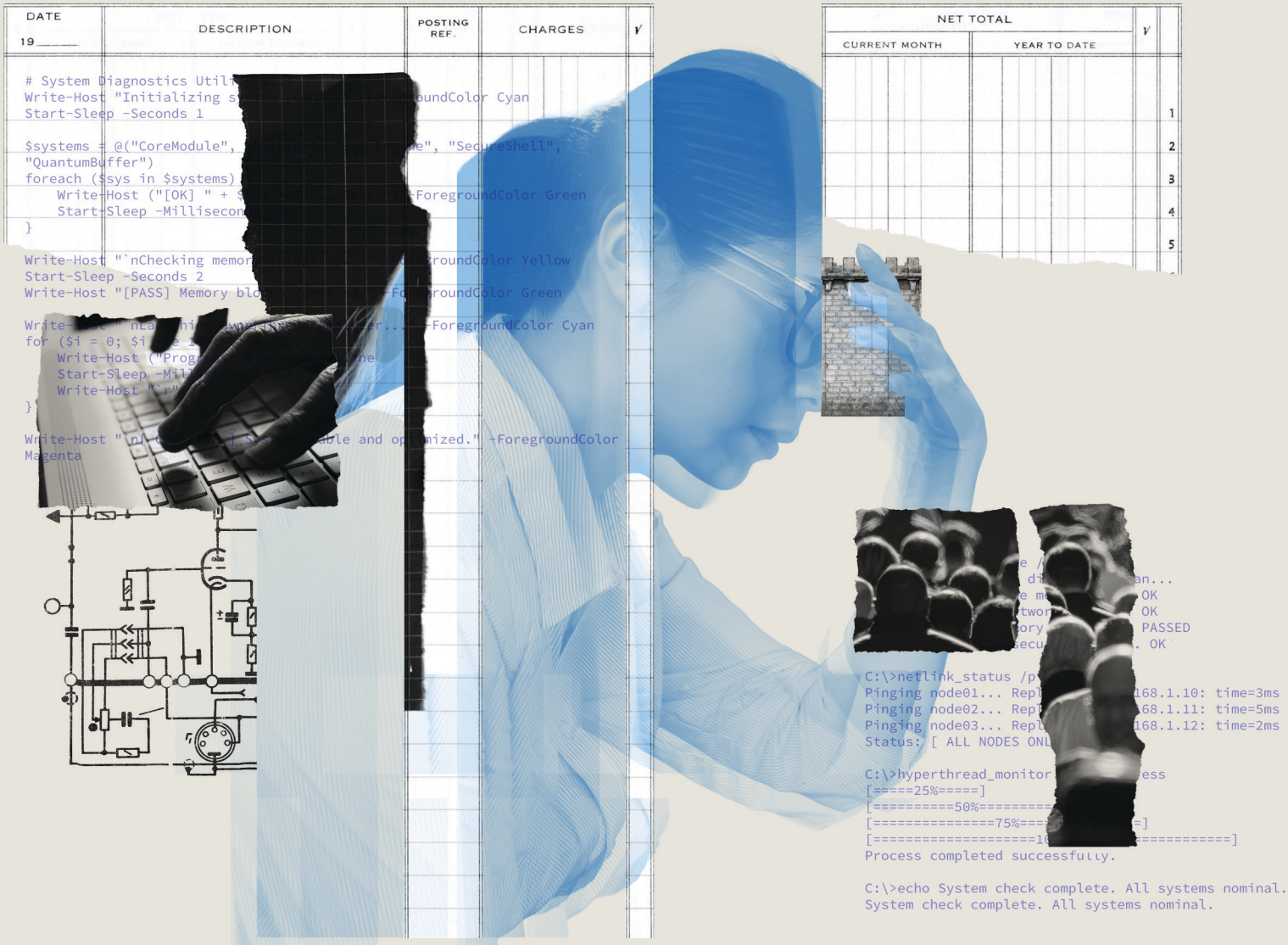
CYBER THREAT ANALYSIS

Recorded Future®

By Insikt Group®

September 4, 2025



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

Insikt Group discovered TAG-150's large multi-tier infrastructure, consisting of victim-facing C2 servers, as well as higher-level servers used for administration.

Insikt Group discovered CastleRAT, a TAG-150 RAT in Python and C, designed to gather system data, deliver payloads, and execute commands via CMD and PowerShell.

Further analysis reveals TAG-150's wider toolkit and ecosystem, using file-sharing services, messaging platforms, and utilities like the anti-detection service Kleenscan.

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).

