From CastleLoader to CastleRAT: TAG-150 Advances Operations with Multi-Tiered Infrastructure

By Insikt Group®

Archived: 2026-04-05 18:50:43 UTC

Executive Summary

Insikt Group has identified a new threat actor, TAG-150, active since at least March 2025, characterized by rapid development, technical sophistication, responsiveness to public reporting, and a large, evolving infrastructure. The infrastructure linked to TAG-150 includes both victim-facing Tier 1 components, such as IP addresses and domains used as command-and-control (C2) servers for multiple malware families, and higher-tier infrastructure composed of multiple layers. Since emerging in March 2025, TAG-150 has deployed multiple likely self-developed malware families, starting with CastleLoader and CastleBot, and most recently CastleRAT, a remote access trojan documented here for the first time. Additionally, Insikt Group has identified multiple services likely leveraged by TAG-150, including file-sharing platforms, anti-detection services, and others.

To protect against TAG-150, security defenders should block IP addresses and domains tied to associated loaders, infostealers, and RATs, flag and potentially block connections to unusual LIS such as Pastebin, and deploy updated detection rules (YARA, Snort) for current and historical infections. Other controls include implementing email filtering and data exfiltration monitoring. See the **Mitigations** section for implementation guidance and **Appendix A** for a complete list of indicators of compromise (IoCs). In the long term, analysts should continuously monitor the cybercriminal ecosystem for emerging threats and adapt controls accordingly.

Key Findings

- Insikt Group uncovered a large infrastructure set operated by the threat actor tracked as TAG-150, known for deploying malware such as CastleLoader. The infrastructure follows a multi-tiered model, with victim-facing Tier 1 servers as well as higher-level Tier 2, Tier 3, and Tier 4 infrastructure.
- In addition, Insikt Group identified a new remote access trojan linked to TAG-150, dubbed CastleRAT. Available in both Python and C variants, CastleRAT's core functionality consists of collecting system information, downloading and executing additional payloads, and executing commands via CMD and PowerShell.
- Further analysis also provides insights into TAG-150’s broader tool set and operational ecosystem, which leverages multiple file-sharing services, messaging platforms, and specialized utilities, including the anti-detection service Kleenscan (*kleenscan[.]com*).

Background

TAG-150 is Insikt Group’s designation for the threat actor linked to the development and use of the malware families CastleLoader, CastleBot, and, more recently, CastleRAT. They have been active since at least March 2025

(see **Figure 1**). These malware families are frequently observed as initial infection vectors that deliver a wide range of secondary payloads, including SectopRAT, WarmCookie, HijackLoader, NetSupport RAT, as well as numerous information stealers such as Stealc, RedLine Stealer, Rhadamanthys Stealer, DeerStealer, MonsterV2, among others (1, 2).

