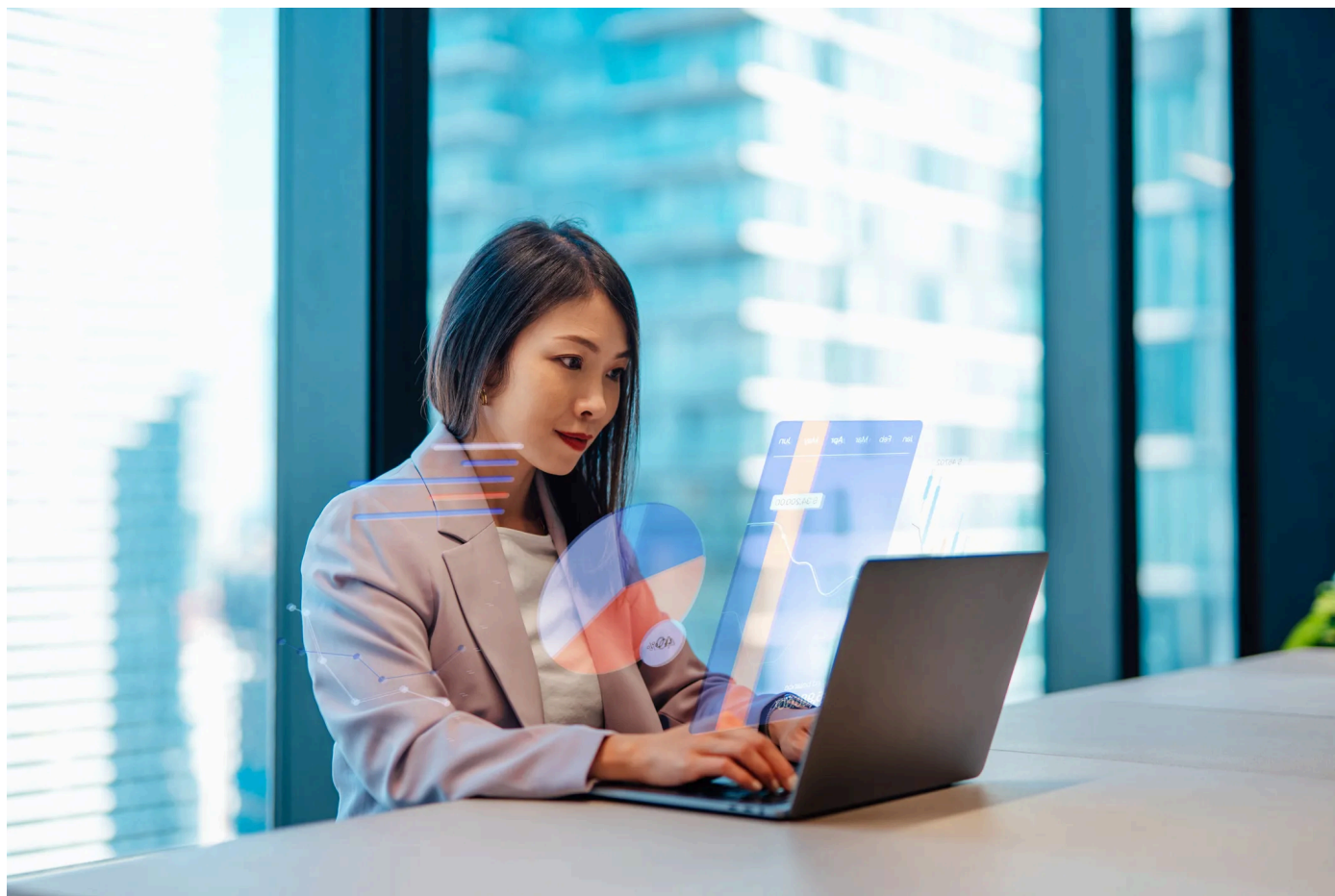


CastleLoader & CastleRAT: Behind TAG150's Modular Malware Delivery System

 darktrace.com/blog/castleloader-castlerat-behind-tag150s-modular-malware-delivery-system

Ahmed Gardezi

November 26, 2025



What is TAG-150?

