establish initial access and deliver follow-up payloads such as stealers, RATs, and ransomware. It focuses on stealth, flexibility, and rapid payload rotation, making it an effective tool for financially motivated threat actors and a persistent problem for enterprise defenders.

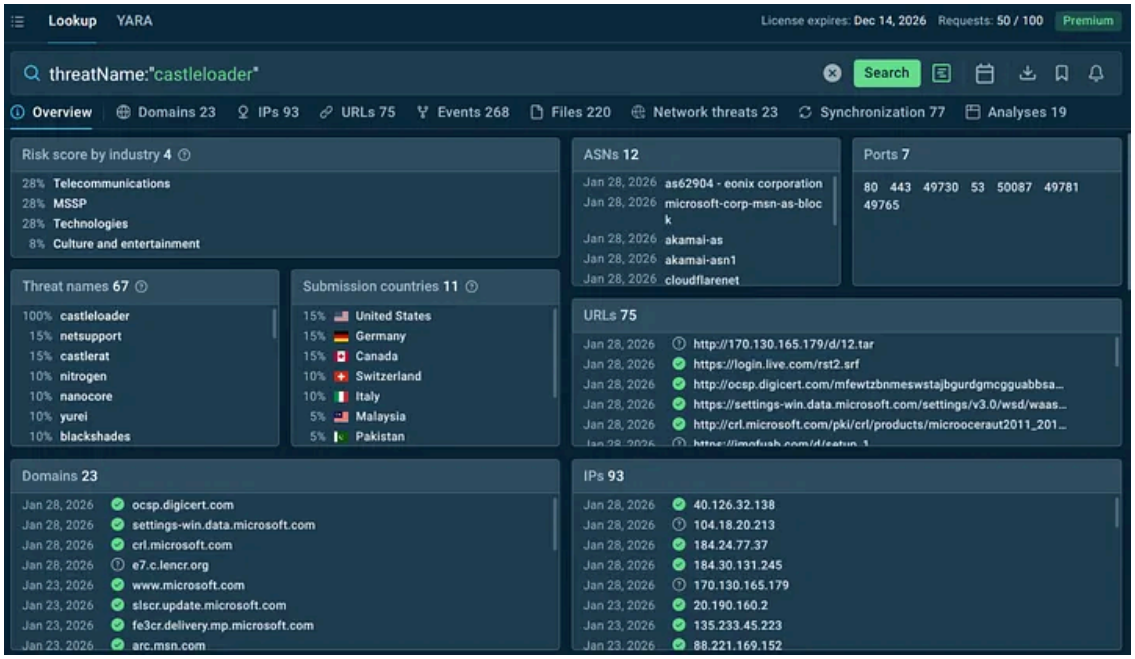
CastleLoader: The Quiet Malware That Opens the Door to Bigger Attacks

Key Takeaways

1. CastleLoader is a **Sophisticated MaaS Operation**; it serves multiple threat actor clusters, delivering diverse secondary payloads including information stealers and RATs with a documented 28.7% infection success rate.
2. Multi-Industry Targeting with Sector-Specific Campaigns: documented campaigns show focused attacks on **logistics, hospitality, government entities, and software developers** through industry-specific social engineering.
3. **ClickFix and Fake Repositories** Are Primary Infection Vectors.
4. **Advanced Evasion Through Multi-Stage Execution**: CastleLoader employs a three-stage architecture (stager/downloader, loader, core backdoor) with anti-VM detection, in-memory execution, PEB walking, and process hollowing.
5. ANY.RUN's Threat Intelligence Lookup helps SOCs quickly understand campaign scope and relationships.

threatName:"castleloader"