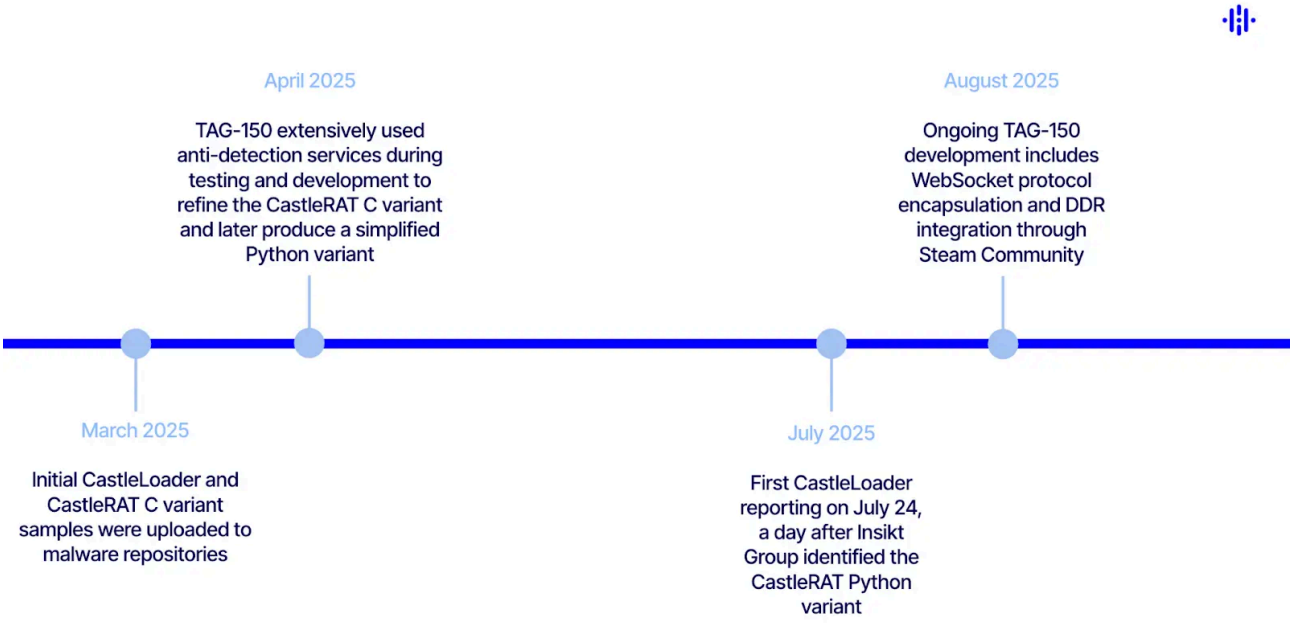

***Figure 1**: Timeline of TAG-150 activity (Source: Recorded Future)*

Infections are most commonly initiated through Cloudflare-themed “ClickFix” phishing attacks or fraudulent GitHub repositories masquerading as legitimate applications. The operators employ the ClickFix technique by leveraging domains that imitate software development libraries, online meeting platforms, browser update alerts, and document verification systems. Victims are tricked into copying and executing malicious PowerShell commands on their own devices, thereby enabling the compromise. Public reporting indicates that although overall clicks and downloads were limited, the 28.7% infection rate among victims who interacted with malicious links underscores the effectiveness of TAG-150.

Prior public reporting has suggested that TAG-150 operates on a Malware-as-a-Service (MaaS) model, which is supported by its use in delivering a wide variety of second-stage payloads, the number of observed CastleLoader admin panels, and the presence of features commonly associated with MaaS platforms (as noted by PRODAFT). However, Insikt Group has not identified any advertisements or discussions of such services on underground forums. Furthermore, Recorded Future Network Intelligence analysis suggests that TAG-150 primarily interacts with its associated infrastructure, with only a small number of other IP addresses, potentially linked to external customers or affiliates, communicating with it. This network traffic, potentially associated with external customers or affiliates, is largely connected to Tor nodes, which complicates its classification.

Infrastructure Analysis

Insikt Group identified an extensive, multi-tiered infrastructure tied to TAG-150. The infrastructure consists of Tier 1 victim-facing C2 servers associated with malware families such as CastleLoader, SecTopRAT,

WarmCookie, and the newly discovered CastleRAT, as well as Tier 2, Tier 3, and Tier 4 servers, the latter of which are likely used for backup purposes. **Figure 2** provides an overview of the entire infrastructure, while subsequent sections explore each component in greater detail.