TAG-150, a relatively new Malware-as-a-Service (MaaS) operator, has been active since March 2025, demonstrating rapid development and an expansive, evolving infrastructure designed to support its malicious operations. The group employs two custom malware families, CastleLoader and CastleRAT, to compromise target systems, with a primary focus on the United States [1]. TAG-150's infrastructure included numerous victim-facing components, such as IP addresses and domains functioning as command-and-control (C2) servers associated with malware families like SecTopRAT and WarmCookie, in addition to CastleLoader and CastleRAT [2].

As of May 2025, CastleLoader alone had infected a reported 469 devices, underscoring the scale and sophistication of TAG-150's campaign [1].

What are CastleLoader and CastleRAT?

CastleLoader is a loader malware, primarily designed to download and install additional malware, enabling chain infections across compromised systems [3]. TAG-150 employs a technique known as [ClickFix](#), which uses deceptive domains that mimic document verification systems or browser update notifications to trick victims into executing malicious scripts. Furthermore, CastleLoader leverages fake GitHub repositories that impersonate legitimate tools as a distribution method, luring unsuspecting users into downloading and installing malware on their devices [4].

CastleRAT, meanwhile, is a remote access trojan (RAT) that serves as one of the primary payloads delivered by CastleLoader. Once deployed, CastleRAT grants attackers extensive control over the compromised system, enabling capabilities such as keylogging, screen capturing, and remote shell access.

TAG-150 leverages CastleLoader as its initial delivery mechanism, with CastleRAT acting as the main payload. This two-stage attack strategy enhances the resilience and effectiveness of their operations by separating the initial infection vector from the final payload deployment.

How are they deployed?

Castleloader uses code-obfuscation methods such as dead-code insertion and packing to hinder both static and dynamic analysis. After the payload is unpacked, it connects to its command-and-control server to retrieve and running additional, targeted components.

Its modular architecture enables it to function both as a delivery mechanism and a staging utility, allowing threat actors to decouple the initial infection from payload deployment. CastleLoader typically delivers its payloads as Portable Executables (PEs) containing embedded shellcode. This shellcode activates the loader's core module, which then connects to the C2 server to retrieve and execute the next-stage malware.[6]

Following this, attackers deploy the ClickFix technique, impersonating legitimate software distribution platforms like Google Meet or browser update notifications. These deceptive sites trick victims into copying and executing PowerShell commands, thereby initiating the infection kill chain. [1]

When a user clicks on a spoofed Cloudflare "Verification Step" prompt, a background request is sent to a PHP script on the distribution domain (e.g., /s.php?an=0). The server's response is then automatically copied to the user's clipboard using the 'unsecuredCopyToClipboard()' function. [7].

The Python-based variant of CastleRAT, known as "PyNightShade," has been engineered with stealth in mind, showing minimal detection across antivirus platforms [2]. As illustrated in Figure 1, PyNightShade communicates with the geolocation API service ip-api[.]com, demonstrating both request and response behavior

Figure 1: Packet Capture (PCAP) of PyNightShade, the Python-based variant of CastleRAT, communicating with the geolocation API service ip-api[.]com.

Darktrace Coverage

In mid-2025, Darktrace observed a range of anomalous activities across its customer base that appeared linked to CastleLoader, including the example below from a US based organization.

The activity began on June 26, when a device on the customer's network was observed connecting to the IP address 173.44.141[.]89, a previously unseen IP for this network along with the use of multiple user agents, which was also rare for the user. It was later determined that the IP address was a known indicator of compromise (IoC) associated with TAG-150's CastleRAT and CastleLoader operations [2][5].

Figure 2: Darktrace's detection of a device making unusual connections to the malicious endpoint 173.44.141[.]89.

The device was observed downloading two scripts from this endpoint, namely '/service/download/data_5x.bin' and '/service/download/data_6x.bin', which have both been linked to CastleLoader infections by open-source intelligence (OSINT) [8]. The archives contains embedded shellcode, which enables attackers to execute arbitrary code directly in memory, bypassing disk writes and making detection by endpoint detection and response (EDR) tools significantly more difficult [2].

Figure 3: Darktrace's detection of two scripts from the malicious endpoint.