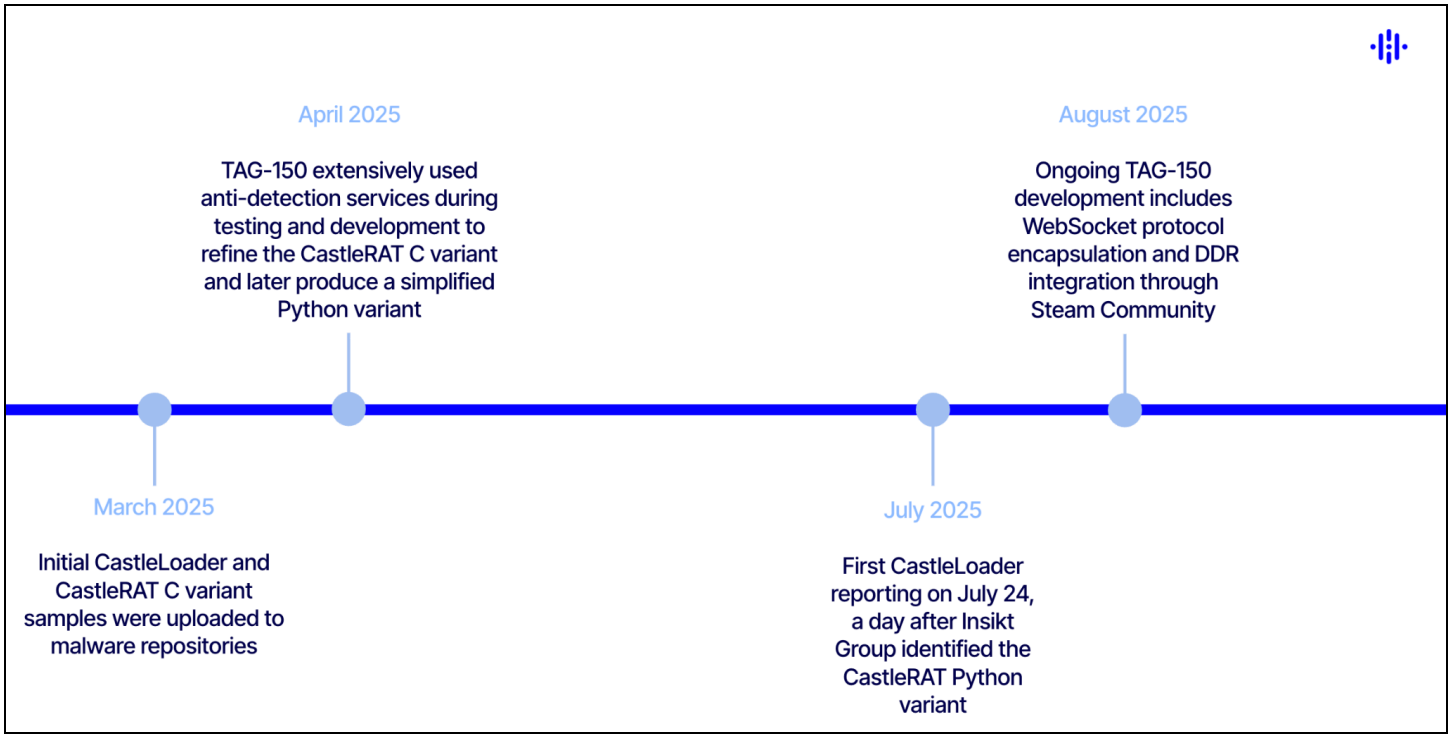


***Figure 1**: Timeline of TAG-150 activity (Source: Recorded Future)*

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.

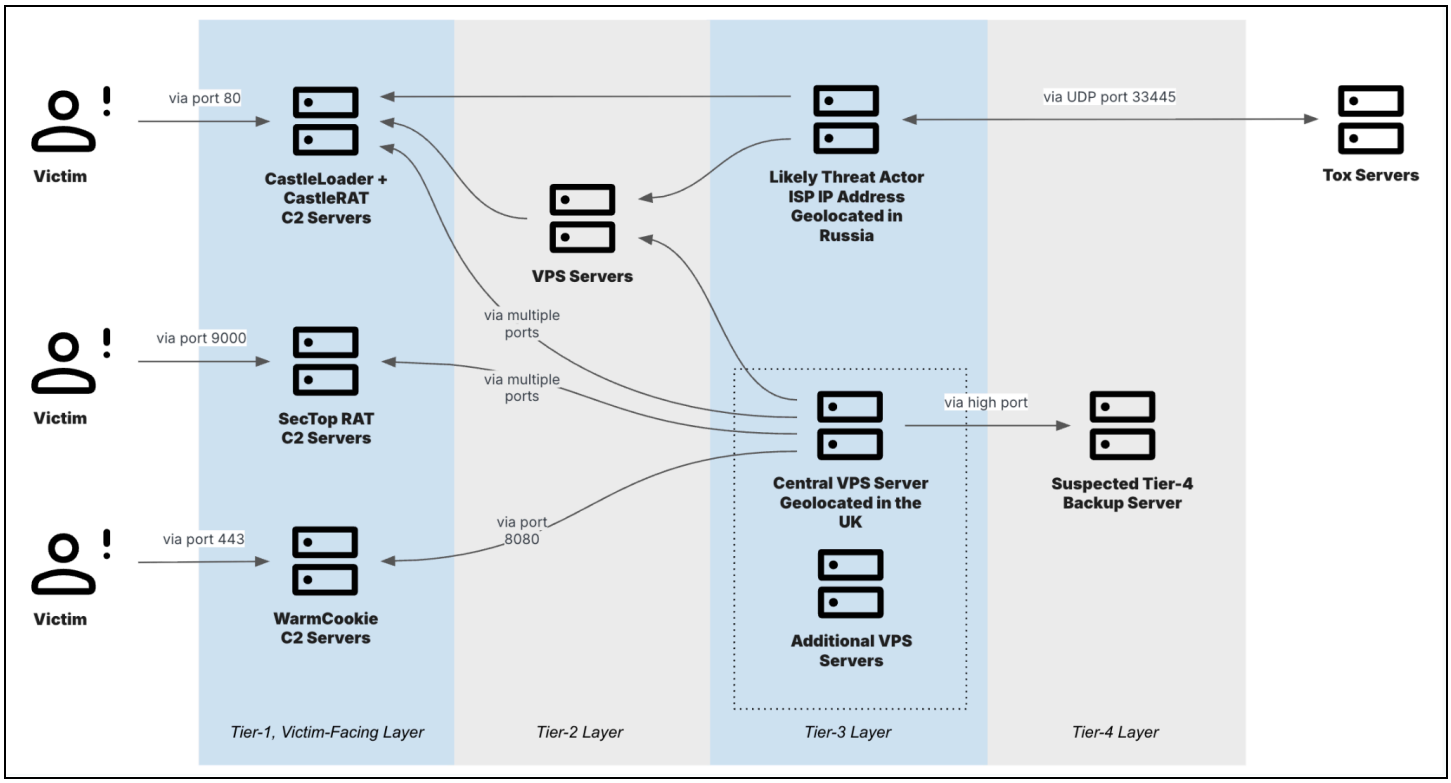


***Figure 2**: Multi-tiered infrastructure linked to TAG-150 (Source: Recorded Future)*

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.

