

CastleRAT attack first to abuse Deno JavaScript runtime to evade enterprise security

 threatdown.com/blog/castlerat-cyber-attack-is-the-first-to-abuse-deno-javascript-runtime-to-evade-enterprise-security

March 10, 2026



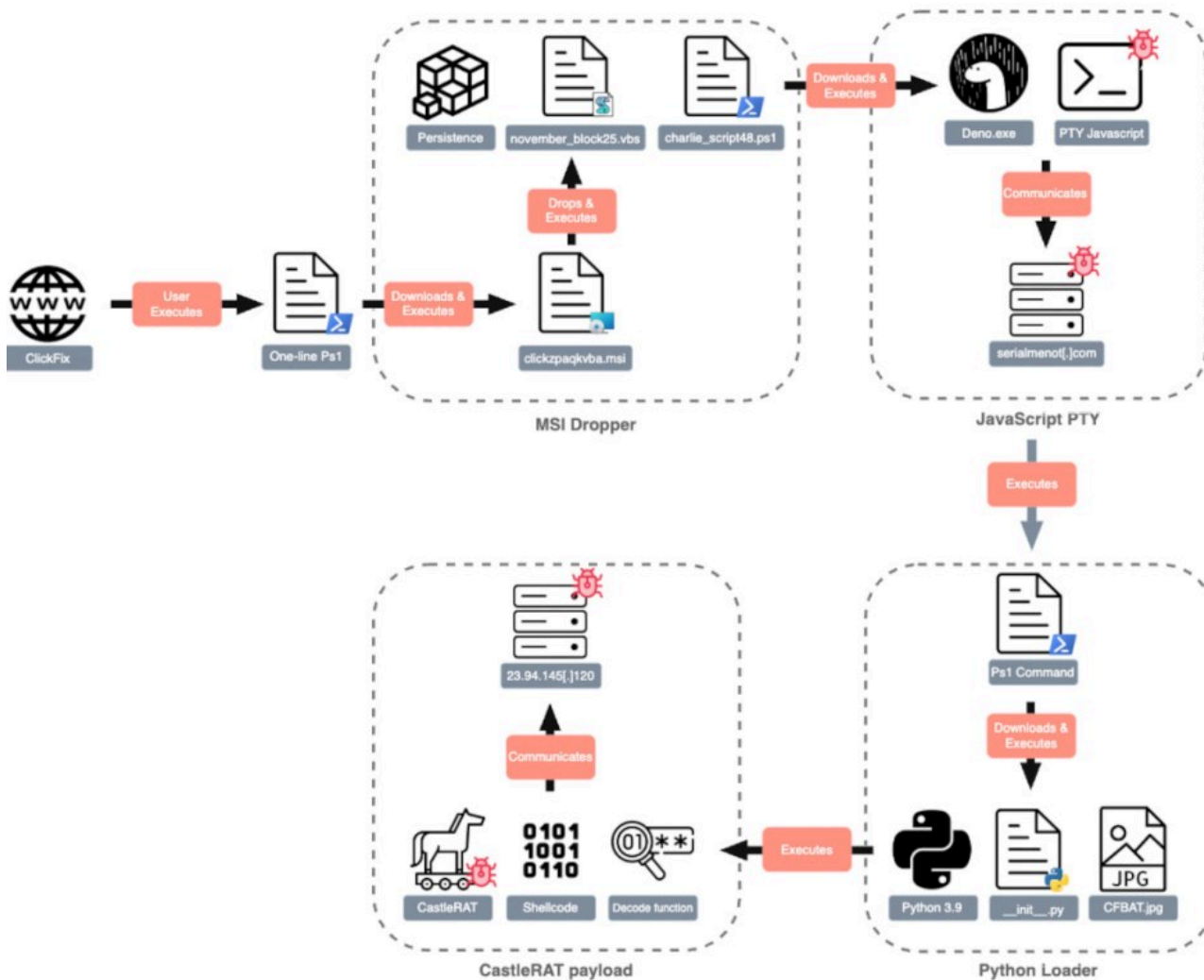
[Threats](#), [Threat Intelligence](#)

ThreatDown has discovered a sophisticated new infection chain that installs the CastleRAT malware without leaving a trace on disk.

[Lorenzo Corazzi](#)

In a recent investigation, the ThreatDown Research team analyzed a highly sophisticated infection chain that demonstrates just how creative threat actors are becoming. Notably, this campaign represents a significant milestone in offensive cyber-attack evolution: it is the first documented case of attackers abusing the Deno runtime as a malicious framework. The attack ultimately culminates in the installation of CastleRAT, a powerful tool for espionage and data theft. However, what makes this campaign particularly concerning is not just the final payload, but the incredible level of camouflage used to deliver it. By leveraging social engineering, pioneering the abuse of Deno, and hiding malicious code inside a seemingly harmless JPEG image, the attackers managed to create an infection that is virtually invisible to traditional security systems.

Here is how the perfect heist unfolds, step by step:



1. The “ClickFix” social engineering trap

The attack doesn’t begin with a complex exploit, but by targeting the weakest link in the chain: a user. The victim is lured to a compromised web page displaying a fake browser error message or a fake CAPTCHA check (“Verify you are human”). To “fix” the issue, the page instructs the user to manually copy and paste a command into the Windows terminal or the “Run” dialog.

This technique, known as ClickFix, bypasses web security filters because the user voluntarily executes the initial command themselves. This simple copy-and-paste action silently triggers the download of a malicious installer.