In addition to this, the affected device exhibited a high volume of internal connections to a broad range of endpoints, indicating potential scanning activity. Such behavior is often associated with reconnaissance efforts aimed at mapping internal infrastructure.

[Darktrace / NETWORK](#) correlated these behaviors and generated an Enhanced Monitoring model, a high-fidelity security model designed to detect activity consistent with the early stages of an attack. These high-priority models are continuously monitored and triaged by Darktrace's Security Operations Center (SOC) as part of the Managed Threat Detection and Managed Detection & Response services, ensuring that subscribed customers are promptly alerted to emerging threats.

Figure 4: Darktrace detected an unusual ZIP file download alongside the anomalous script, followed by internal connectivity. This activity was correlated under an Enhanced Monitoring model.

Darktrace Autonomous Response

Fortunately, Darktrace's Autonomous Response capability was fully configured, enabling it to take immediate action against the offending device by blocking any further connections external to the malicious endpoint, 173.44.141[.]89. Additionally, Darktrace enforced a 'group pattern of life' on

the device, restricting its behavior to match other devices in its peer group, ensuring it could not deviate from expected activity, while also blocking connections over 443, shutting down any unwanted internal scanning.

Figure 5: Actions performed by Darktrace's Autonomous Response to contain the ongoing attack.

Conclusion

The rise of the MaaS ecosystem, coupled with attackers' growing ability to customize tools and techniques for specific targets, is making intrusion prevention increasingly challenging for security teams. Many threat actors now leverage modular toolkits, dynamic infrastructure, and tailored payloads to evade static defenses and exploit even minor visibility gaps. In this instance, Darktrace demonstrated its capability to counter these evolving tactics by identifying early-stage attack chain behaviors such as network scanning and the initial infection attempt. Autonomous Response then blocked the CastleLoader IP delivering the malicious ZIP payload, halting the attack before escalation and protecting the organization from a potentially damaging multi-stage compromise

Edited by Ryan Traill (Analyst Content Lead)

Appendices

Darktrace Model Detections

- Anomalous Connection / Unusual Internal Connections
- Anomalous File / Zip or Gzip from Rare External Location
- Anomalous File / Script from Rare External Location
- Initial Attack Chain Activity (Enhanced Monitoring Model)

MITRE ATT&CK Mapping

- T15588.001 - Resource Development – Malware
- TG1599 – Defence Evasion – Network Boundary Bridging
- T1046 – Discovery – Network Service Scanning
- T1189 – Initial Access

List of IoCs

IoC - Type - Description + Confidence

- 173.44.141[.]89 – IP – CastleLoader C2 Infrastructure
- 173.44.141[.]89/service/download/data_5x.bin – URI – CastleLoader Script
- 173.44.141[.]89/service/download/data_6x.bin – URI - CastleLoader Script
- wsc.zip – ZIP file – Possible Payload

References

- [1] - <https://blog.polyswarm.io/castleloader>
- [2] - <https://www.recordedfuture.com/research/from-castleloader-to-castlerat-tag-150-advances-operations>
- [3] - <https://www.pcrisk.com/removal-guides/34160-castleloader-malware>
- [4] - <https://www.scworld.com/brief/malware-loader-castleloader-targets-devices-via-fake-github-clickfix-phishing>
- [5] <https://www.virustotal.com/gui/ip-address/173.44.141.89/community>
- [6] <https://thehackernews.com/2025/07/castleloader-malware-infected-469.html>
- [7] <https://www.cryptika.com/new-castleloader-attack-using-cloudflare-themed-clickfix-technique-to-infect-windows-computers/>
- [8] <https://www.cryptika.com/castlebot-malware-as-a-service-deploys-range-of-payloads-linked-to-ransomware-attacks/>

Inside the SOC

Darktrace cyber analysts are world-class experts in threat intelligence, threat hunting and incident response, and provide 24/7 SOC support to thousands of Darktrace customers around the globe. *Inside the SOC* is exclusively authored by these experts, providing analysis of cyber incidents and threat trends, based on real-world experience in the field.