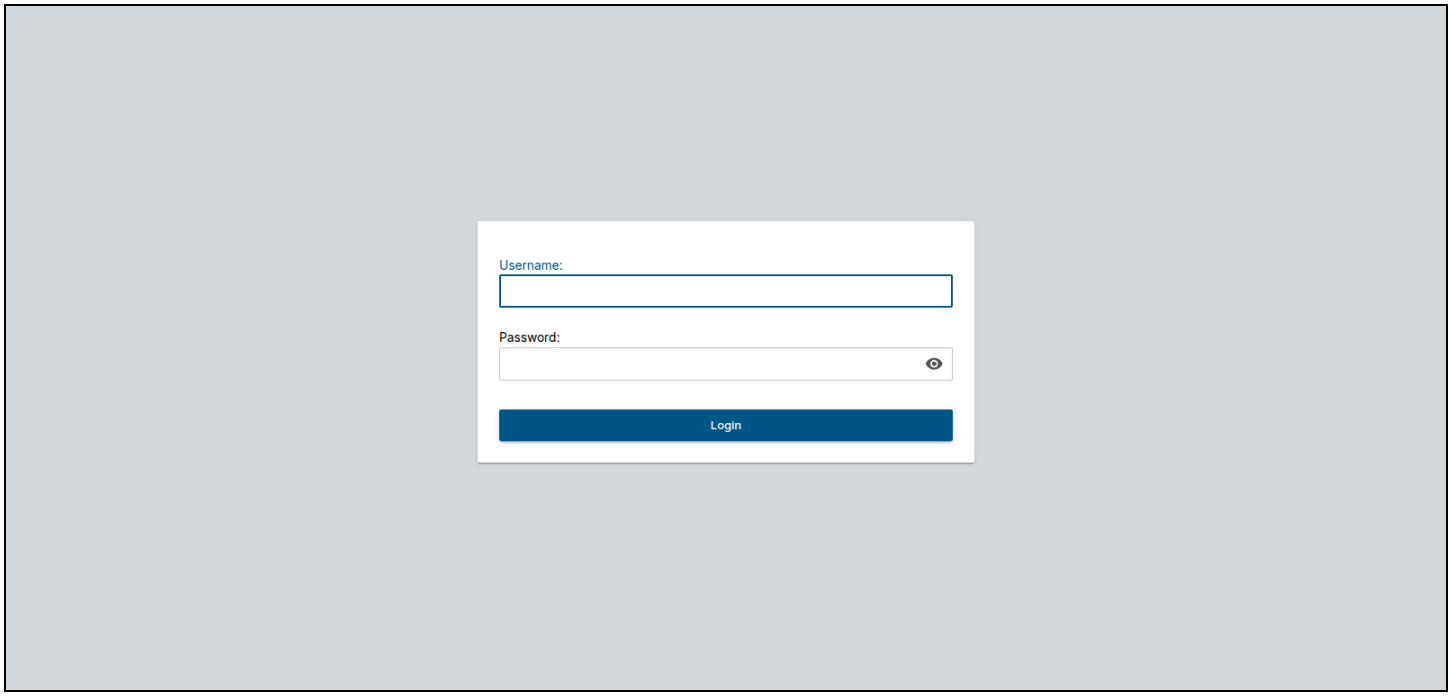


Figure 3: *CastleLoader C2 admin panel (Source: URLScan)*

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.

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

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**).