Press enter or click to view image in full size

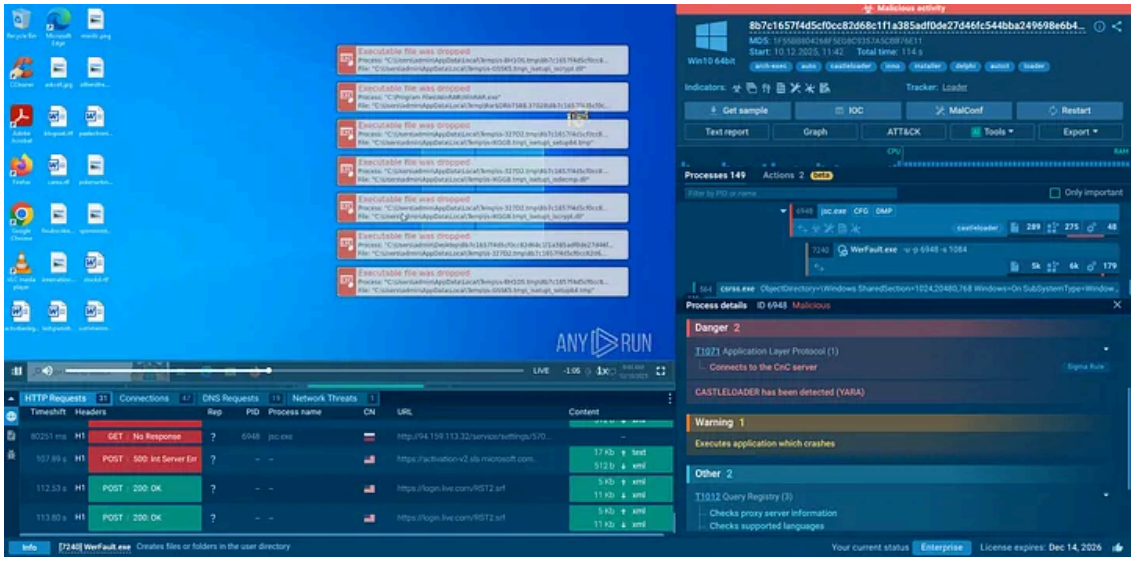


CastleLoader overview in TI Lookup: targeted industries and countries; IOCs; samples

ANY.RUN's Interactive Sandbox allows defenders to safely observe CastleLoader behavior and extract actionable indicators in real time.

View analysis

Press enter or click to view image in full size



CastleLoader malware analysis

What is CastleLoader Malware?

Developed and operated by the threat actor tracked as GrayBravo (formerly TAG-150), this loader combines advanced evasion techniques with a robust delivery infrastructure that enables multiple threat actors to leverage it for their campaigns.

The malware's architecture consists of multiple components working in concert. At its core, CastleLoader employs a three-stage execution chain: a shellcode stager/downloader, a loader component, and a core backdoor module. This modular design allows threat actors to separate the initial infection vector from eventual malware behavior, significantly complicating attribution efforts and enabling rapid adaptation to defensive measures.

CastleLoader utilizes sophisticated anti-analysis mechanisms including dead code injection, runtime packing, and virtual machine detection capabilities. The malware can escalate privileges to run with administrator rights and displays decoy messages such as fake system warnings to mask its true purpose. Once deployed, it establishes communication with command-and-control (C2) servers to retrieve and execute next-stage payloads, all while maintaining a low detection profile through in-memory execution techniques.

Recent variants have evolved to include Python-based loaders that leverage windowless interpreters (pythonw.exe) to rebuild and launch CastleLoader directly in memory, avoiding disk-based detection. The malware employs PEB (Process Environment Block) Walking to resolve required APIs at runtime, further enhancing its ability to bypass traditional security controls.

What makes CastleLoader notable is its operational discipline. Payloads are often updated, infrastructure is frequently rotated, and delivery techniques evolve quickly. This reduces the effectiveness of static indicators and signature-based defenses, forcing defenders to rely on behavioral analysis and threat intelligence correlation.

How CastleLoader threatens businesses and organizations

For organizations, CastleLoader is dangerous precisely because it is not the final threat, but the opening act.

Key business risks include:

- **Initial access** for larger attacks: CastleLoader is often the first step toward ransomware deployment or long-term espionage.
- **Credential theft and lateral movement**: Follow-up payloads frequently target browsers, email clients, VPNs, and internal authentication mechanisms.
- **Data breaches and compliance exposure**: Stolen credentials and data can lead to regulatory violations, fines, and reputational damage.
- **Operational disruption**: Once access is established, attackers can deploy tools that disrupt business operations at a chosen moment.
- **High dwell time**: Because loaders aim to stay unnoticed, attackers may remain inside networks for weeks before triggering visible damage.