2. A first-of-its-kind “living off the land” tactic

Once an attacker has gained access, the attackers don't download the malware immediately. Instead, they prepare the ground using legitimate tools to avoid raising suspicion—and they do so in a completely novel way.

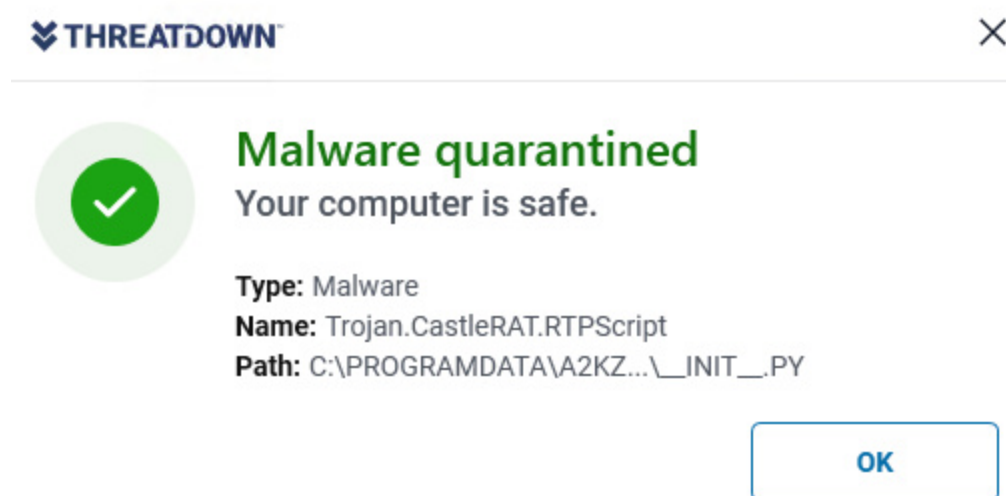
Article continues below this ad.

[Read the 2026 State of Malware](#)

The initial script downloads and installs Deno, a modern and secure JavaScript runtime used by developers worldwide. Because Deno is legitimate software with a valid digital signature, antivirus programs typically ignore it.

In what our researchers identify as an industry first, the attackers weaponize this specific framework, using Deno as a Trojan horse to execute obfuscated JavaScript code. Since the code runs inside a process that the system trusts, it inherits elevated privileges and full system access without triggering any alarms.

- **Espionage and keylogging:** CastleRAT captures all keyboard input by hooking into the operating system via the `SetWindowsHookEx()` API, silently logging keystrokes into hidden local files such as `%AppData%\Local\MashaLasley666`.
- **Clipboard hijacking:** Using dedicated monitoring threads, it continuously reads the clipboard to steal copied passwords and crypto addresses. It can also simulate paste actions via the `SendInput()` API to exfiltrate harvested data.
- **Digital identity and cryptocurrency theft:** It targets and extracts cookies, browsing history, saved browser credentials, browser extension data, and crypto wallet files. It also targets specific app session tokens, like those for Telegram Desktop and Discord, and developer SSH keys. It even leverages commands like `rundll32.exe shell32.dll, #61` to pop up the Windows Run dialog, tricking users into typing commands or credentials.
- **Audio and video surveillance:** It can secretly enumerate and initialize the victim's webcams and microphones using Windows media APIs like `MFEnumDeviceSources()` for media capture.
- **Invisible backdoor and persistence:** It provides an interactive backdoor shell to the attacker using anonymous IPC pipes, allowing full remote access with no visible console window. To survive system reboots, it silently registers a Scheduled Task via PowerShell (e.g., `VirtualSmokestGuy666`) that points right back to the obfuscated Python loader, ensuring the in-memory execution loop starts again.



Conclusion

The CastleRAT campaign is practical proof of how malware is evolving towards invisibility. By becoming the first threat actor to successfully co-opt the Deno framework, these attackers have shown that relying solely on analyzing files downloaded to the disk is no longer sufficient.

Defend against advanced threats like this requires endpoint behavioral monitoring. Platforms like ThreatDown can detect and block CastleRAT at multiple stages of its execution chain (identified as *Trojan.CastleLoader* and *Trojan.CastleRAT*), analyzing anomalies in process execution (such

as a Deno instance attempting in-memory injections) and severing communication with command and control (C2) servers before data can be stolen.

Partial list of indicators of compromise (IOCs)

Security teams can use the following indicators for threat hunting within their environments:

- **C2 domains:** dsennbuappec[.]zhivachkapro[.]com (ClickFix C2), serialmenot[.]com (JS loader C2)
- **IP addresses:** 172[.]86.123.222 (Python loader C2), 23[.]94.145.120 (CastleRAT C2)
- **Hashes (SHA256):**
 - bd8203ab88983bc081545ff325f39e9c5cd5eb6a99d04ae2a6cf862535c9829a (clickzpaqkvba.msi)
 - a4787a42070994b7f1222025828faf9b153710bb730e58da710728e148282e28 (CastleRAT PE)
- **Associated files and paths:** clickzpaqkvba.msi, november_block25.vbs, charlie_script48.ps1, CFBAT.jpg
- **Scheduled tasks:** VirtualSmokestGuy666

(For the complete list of file hashes, registry modifications, and YARA rules for detecting NightshadeC2/CastleRAT, please contact our Threat Intelligence team).

[CastleRAT Deno](#)

[Read the 2026 State of Malware](#)