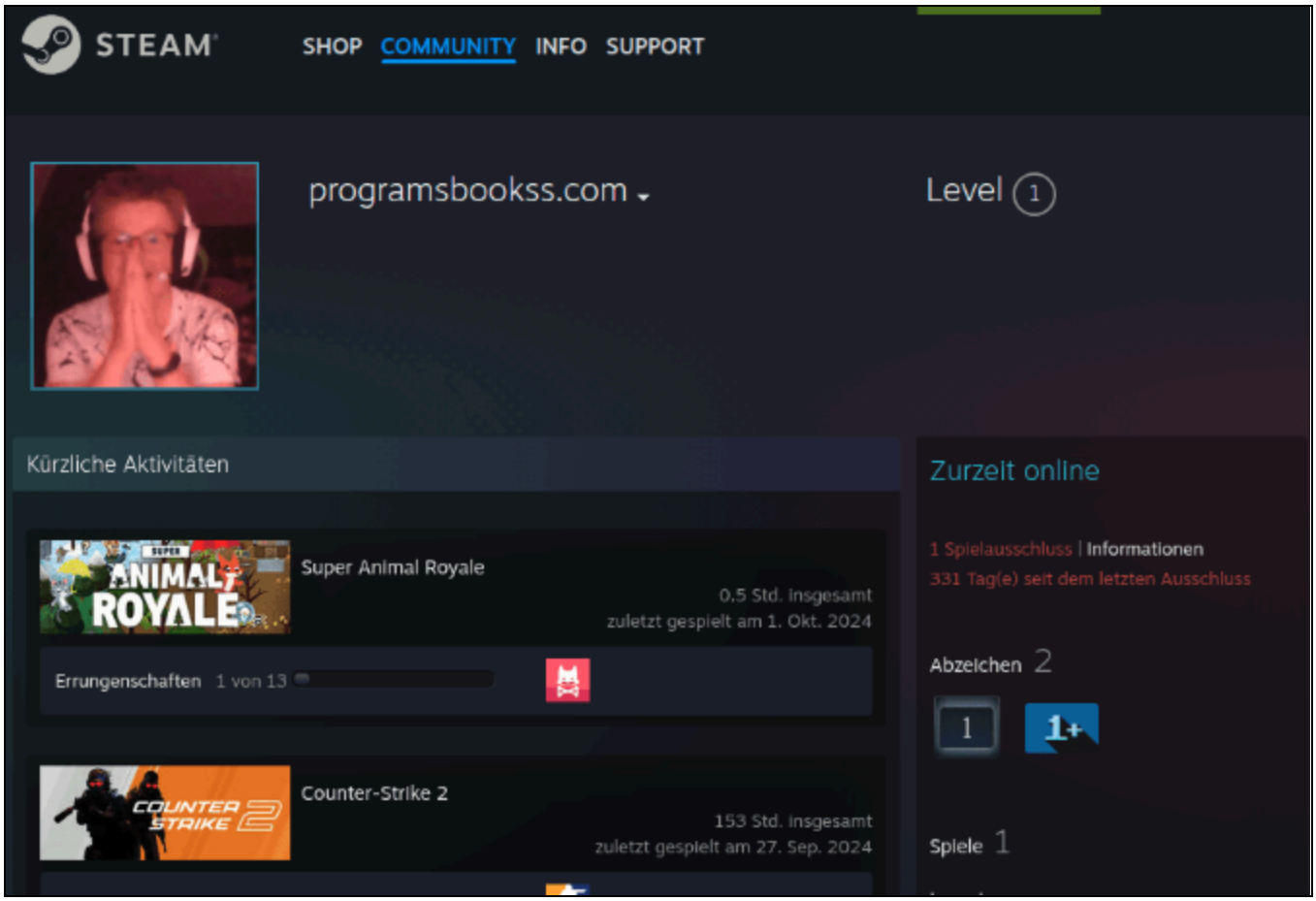


***Figure 4**: TAG-150's CastleRAT using Steam Community for dead drop resolving (Source: Recorded Future)*

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.

```
dynamic.network.http.sequence.request.url contains "/line/?fields=16385"
```

***Figure 6**: Recorded Future Malware Intelligence query to hunt for CastleRAT Python variant (Source: Recorded Future)*

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
- Download and execute executables (EXEs) or dynamic-link libraries (DLLs)
- 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.

```
dynamic.network.http.sequence.request.url contains "/line/?fields=147505"
dynamic.network.http.sequence.request.url contains "/line/?fields=147457"
```

***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
- sPEJlOGDsionsgfdUewg
- KolokolBozhii
- FkgflJGgJgdiJGDGHDjMGjia
- 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.

Appendix A: Indicators of Compromise (IoCs)

CastleLoader C2 IP Addresses:

62[.]60[.]226[.]73
62[.]60[.]226[.]211
62[.]60[.]226[.]254
79[.]132[.]130[.]142
80[.]77[.]23[.]48
85[.]158[.]108[.]135
94[.]159[.]113[.]123
107[.]158[.]128[.]45
107[.]158[.]128[.]90
170[.]130[.]165[.]37
173[.]44[.]141[.]89
173[.]232[.]146[.]90
185[.]212[.]47[.]84
185[.]219[.]220[.]128
213[.]209[.]150[.]229

CastleLoader C2 Domains:

cisco-webexxapp[.]xyz
estetic-online[.]com
higueruela[.]net
lekuvam[.]com
mhousecreative[.]com
notionus[.]org
oneyogasite[.]com
panelv1[.]hostingzealoft[.]today
polarcompany[.]org
rinasalleh[.]com
sftp[.]sagargolf[.]com
vilaoaza[.]com

CastleRAT Python and C C2 IP Addresses:

34[.]72[.]90[.]40
45[.]61[.]136[.]81
91[.]212[.]166[.]17
94[.]141[.]122[.]164
104[.]225[.]129[.]171
144[.]208[.]126[.]50
180[.]178[.]189[.]17
185[.]149[.]146[.]118
185[.]196[.]10[.]8
195[.]85[.]115[.]44
195[.]201[.]108[.]189

CastleRAT C2 Deaddrops:
steamcommunity[.]com/id/tfy5d6gohu8tgy687r7
steamcommunity[.]com/id/krouvhsin34287f7h3
steamcommunity[.]com/id/huilo
steamcommunity[.]com/id/desdsfds34324y3g

SectopRAT C2 IP Addresses:
45[.]141[.]84[.]229
83[.]222[.]191[.]98
92[.]255[.]57[.]32
176[.]126[.]163[.]56
185[.]93[.]89[.]56
194[.]26[.]29[.]44
217[.]12[.]206[.]21