Share this post

Latest blogs

[From Amazon to Louis Vuitton: How Darktrace Detects Black Friday Phishing Attacks](#)

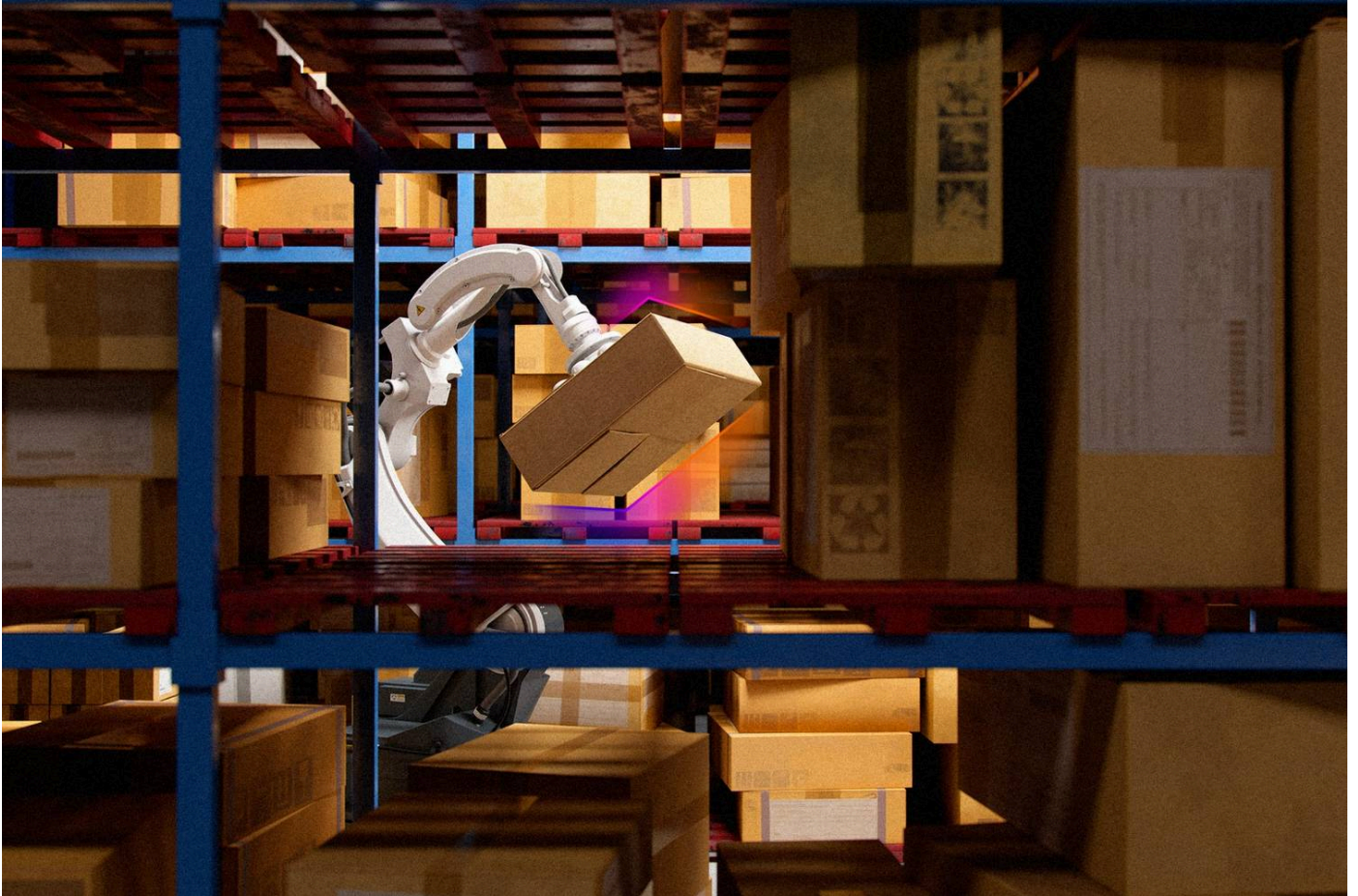
[Email](#)

•

[November 27, 2025](#)

[Ryan Traill](#)

[Analyst Content Lead](#)



[Phishing attacks surge by 620% in the lead-up to Black Friday.](#)

[Email](#)

[:](#)

[November 27, 2025](#)

[Carlos Gray](#)

[Senior Product Marketing Manager, Email](#)