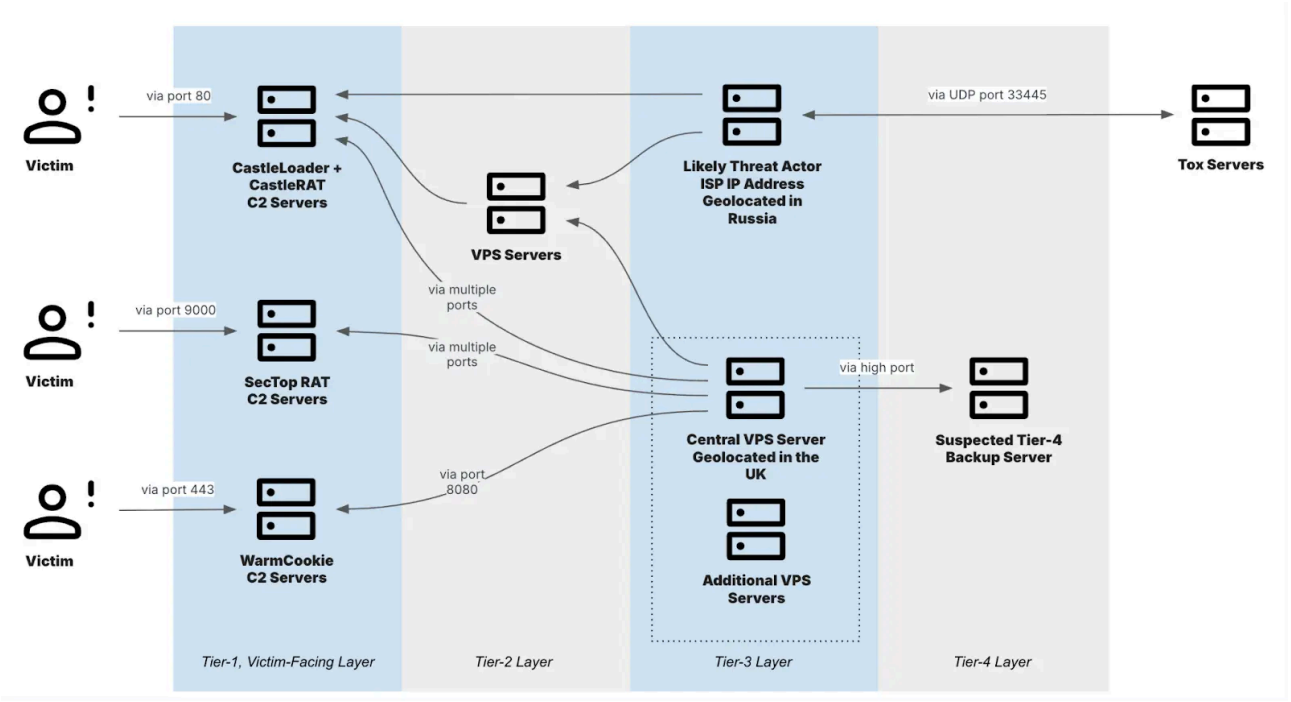

***Figure 2**: Multi-tiered infrastructure linked to TAG-150 (Source: Recorded Future)*

Multi-Tiered Infrastructure

Tier 1

Tier 1 infrastructure comprises numerous C2 servers associated with various malware families, such as CastleLoader, CastleRAT, SecTopRAT, and WarmCookie, among others. These servers are generally managed through Tier 2 servers, though in some cases, Tier 3 servers interact directly with them.

CastleLoader

Insikt Group identified a significant number of CastleLoader C2 servers associated with TAG-150, as outlined in **Appendix B**. These servers' IP addresses often host domains registered through NameCheap, Inc. or TUCOWS, INC., though the domains do not adhere to any consistent naming convention. While CastleLoader C2 infrastructure has been observed across various autonomous system numbers (ASNs), a considerable portion is tied to the hosting providers servinga GmbH, FEMO IT SOLUTIONS LIMITED, and Eonix Corporation. FEMO IT SOLUTIONS LIMITED is assessed as a threat activity enabler (TAE) and is actively tracked by Insikt Group.

Among the domains analyzed, *panelv1[.]hostingzealoft[.]today* stood out, as it mimics the legitimate domain of a known hosting provider, *hostingzealot[.]com*, which also hosts the IP address associated with this domain. The reason for this naming choice remains unclear. Beyond this, TAG-150 does not seem to follow a consistent naming convention or thematic pattern across the other domains.

CastleLoader Admin Panel

Most CastleLoader C2 servers observed by Insikt Group provide both C2 functionality, primarily on port 80, and an admin panel, typically hosted on port 5050 and occasionally on port 9999. **Figure 3** illustrates an example of a CastleLoader admin panel.