WarmCookie C2 IP Address:
170[.]130[.]165[.]112

Possibly Linked WarmCookie C2 IP Address:
192[.]36[.]57[.]164

Payload Servers:
45[.]32[.]69[.]11
138[.]68[.]250[.]216

CastleLoader Samples (SHA256):
8b7c1657f4d5cf0cc82d68c1f1a385adf0de27d46fc544bba249698e6b427856
18e535d4a641821c4c212b30d79fcebf3fd42d9831972b40dc262b614a08d114
6444f0e3f78254aef663837562d258a2236a77f810ee8d832de7d83e0fdd5783
05ecf871c7382b0c74e5bac267bb5d12446f52368bb1bfe5d2a4200d0f43c1d8
f4bdea09e45471612689bd7d76aa5492fb9de69582d3cf5082d585c16e340d4c
bf21161c808ae74bf08e8d7f83334ba926ffa0bab96ccac42dde418270387890
007f031d4ba5f964136fe73615f524eccdeced5cd7573c281bc1455d5cab2ff6
65493c28b5991bb8e73d1ceb94b3633137542c422ffc5dfd90801909dd475d58
53dddae886017fbfbb43ef236996b9a4d9fb670833dfa0c3eac982815dc8d2a5
f0e1963efa5bfa96ae1a1e370fa2c70a044a03279f2fdbf07391c7e08e295e93
1bb10490d6f13e80d874896428908f6b5758b9722b959841c369c6ddc435230e
4cef6738ef175fa988e9867ca19d2a12f1bf55d2cab07246010833fdb0f4d0f0
88d16948e8cf885d475bc44afa477d2f5b38721e32248425a9e5429c48a4af26
25e0008aba82690e0f58c9d9fcfbc5d49820aa78d2f7bfcd0b85fb969180fc04
e6aab1b6a150ee3cbc721ac2575c57309f307f69cd1b478d494c25cde0baaf85

CastleRAT Python Variant Samples (SHA256):
94dc0f696a46f3c225b0aa741fbd3b8997a92126d66d7bc7c9dd8097af0de52a
401b0eb132cacd6e32d4b4af627370288f9f3e59af36ccfd43a501564937f93c
53775af67e9df206ed3f9c0a3756dbbc4968a77b1df164e9baddb51e61ac82df
58d54e2454be3e4e9a8ea86a3f299a7a60529bc12d28394c5bdf8f858400ff7b

6d62210addb8268d0bd3e6ef0400d54c84e550ccad49f5867fdc51edc0c1db2c
282fa3476294e2b57aa9a8ab4bc1cc00f334197298e4afb2aae812b77e755207
a2feb262a667de704e5e08a8a705c69bbcc806e0d52f0f8e3f081a6aa6c8d7b4
85b4d29f2830a3be3a0f51fbe358bea1a35d2a8aaa6a24f5cc1f2e5d2769716e
4ef63fa536134ad296e83e37f9d323beb45087f7d306debdc3e096fed8357395

CastleRAT C Variant Samples (SHA256):
0fd7eb57f5f9d817dd497c1ce3be0791f5e798077f8dc2c3a4e2b2b0b0bdc2c6
5a741df3e4a61b8632f62109a65afc0f297f4ed03cd7e208ffd2ea5e2badf318
3dd877835c04fde3f2d14ce96f23a1c00002fefa9d731e8c4ce3b656aac90063
7e0d097412ca8c3acdbaaa7c1f79c42cda3a4e50b52c0a8b34d6c75cc764ce42
a67027c3dec4fc4a5a09c68950f494f631ee6aa42b85dd82d74c5b5399d08d19
66aac2857eee73b1f5f715214bb50a03c0dc052d4bb3e64d6b0b492f2c85f374
2fcb76dfdfcd390658bbc032faafef607804d5d4a2f1c0005f274ab2e06d8af4
a97ff41736299857a3cae7c1917456eef5e0fcc703d0a1e475d0b9cfe42452c7
7a682be245a2e51f473ee1c60d537e57423ab2c3d9ae990445cdb6e43aeb5c76
f2e36ccfeb225009ae229a2be905deff587c471b8d47690dc7f5111e1bc611af
ce6a7af556090b3ff762e27058be2327e6c5188d6ed54703d794089f577fd20c
39b40746de01af66c0e5ce5888df4c42e474adcdb4301275b1474423d7a0ff1f
9d356492e433e068c5e71f73638180e3f6a5d992e55ad496a8dafa5174e0a827
13a5c1a535c161fd2724423dad1dfa6885c705713569d4ed4f2ebf900df25ed7
b0b24ff78ab1c4322764bcb332254069504b168cb8aaca469bdf1d37f313d4d3
c2054617b8dcb619749c0402dc31eeb473386b3829f17176bc27b1447a8b6d92
60125159523c356d711ffa1076211359906e6283e25f75f4cf0f9dc8da6bf7b0
1ff6ee23b4cd9ac90ee569067b9e649c76dafac234761706724ae0c1943e4a75
d51f81ee026df39447143b67eaf16326c30e0c9477c0d50507f1fbfffe53abd6
e6bcdf375649a7cbf092fcab65a24d832d8725d833e422e28dfa634498b00928
67cf6d5332078ff021865d5fef6dc61e90b89bc411d8344754247ccd194ff65b
963c012d56c62093d105ab5044517fdcce4ab826f7782b3e377932da1df6896d
f2ff4cbcd6d015af20e4e858b0f216c077ec6d146d3b2e0cbe68b56b3db7a0be

SectopRAT Samples (SHA256):
ae78caabec6a4241c64357ca5ca05de2e181fe253963de528807bf051fc3608e
Af88dc52b37022583a6687214bb5e345b606c6a0a3f37cfe41576d89c3d8e65d

WarmCookie Samples (SHA256):
e62684a48067d8bf5f219f007bb5908301ca3303b9c57a2f0c3212cf0eb8d7b7