In short, CastleLoader turns a single user mistake into a multi-stage business incident.

Victimology: vulnerable industries and sectors

CastleLoader demonstrates broad targeting capabilities with specific threat clusters focusing on particular industries:

- **Logistics and Transportation**: The most extensively documented campaign (tracked as TAG-160) specifically targets the logistics sector through sophisticated phishing operations. Threat actors impersonate legitimate logistics firms and exploit freight-matching platforms like DAT Freight & Analytics and Loadlink Technologies.
- **Government Entities**: The sensitive nature of governmental data and the potential for espionage make these entities particularly attractive targets for threat actors.
- **Hospitality Industry**: Campaign clusters have leveraged Booking.com-themed phishing attacks, indicating focused targeting of hospitality sector organizations and their customers. These campaigns exploit the industry's reliance on online booking systems and customer communications.
- **Technology and Software Development** through fake GitHub repositories mimicking legitimate development tools like SQL Server Management Studio (SSMS), RVTools, and Zabbix.
- **Healthcare facilities** have been affected by secondary payloads delivered via CastleLoader, particularly ransomware variants that cause operational disruptions.
- **Financial Services**: Any organization handling financial transactions, payment processing, or banking operations faces elevated risk due to the information-stealing capabilities of CastleLoader's secondary payloads.
- **Small and Medium Enterprises (SMEs)**: Companies with limited security resources are particularly vulnerable to CastleLoader's social engineering tactics, as they may lack robust security awareness training and advanced detection capabilities.

The geographical targeting shows strong focus on North American organizations, particularly in the United States, though the infrastructure and MaaS model enable global operations.

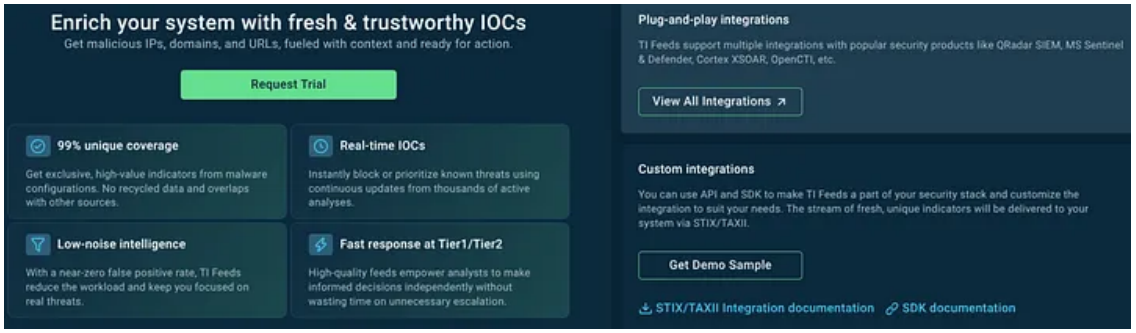
How Can Businesses Proactively Protect Against CastleLoader

ANY.RUN's Threat Intelligence Feeds deliver real-time, actionable IOCs (domains, URLs, IPs) derived from sandbox detonations and global submissions. For CastleLoader, feeds supply emerging C2s, loader variants, and linked payloads (e.g., CastleRAT), enabling automated blocking in firewalls, EDR, SIEMs. This helps organizations stay ahead of evolving MaaS campaigns, minimize dwell time, and prevent chain infections — critical for high-velocity threats like loaders.

Business Impact:

- **Reduced Mean Time to Detect (MTTD):** Automated indicator ingestion identifies CastleLoader activity within minutes rather than hours or days
- **Prevention of Initial Compromise:** Blocking C2 infrastructure and malicious domains prevents CastleLoader from establishing footholds
- **Operational Continuity:** Early detection and automated blocking minimize disruption to business operations
- **Improved Security ROI:** Leveraging threat intelligence from 15,000+ organizations maximizes detection capabilities without corresponding cost increases.