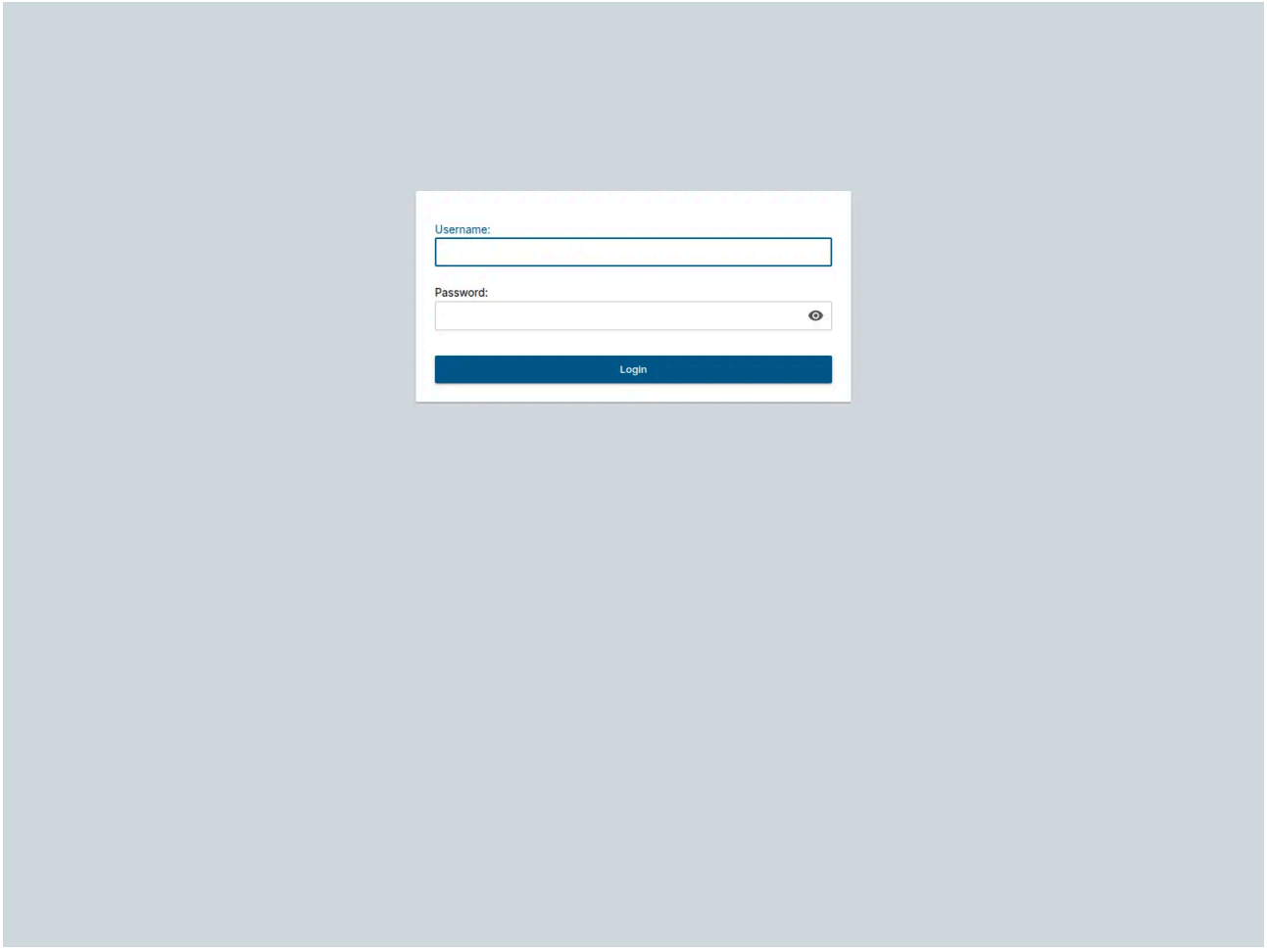

Figure 3: *CastleLoader C2 admin panel (Source: URLScan)*

CastleRAT

Beyond CastleLoader and CastleBot, which have been previously reported on, Insikt Group has identified a new malware family, dubbed CastleRAT, which is detailed further in the **CastleRAT** section. Insikt Group discovered both C and Python variants of CastleRAT. **Appendix B** lists the CastleRAT C2 servers, typically exposed on ports 80, 443, 7777, and occasionally on other ports. CastleRAT C2 servers have been observed across multiple ASNs, with one particularly notable instance hosted on a Google Cloud IP address.

SectopRAT

Insikt Group identified at least seven SectopRAT C2 servers associated with TAG-150, six of which were accessed through TAG-150's higher-tier infrastructure (see **Appendix B**). The primary channels for C2 communication are TCP ports 15647, 15747, 15847, 15947, 14367, or 9000. In **Appendix B**, the first and last seen dates represent the

earliest and latest instances in which these servers were observed communicating with TAG-150's higher-tier infrastructure. The IP address *92[.]255[.]57[.]32* has not been observed communicating with TAG-150's higher-tier infrastructure; however, it is assessed to be associated with TAG-150 due to observed overlaps among victims.