Pastebin URLs:
https://pastebin[.]com/raw/2wW91Tby

Appendix B: C2 Servers

CastleLoader C2 Servers

Domain	IP Address	ASN	First Seen	Last Seen
sftp[.]sagargolf[.]com	62[.]60[.]226[.]73	AS214351 - FEMO IT SOLUTIONS LIMITED	2025-06-22	2025-08-20
sftp[.]sagargolf[.]com	62[.]60[.]226[.]211	AS214351 - FEMO IT SOLUTIONS LIMITED	2025-06-22	2025-08-20
N/A	62[.]60[.]226[.]254	AS214351 - FEMO IT SOLUTIONS LIMITED	2025-05-28	2025-06-15
higueruela[.]net	79[.]132[.]130[.]142	AS39378 - servinga GmbH	2025-07-23	2025-08-08
notionus[.]org	80[.]77[.]23[.]48	AS212228 - servinga GmbH	2025-05-09	2025-06-08
panelv1[.]hostingzealoft[.]today	85[.]158[.]108[.]135	AS59711 - HZ Hosting Ltd	2025-06-14	2025-08-26
cisco-webexxapp[.]xyz	94[.]159[.]113[.]123	AS216334 - New Hosting Technologies LLC	2025-04-26	2025-07-07
rinasalleh[.]com	107[.]158[.]128[.]45	AS62904 - Eonix Corporation	2025-06-30	2025-07-29
oneyogasite[.]com	107[.]158[.]128[.]90	AS62904 - Eonix Corporation	2025-07-24	2025-08-20
mhousecreative[.]com	170[.]130[.]165[.]37	AS62904 -	2025-04-29	2025-05-29

Domain	IP Address	ASN	First Seen	Last Seen
		Eonix Corporation		
polarcompany[.]org	173[.]44[.]141[.]89	AS62904 - Eonix Corporation	2025-05-24	2025-06-19
estetic-online[.]com	173[.]232[.]146[.]90	AS62904 - Eonix Corporation	2025-07-24	2025-08-21
lekuvam[.]com	185[.]212[.]47[.]84	AS39378 - servinga GmbH	2025-06-27	2025-07-28
vilaoaza[.]com	185[.]219[.]220[.]128	AS39378 - servinga GmbH	2025-06-26	2025-08-08
sftp[.]sagargolf[.]com	213[.]209[.]150[.]229	AS214943 - Virtualine Technologies	2025-06-24	2025-07-23

(Source: Recorded Future)

CastleRAT C2 Servers

IP Address	Port	ASN	Variant	RC4 Key
104[.]225[.]129[.]171	443	AS395092 - Shock Hosting LLC	C	NanuchkaUpyachka
91[.]212[.]166[.]17	33334	AS198953 - Proton66 LLC	C	N/A
94[.]141[.]122[.]164	33337, 33336	AS215826 - Partner Hosting LTD	C	NanuchkaUpyachka
144[.]208[.]126[.]50	443	AS395092 - Shock Hosting LLC	C	NanuchkaUpyachka
34[.]72[.]90[.]40	443	AS396982 - Google LLC	C	NanuchkaUpyachka
185[.]149[.]146[.]118	33336	AS212701 - Hostinux Limited	C	ALB9SxZBzCqwPFnD
180[.]178[.]189[.]17	443, 33338	AS214351 - FEMO IT SOLUTIONS LIMITED	C	NanuchkaUpyachka GerbertGerbertSS
195[.]85[.]115[.]44	443	AS399629 - BL Networks	C	NanuchkaUpyachka
195[.]201[.]108[.]189	33336	AS24940 - Hetzner Online GmbH	C	NM8KXjTTaxWJRgmL
45[.]61[.]136[.]81	80	AS399629 - BL Networks	Python and C	AeSlekwmgdlSa3sa (Python) KeyKeyKluchCCCCp (C version)
45[.]11[.]180[.]174	80, 6666	AS212228 - servinga GmbH	Python	AeSlekwmgdlSa3sa
102[.]135[.]95[.]102	7777	AS197450 - SUNUCUN	C	RandOmKey322666B
87[.]120[.]93[.]167	7777	AS215730 - H2NEXUS LTD	C	RandOmKey322666B
45[.]144[.]53[.]62	7777	AS215730 - H2NEXUS LTD	C	RandOmKey322666B

IP Address	Port	ASN	Variant	RC4 Key
185[.]125[.]50[.]125	7777	AS215730 - H2NEXUS LTD	C	RandOmKey322666B
77[.]90[.]153[.]43	7777	AS214943 - Virtualine Technologies	C	RandOmKey322666B
185[.]208[.]158[.]250	7777	AS42624 - Global-Data System IT Corporation	C	RandOmKey322666B
79[.]132[.]131[.]200	7777	AS39378 - servinga GmbH	C	RandOmKey322666B
45[.]11[.]180[.]198	7777	AS212228 - servinga GmbH	C	RandOmKey322666B
185[.]196[.]9[.]222	7777	AS42624 - Global-Data System IT Corporation	C	RandOmKey322666B
77[.]238[.]241[.]203	7777	AS216071 - VDSINA	C	NanuchkaUpyachka
5[.]35[.]44[.]176	443	AS216071 - VDSINA	C	NanuchkaUpyachka
85[.]192[.]49[.]6	7777	AS215730 - H2NEXUS LTD	C	RandOmKey322666B
185[.]196[.]9[.]80	7777	AS42624 - Global-Data System IT Corporation	C	KeyKeyKluchCCCCp
185[.]196[.]10[.]8	7777	AS42624 - Global-Data System IT Corporation	C	RandOmKey322666B
85[.]208[.]84[.]115	7777	AS211659 - Oniks LLC	C	RandOmKey322666B
91[.]202[.]233[.]250	80	AS200593 - PROSPERO OOO	Python	BeshBarMakwwwRTY
178[.]17[.]57[.]102	80	AS8661 - Telekomi i Kosoves SH.A.	C	KeyKeyKluchCCCCp