Press enter or click to view image in full size



TI Feeds benefits and integration options

Infection Vectors and Propagation Methods

The primary infection vector utilizes the ClickFix technique, where victims encounter fraudulent web pages themed around Cloudflare services, software development libraries, online meeting platforms (like Google Meet), or browser update notifications.

These pages display fake error messages, CAPTCHA verification prompts, or security warnings that instruct users to copy and execute malicious PowerShell commands via the Windows Run dialog (Win+R).

CastleLoader operators also create convincing fake GitHub repositories under the names of legitimate applications. For example, repositories named “ssms-lib” (impersonating SQL Server Management Studio) and “zscaler-dir/Zscaler-Client-Connector” have been used to distribute trojanized installers.

Threat actors employ search engine optimization techniques to ensure malicious download pages rank higher than legitimate software distributors in search results. Finally, traditional phishing remains part of the infection chain, particularly in logistics sector targeting.

Propagation Mechanism

Once initial infection occurs via PowerShell script execution, CastleLoader uses built-in Windows utilities (curl.exe, tar.exe) to download and stage payloads in hidden AppData folders. The malware then establishes C2 communication to retrieve additional modules and secondary payloads based on the victim’s value and environment. This staged approach allows operators to deploy targeted malware to high-value victims while maintaining flexibility in payload selection.

How CastleLoader functions

CastleLoader operates through a sophisticated multi-stage execution chain:

Get ANY.RUN’s stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

Stage 1: Initial Delivery and Execution

The infection begins with a packed executable, often delivered via Inno Setup installers containing AutoIT scripts. When executed, the malware unpacks itself at runtime, employing dead code injection to hinder static analysis. Recent variants use Python bytecode executed via pythonw[.]exe to avoid console windows and disk-based detection.

Stage 2: Shellcode Stager/Downloader

The initial stage deploys a shellcode stager that performs environment checks to detect virtual machines, sandboxes, and analysis tools. If running in a legitimate environment, it proceeds to establish initial C2 communication. The stager uses process hollowing techniques to inject code into legitimate Windows processes, masking malicious activity within trusted executables.

Stage 3: Loader Component

The loader module connects to the C2 server using HTTP/HTTPS connections with hardcoded User-Agent strings (notably “GoogleBot”) for identification. It downloads encrypted payload packages from the attacker’s infrastructure. The loader employs DLL side-loading techniques, placing malicious DLLs alongside legitimate executables to achieve persistence and execution.

Stage 4: Core Backdoor (CastleBot)

The core module establishes robust C2 communication and awaits task instructions. It gathers system information including:

- Computer name and username
- Operating system version and architecture
- Installed applications and security products
- Network configuration
- Active process list

This reconnaissance data allows operators to filter victims and determine appropriate secondary payloads.

Payload Deployment

Based on C2 instructions, CastleLoader downloads and executes various malware families:

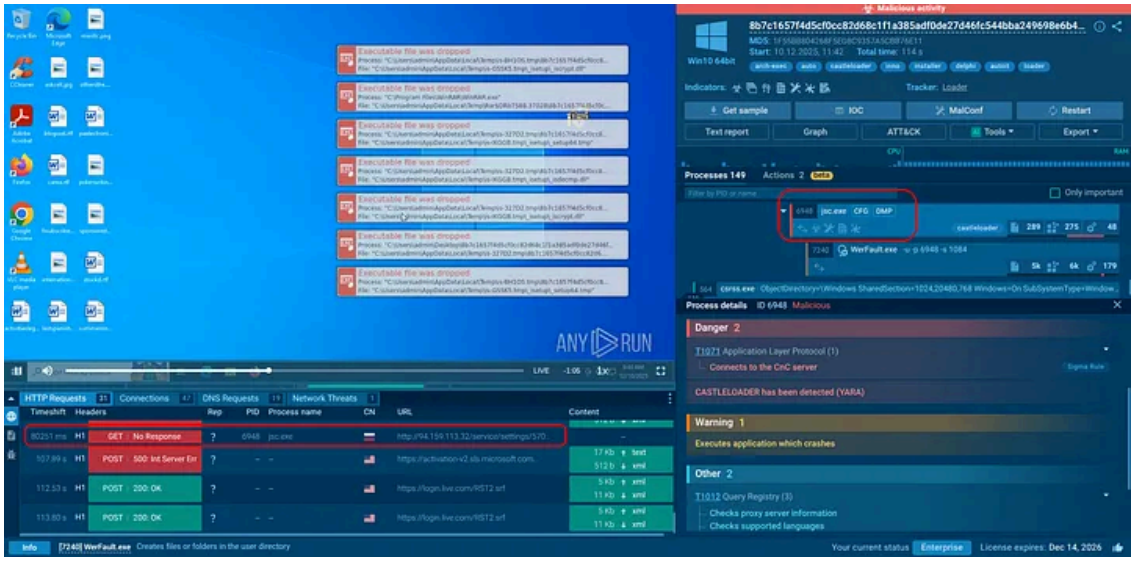
- Information Stealers: DeerStealer, RedLine, StealC, Rhadamanthys, MonsterV2 — These extract credentials from browsers, email clients, FTP clients, cryptocurrency wallets, and VPN software
- Remote Access Trojans: NetSupport RAT, SectopRAT, CastleRAT — These provide persistent backdoor access for command execution, file manipulation, and lateral movement
- Additional Loaders: Hijack Loader (GhostPulse) — These extend the infection chain, enabling deployment of even more malware variants.

Sandbox Analysis of CastleLoader Sample

ANY.RUN's analysts have detonated a CastleLoader sample in the Interactive Sandbox to extract runtime configuration, C2 infrastructure, and high-confidence IOCs.

View analysis

Press enter or click to view image in full size



CastleLoader dissected in the Interactive Sandbox

What instantly grabs attention here is a system process chain, at the end of which a request to 94[.]159[.]113[.]32:80 was sent.

Binary analysis shows that the process incorporates **Object Pascal** (Delphi) and **Inno Setup Module** (installer).

The static and dynamic analysis of the components reveals the path to the payload delivery. You can read the detailed analysis in ANY.RUN's Blog.

The original Inno Setup installer turned out to be a container with a set of auxiliary files, among which the **AutoIt3.exe + freely.a3x** combination played a key role. It is possible to extract and partially decompile the AutoIt script.

Static analysis showed that the script prepares the environment and launches the next stage, while dynamic analysis confirmed that after **jsc.exe** is started, one of the process hollowing techniques is executed: another executable module is injected into the process's address space.

As a result, a fully functional **PE file** — the main CastleLoader module — was discovered inside the process.

Such a sophisticated multi-stage execution chain was not implemented merely to complicate analysis, but specifically as an attempt to conceal the execution of the main payload from detection mechanisms. Using Inno Setup as a container, an AutoIt script as an intermediate layer, and process hollowing over jsc.exe, allows CastleLoader to distribute across several components that appear benign at first glance.

The execution model reduces the likelihood of detection, as each individual stage appears legitimate, and the final payload only manifests in memory after the controlled process has been altered. As a result, static signatures,

simple behavioral heuristics, and process monitoring systems become ineffective. A fully functional malicious module exists only at runtime, and only within an already modified process.

Gathering Threat Intelligence on CastleLoader Malware

ANY.RUN's Threat Intelligence Lookup provides critical capabilities for detecting, investigating, and responding to CastleLoader threats:

Rapid IOC Validation and Enrichment

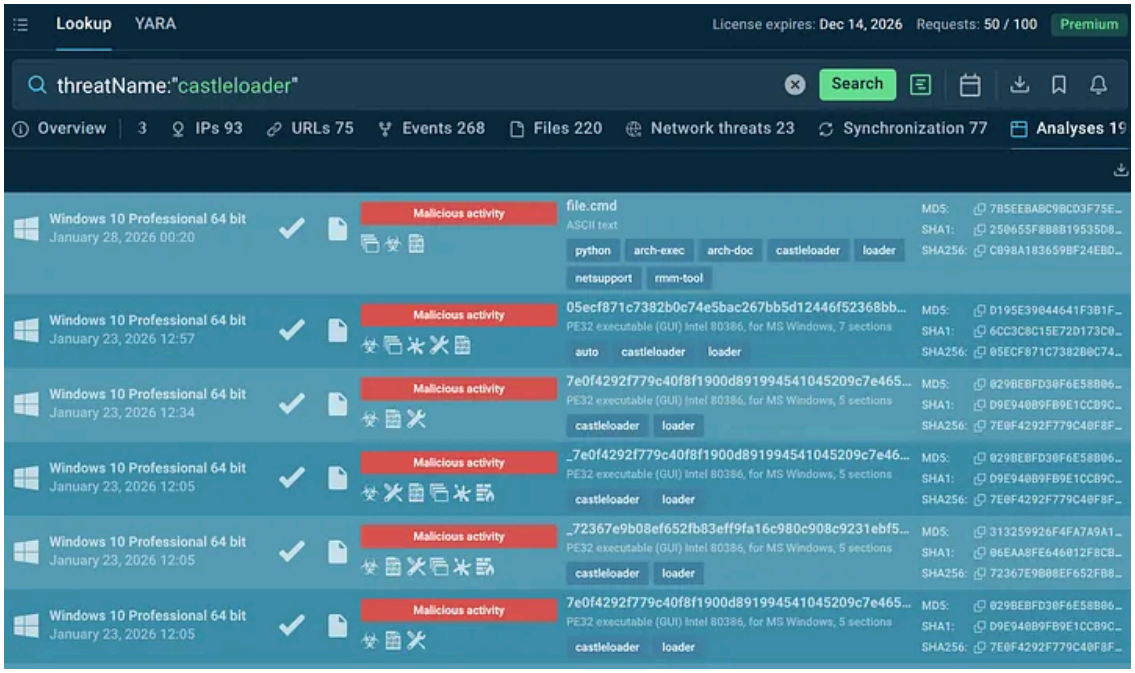
When security alerts trigger on potential CastleLoader indicators (IPs, domains, file hashes, PowerShell command patterns), SOC analysts can query TI Lookup to instantly determine if an indicator is associated with known CastleLoader campaigns. The platform provides contextual information including malware family classification, campaign attribution, and related artifacts — turning isolated indicators into actionable intelligence within seconds.

Deep Behavioral Analysis Access

TI Lookup provides direct links to interactive sandbox sessions where CastleLoader was analyzed. Analysts can observe the complete execution chain. Start exploring with the threat name lookup:

threatName:"castleloader"

Press enter or click to view image in full size



Fresh CastleLoader sandbox analyses found via TI Lookup

Comprehensive Event Correlation

With over 40 search parameters including registry keys, process command lines, network connections, file paths, and TLS fingerprints, analysts can investigate CastleLoader infections across multiple dimensions. For example,

searching for specific registry modifications or PowerShell patterns associated with ClickFix campaigns reveals all related samples and campaigns in the database.

YARA Rule Development and Testing

TI Lookup's integrated YARA Search allows security teams to scan ANY.RUN's threat intelligence database with custom detection rules. Teams can develop YARA rules targeting CastleLoader's unique characteristics (specific API call patterns, mutex names, shellcode signatures) and immediately test them against millions of analyzed samples to validate effectiveness and minimize false positives.

Threat Hunting Capabilities

Analysts can proactively search for CastleLoader indicators that may have bypassed initial detection.

Value for SOCs and MSSPs:

- Reduced Mean Time to Respond (MTTR);
- Lower False Positive Rates;
- Enhanced Detection Coverage;
- Improved Analyst Efficiency;
- Cost Optimization.

> *Integrate ANY.RUN's threat intelligence solutions in your company.*
> ***Contact us***

Conclusion

CastleLoader exemplifies how modern malware prioritizes access over immediate impact. By the time defenders notice the loader, the real damage may already be queued for deployment. Combating such threats requires not just detection, but context, speed, and intelligence-driven response. Threat intelligence turns CastleLoader from a silent entry point into a visible, disruptable operation.

Trial TI Lookup to start gathering actionable threat intelligence on the malware that threatens your business sector and region: just sign up to ANY.RUN.