During analysis, Insikt Group also identified IP address *91[.]210[.]164[.]26*, which is potentially linked to TAG-150 but has not been observed talking to TAG-150's higher-tier infrastructure.Notably, IP address 176[.]126[.]163[.]56 hosts a self-signed transport layer security (TLS) certificate with the common name krona186380. During analysis, Insikt Group also identified IP address 91[.]210[.]164[.]26 within the same ASN, which presented a similar self-signed TLS certificate with the common name krona184679. Although no samples or higher-tier infrastructure communications have been observed with this IP address, Insikt Group assesses it may be linked to TAG-150 due to these similarities.

During analysis, Insikt Group also identified IP address 91[.]210[.]164[.]26, which is potentially linked to TAG-150 but has not been observed talking to TAG-150's higher-tier infrastructure.

WarmCookie

Insikt Group identified at least one WarmCookie C2 server associated with TAG-150, as detailed in **Appendix B**. This same IP address had previously been reported in connection with CastleLoader. The campaign IDs linked to the observed WarmCookie samples were `traffic1` and `traffic2`. The SHA256 hash of the campaign ID is used to construct the CastleLoader GET request endpoint, which is suspected to be the prerequisite for retrieving the correct follow-on payload(s).

Tier 2

Insikt Group identified Tier 2 VPS servers likely functioning as intermediaries between victim-facing Tier 1 servers and the Tier 3 infrastructure. Specifically, TAG-150 was observed accessing Tier 2 servers via RDP port 3389 before subsequently connecting to Tier 1 servers over a variety of other ports. Connections were observed to CastleLoader, CastleRAT, SectopRAT, and WarmCookie, among others. Notably, in several instances, TAG-150 bypassed Tier 2 entirely, connecting directly from the Tier 3 layer to Tier 1 servers. Insikt Group assesses this behavior as either a shift in operational procedures by the same operators associated with TAG-150 or the result of different operators employing alternative methods.

Tier 3

TAG-150's Tier 3 infrastructure appears to be split into two parts. On one side, Insikt Group identified a set of VPS servers all using the same TLS certificate, with one server standing out as the likely hub based on heavy traffic and observed links to what's assessed as Tier 4, which is discussed in the next section.

Separately, Insikt Group identified a Russian residential IP address assessed as Tier 3, which has been observed communicating with both Tier 2 and Tier 1 servers. The Russian IP address is announced by AS35807 (AS-SKYNET-SPB). This separation between VPS infrastructure and the residential IP address could signal the presence of a second operator tied to TAG-150. Of note, the Russian residential IP has been observed

communicating regularly with Tox servers via the default user datagram protocol (UDP) port of 33445, suggesting that TAG-150 leverages Tox for its internal communications.

Tier 4

The primary Tier 3 server has been observed communicating with another server, which Insikt Group assesses to be a potential backup server, over a persistent high-port-to-high-port UDP session spanning several weeks. This server is tracked as a Tier 4 server. The Tier 4 server is associated with an IP address announced by AS204601 (ON-LINE-DATA), and in at least one instance, was observed communicating directly with a CastleLoader panel, an activity assessed as an operational security lapse.

Additionally, Insikt Group identified another set of servers likely part of Tier 4.

Services Used by TAG-150

Through monitoring TAG-150's activities using Recorded Future Network Intelligence and other sources, Insikt Group has assessed that TAG-150 is highly likely leveraging a range of operational resources. These include the Oxen network (formerly Lokinet), which provides infrastructure for privacy-focused applications such as secure messaging platforms; Kleenscan (*kleenscan[.]com*), an alternative to the recently dismantled AVCheck; the file-sharing service *temp[.]sh*; the cryptocurrency exchange *simpleswap[.]io*; the file hosting service *mega[.]nz*; and, additionally, Exploit Forum, which the group is also likely to use. Insikt Group has previously noted that following AVCheck's disruption, other cybercriminals, including Lumma affiliates, began using Kleenscan. In June 2025, Insikt Group identified TAG-150 briefly interacting with a Matanbuchus Loader panel hosted on *185[.]39[.]19[.]164*.