(Source: Recorded Future)

SectopRAT C2 Servers

IP Address	ASN	First Seen	Last Seen
45[.]141[.]84[.]229	AS206728 Media Land LLC	2025-06-16	2025-07-03
83[.]222[.]191[.]98	AS204428 SS-Net	2025-07-01	2025-07-22
92[.]255[.]57[.]32	AS57523 Chang Way Technologies Co. Limited	2025-02-06	2025-05-10
176[.]126[.]163[.]56	AS204957 GREEN FLOID LLC	2025-06-11	2025-06-12
185[.]93[.]89[.]56	AS213790 Limited Network LTD	2025-08-09	2025-08-14
194[.]26[.]29[.]44	AS206728 Media Land LLC	2025-05-13	2025-06-13

(Source: Recorded Future)

WarmCookie C2 Servers

IP Address	ASN	First Seen	Last Seen
170[.]130[.]165[.]112	AS62904 - Eonix Corporation	2025-06-05	2025-07-06

(Source: Recorded Future)

TAG-150 Payload C2 Servers

Domain	IP Address	ASN	First Seen	Last Seen
bytehub[.]asia	Cloudflare	AS13335	2025-06-07	2025-08-19
teamsi[.]org	Cloudflare	AS13335	2025-06-27	2025-08-05
teamsio[.]com	Cloudflare	AS13335	2025-08-08	2025-08-19
teamsoftdigital[.]com	138[.]68[.]250[.]216	AS14061 - Digital Ocean LLC	2025-08-04	2025-08-08
programsbookss[.]com	45[.]32[.]69[.]11	AS20473 - Vultr Holdings, LLC	2025-07-02	2025-08-17

(Source: Recorded Future)

Appendix C: MITRE ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Initial Access: Phishing	T1566
Initial Access: Drive-by Compromise	T1189
Execution: User Execution: Malicious File	T1204.002
Execution: User Execution: Malicious Copy and Paste	T1204.004
Execution: Command and Scripting Interpreter: PowerShell	T1059.001
Execution: Command and Scripting Interpreter: AutoHotKey & AutoIT	T1059.010
Resource Development: Acquire Infrastructure: Domains	T1583.001
Resource Development: Acquire Infrastructure: Virtual Private Server	T1583.003
Resource Development: Acquire Infrastructure: Server	T1583.004
Resource Development: Acquire Access	T1650
Resource Development: Obtain Capabilities: Tool	T1588.002
Resource Development: Compromise Accounts: Email Accounts	T1586.002
Defense Evasion: Masquerading	T1036
Command and Control: Proxy: External Proxy	T1090.002
Command and Control: Application Layer Protocol: Web Protocols	T1071.001
Command and Control: Ingress Tool Transfer	T1105
Collection: Data from Local System	T1005

Appendix D: YARA Rules

CastleLoader

```
rule MAL_CastleLoader {
    meta:
        author = "Insikt Group, Recorded Future"
        date = "2025-08-06"
        description = "Detection of the CastleLoader malware executable"
        version = "1.0"
        reference =
"https://www.ibm.com/think/x-force/dissecting-castlebot-maas-operation"
        hash = "1b6befc65b19a63b4131ce5bcc6e8c0552fe1e1d136ab94bc7d81b3924056156"
        hash = "202f6b6631ade2c41e4762e5877ce0063a3beabce0c3f8564b6499a1164c1e04"
        hash = "25e0008aba82690e0f58c9d9fcfbc5d49820aa78d2f7bfcd0b85fb969180fc04"
        hash = "b45cce4ede6ffb7b6f28f75a0cbb60e65592840d98dcb63155b9fa0324a88be2"
        hash = "fb9de7448e9e30f717c171f1d1c90ac72828803a16ad385757aeecc853479d3c"
        hash = "6444f0e3f78254aef663837562d258a2236a77f810ee8d832de7d83e0fdd5783"
        malware = "CastleLoader"
        malware_id = "8RF9P9"
        category = "MALWARE"
    strings:
        $vmware_check = { 3D 56 4D 77 61 75 ?? 81 7D F8 72 65 56 4D 0F 85 ?? ?? ?? ?? 81
7D F4 77 61 72 65 }
        $api_hashing = { 0F BE 0C 1E 8B C2 F6 C3 01 75 0F C1 E8 03 0F AF C1 8B CA C1 E1 07
33 C1 }
        $stack_str_url = { C7 ?5 [1-4] 74 00 74 00 C7 ?5 [1-4] 69 00 6E 00 C7 ?5 [1-4] 67
00 73 00 }
        $mov_edx_apihash1 = { BA 44 A0 2D 39 } // CreateMutexW
        $mov_edx_apihash2 = { BA 2B C2 86 58 } // GetLastError
        $mov_edx_apihash3 = { BA 94 F9 86 F8 } // RtlAllocateHeap
        $mov_edx_apihash4 = { BA B2 48 70 60 } // ExitProcess
    condition:
        uint16(0) == 0x5A4D and all of them
}
```