Payload Delivery Infrastructure

Insikt Group discovered several payload delivery domains associated with CastleLoader, most of which are hosted behind Cloudflare, with a single exception. All related indicators are provided in **Appendix B**.

Potential Play Ransomware Activity

During the investigation of TAG-150 activity, Insikt Group identified a French ISP IP that communicated with both the CastleLoader panel on the IP address *107[.]158[.]128[.]45* and with a WarmCookie C2 server *192[.]36[.]57[.]164*. Of note, this WarmCookie C2 server was observed in network exfiltration involving an IP address linked to a known Play Ransomware victim. Since the timing of the exfiltration coincides with the victim organization's Play Ransomware compromise, Insikt Group assesses it is possible that Play Ransomware or one of their affiliates used CastleLoader.

While Insikt Group did not find the full infection chain linking the specific WarmCookie and CastleLoader instances, a WarmCookie sample with the same mutex was identified, which had been deployed via CastleLoader. This finding increases the likelihood that the WarmCookie sample associated with *192[.]36[.]57[.]164* was also deployed through CastleLoader, and may therefore be directly connected to *107[.]158[.]128[.]45*.

To date, however, no public reporting has associated Play Ransomware with either WarmCookie or CastleLoader. It therefore remains possible that the victim was targeted by multiple threat actors and that the WarmCookie infection was unrelated to the Play Ransomware incident.

CastleRAT is a RAT that includes C and Python variants sharing the following commonalities:

- Custom binary protocol using RC4 encryption with hard-coded 16-byte keys
- Queries the geolocation API *ip-api[.]com* to obtain location and other information through the infected host's public IP address
- Download and execution of executables
- Remote shell

The C variant of CastleRAT also includes more advanced stealing capabilities, such as keylogging and screen capturing. Both variants are in continual development. For example, C2 deaddrops hosted on Steam Community pages is a new development, first observed in late August 2025 (see **Figure 4**).

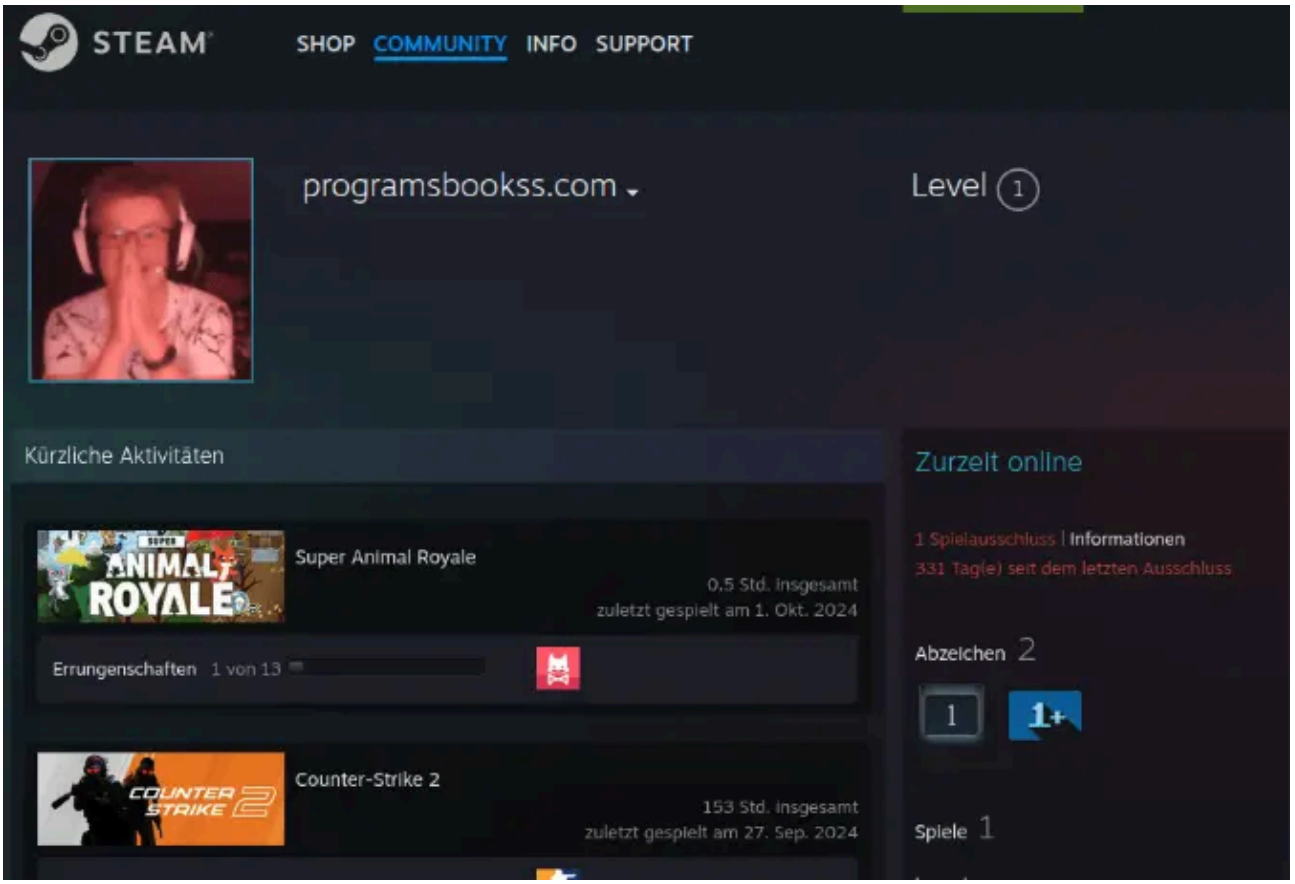

***Figure 4**: TAG-150's CastleRAT using Steam Community for dead drop resolving (Source: Recorded Future)*

Notably, although CastleRAT has so far only been observed deployed alongside CastleLoader and its infrastructure shows clear links to TAG-150, this does not necessarily indicate that CastleRAT was developed by the same actor(s) behind CastleLoader; it remains possible that the malware was obtained elsewhere.

CastleRAT Python Variant

CastleRAT is a lightweight RAT first identified by Insikt Group in early August 2025 as a CastleLoader payload. Notably, this Python variant of the malware was publicly referenced in late August under the name PyNightshade, though it remained otherwise undocumented.

The C variant of CastleRAT has yet to be publicly identified, but is flagged by numerous generic antivirus detections not specifically linked to any malware family. It is therefore plausible that the Python variant of CastleRAT was designed with stealth in mind, as it currently exhibits zero or very few antivirus detections. The following features have been implemented and unchanged since the CastleRAT Python variant was first observed in late July 2025:

- Obtain and report country info of the public IP and system information
- Generate ping/keep-alive messages every three seconds
- Download and execute executables (EXEs) or dynamic-link libraries (DLLs)
- Run and report the output of cmd shell commands
- Run and report the output of PowerShell commands
- Self-delete

The country information is retrieved from the well-known IP Geolocation service *ip-api[.]com*. The field's status and country are queried (see **Figure 5**).

```
GET /line/?fields=16385 HTTP/1.1
Connection: Keep-Alive
Host: www.ip-api.com

HTTP/1.1 200 OK
Date: Sun, 03 Aug 2025 03:58:43 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 23
Access-Control-Allow-Origin: *
X-Ttl: 60
X-Rl: 44

success
United Kingdom
```

Figure 5*: CastleRAT Python variant request and response to Geolocation API service ip-api[.]com (Source: Recorded Future)*

The Recorded Future Malware Intelligence query shown in **Figure 6** can be used to hunt for CastleRAT Python variants.

Insikt Group assesses that the Python variant of CastleRAT remains under active development. Recent updates introduced features such as encapsulating the binary protocol within WebSockets and leveraging Steam Community pages for C2 dead drops.

CastleRAT C Variant

The C variant of CastleRAT incorporates significantly more functionality than the Python variant, which likely increases its susceptibility to detection by generic antivirus solutions:

- Obtain and report the country and other info of the public IP and system information
- Generate ping/keep-alive messages every six seconds
- Keylogger
- Clipper
- Screencapture
- File Upload
- File Download
- Find and terminate browser processes
- Run and report the output of shell commands
- Run and report the output of PowerShell commands
- Register and un-register persistence
- Execute files via injection or masquerading as a browser
- C2 deaddrops via Steam Community pages

As with the Python variant, the C variant queries the widely abused IP geolocation service *ip-api[.]com* to collect information based on the infected host's public IP address. However, the scope of data has been expanded to include the city, ZIP code, and indicators of whether the IP is associated with a VPN, proxy, or Tor node (see **Figure 7**).

```
GET /line/?fields=147505 HTTP/1.1
Connection: Keep-Alive
Host: www.ip-api.com


HTTP/1.1 200 OK
Date: Tue, 01 Jul 2025 17:37:26 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 40
Access-Control-Allow-Origin: *
X-Ttl: 55
X-Rl: 42

success
United Kingdom
London
EC1N
true
```

Figure 7*: CastleRAT C variant request and response to Geolocation API service ip-api[.]com (Source: Recorded Future)*

Recent versions of the C variant of CastleRAT have removed querying of the city and ZIP code from the *ip-api[.]com* output (see **Figure 8**).

```
GET /line/?fields=147457 HTTP/1.1
Connection: Keep-Alive
Host: www.ip-api.com

HTTP/1.1 200 OK
Date: Fri, 22 Aug 2025 17:21:02 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 28
Access-Control-Allow-Origin: *
X-Ttl: 60
X-Rl: 44

success
United Kingdom
true
```

***Figure 8**: CastleRAT C variant request and response to Geolocation API service ip-api (Source: Recorded Future)*

The Recorded Future Malware Intelligence query shown in **Figure 9** can be used to hunt for CastleRAT C variants.

***Figure 9**: Recorded Future Malware Intelligence query to hunt for CastleRAT C variant (Source: Recorded Future)*

CastleRAT C variant uses the following unique Mutex objects for synchronization:

- Thickwick3
- fsAiodwsfSAFuiefS
- BabaiMazai
- sPEJIOGDsionsgfdUewg
- KolokolBozhii
- FkgfIJGgJgdiJGDGHDjMGjia
- sdgiregdsssaFWIFS
- fsAiodwsfSAFuiefS2
- GoldVekRogerS
- XmGetzKAM8Bw8NCBTUYo5e

It is uncertain whether the Python variant will be updated to incorporate the data-stealing features of the C variant, as well as what additional capabilities the developers may introduce for detection evasion.

Victimology

Insikt Group identified numerous suspected victim IP addresses communicating with the Tier 1 C2 infrastructure associated with TAG-150's various malware families. While the majority of these IP addresses appear to be geolocated in the United States, only a limited number of actual victims could be positively identified. Most victims remain unidentified and cannot be confirmed; however, Insikt Group assesses it is likely that at least some of them represent private individuals who became infected.

Mitigations

- Leverage the IoCs in **Appendix A** to investigate potential past or ongoing infections, both successful and attempted, and use the Recorded Future Intelligence Cloud to monitor for future IoCs associated with TAG-150 and other threat actors.
- Leverage Sigma, YARA, and Snort rules provided in **Appendices C**, **D**, and **E** in your SIEM or endpoint detection and response (EDR) tools to detect the presence or execution of CastleLoader and CastleRAT. In addition, use other detection rules available in the Recorded Future Intelligence Cloud.
- Use Recorded Future Network Intelligence to detect instances of data exfiltration from your corporate infrastructure to known malicious infrastructure. This can be achieved by employing specific queries and filtering the results based on your assets.
- Use the Recorded Future Intelligence Cloud to monitor TAG-150, other threat actors, and the broader cybercriminal ecosystem, ensuring visibility into the latest TTPs, preferred tools and services (for example, specific TAEs used by threat actors), and emerging developments.

Outlook

Insikt Group assesses that TAG-150 will continue to evolve its tooling at a rapid pace, with a particular emphasis on stealth and evasion. TAG-150 has already demonstrated technical sophistication and adaptability and Insikt Group anticipates it will further experiment with anti-detection services and techniques to remain resilient against defensive measures.

Given its history of deploying multiple likely self-developed malware families, including CastleLoader, CastleBot, and now CastleRAT, TAG-150 is highly likely to develop and release additional malware in the near term. Insikt Group also assesses that there is a strong possibility that the group will expand its distribution efforts, whether to increase victim reach or potentially operate in a MaaS capacity.

Insikt Group will continue to closely monitor TAG-150’s infrastructure, tool development, and activity across underground forums to track emerging threats and assess the group’s trajectory.