CastleRAT Python Variant

```
rule MAL_CastleRAT_Python {
    meta:
        author = "Insikt Group, Recorded Future"
        date = "2025-08-18"
        description = "Detection of the python variant of CastleRAT malware"
        version = "1.0"
        reference =
"https://www.ibm.com/think/x-force/dissecting-castlebot-maas-operation"
        reference =
"https://catalyst.prodaft.com/public/report/understanding-current-castleloader-campaigns/o
verview"
```

```
        hash = "94dc0f696a46f3c225b0aa741fbd3b8997a92126d66d7bc7c9dd8097af0de52a"
        hash = "53775af67e9df206ed3f9c0a3756dbbc4968a77b1df164e9baddb51e61ac82df"
        malware = "CastleRAT"
        malware_id = "9WCga-"
        category = "MALWARE"
    strings:
        $cmd1 = "S_CONNECT" fullword
        $cmd2 = "S_COMMAND" fullword
        $cmd3 = "S_PING" fullword
        $cmd4 = "S_CMD" fullword
        $cmd5 = "S_DELETE" fullword
        $cmd6 = "S_POWERSHELL" fullword
        $cmd7 = "S_START_TERMINAL" fullword
        $cmd8 = "S_SESSION_MESSAGE" fullword
        $cmd9 = "S_UPLOAD" fullword
        $fun1 = "CheckElevation():" fullword
        $fun2 = "GetHWID("
        $fun3 = "GetOS("
        $fun4 = "GetIpGeo("
        $fun5 = "rc4createkeyA("
        $fun6 = "EncryptDecryptBufA("
        $fun7 = "RecvTimeout("
        $fun8 = "Send("
        $fun9 = "Connect("
        $fun10 = "ThreadPing("
        $fun11 = "ThreadRecvTerminal("
        $fun12 = "ThreadTerminalSession("
        $fun13 = "ThreadUploadFile("
        $fun14 = "SelfDelete()" fullword
    condition:
        filesize < 50KB and
        7 of ($cmd*) and
        10 of ($fun*)
}
```

CastleRAT C Variant

```
rule MAL_CastleRAT_C {
    meta:
        author = "Insikt Group, Recorded Future"
        date = "2025-08-18"
        description = "Detection of the C variant of CastleRAT malware"
        version = "1.0"
        reference =
"https://www.ibm.com/think/x-force/dissecting-castlebot-maas-operation"
        reference =
"https://catalyst.prodaft.com/public/report/understanding-current-castleloader-campaigns/o
verview"
        hash = "1ff6ee23b4cd9ac90ee569067b9e649c76dafac234761706724ae0c1943e4a75"
        hash = "e6bcdf375649a7cbf092fcab65a24d832d8725d833e422e28dfa634498b00928"
```

```
        hash = "67cf6d5332078ff021865d5fef6dc61e90b89bc411d8344754247ccd194ff65b"
        hash = "963c012d56c62093d105ab5044517fdcce4ab826f7782b3e377932da1df6896d"
        hash = "60125159523c356d711ffa1076211359906e6283e25f75f4cf0f9dc8da6bf7b0"
        malware = "CastleRAT"
        malware_id = "9WCga-"
        category = "MALWARE"
    strings:
        $log_tag1 = "clipboardlog.txt" fullword wide
        $log_tag2 = "keylog.txt" fullword wide
        $wnd_class1 = "IsabellaWine" fullword wide
        $wnd_class2 = "camera!" fullword wide
        $log_fmt1 = "[%02d:%02d %02d.%02d.%02d] %ws" fullword wide
        $log_fmt2 = "[%02d:%02d %02d.%02d.%02d] " fullword wide
        $log_fmt3 = "[%02d.%02d.%02d %02d:%02d] " fullword wide
        $s1 = "(VPN)" wide ascii
        $s2 = "rundll32 \"C:\\Windows\\System32\\shell32.dll\" #61"  wide
        $s3 = "\"%ws\" -no-deelevate" fullword wide
        $s4 = "IsWindowVisible" fullword ascii
        $s5  = "UAC_InputIndicatorOverlayWnd" fullword wide
        $s6 = "www.ip-api.com" fullword wide
        $s7 = "MachineGuid" fullword wide
        $s8 = "line/?fields=" wide
        $s9 = "C:\\Windows\\System32\\cmd.exe" fullword wide
        $s10  = "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe" fullword
wide

     condition:
       uint16(0) == 0x5a4d and
       any of ($log_tag*) and
       any of ($wnd_class*) and
       any of ($log_fmt*) and
       all of ($s*)
}
```

Appendix E: Sigma Rule

```
title: CastleRAT Python Malware Self Deletion
id: 1050a0c4-1110-4b55-938c-0d27259ddd1e
status: stable
description: Detects the execution of powershell by the Python variant of CastleRAT
malware to delete itself.
references:
  - https://tria.ge/250822-r3a6qaak2t
author: Insikt Group, Recorded Future
date: 2025-08-28
tags:
  - attack.t1070.004   # Indicator Removal: File Deletion
logsource:
    product: windows
```

```
    category: process_creation
detection:
    self_delete:
        CommandLine|endswith: 'powershell Start-Sleep -Seconds 4; Remove-Item -Path '*'
-Force; exit'
    condition: self_delete
level: high
falsepositives:
  - Potential benign installer activity
```

```
title: CastleRAT C Variant Malware Log File Creation
id: 4d785ac8-17fe-4765-b427-9a31073ad1a7
status: stable
description: Detects CastleRAT C variant malware log file creation events. The log file is
used to store output from the keylogger and clipboard stealer.
references:
  - https://tria.ge/250701-v6911aykv9
author: Insikt Group, Recorded Future
date: 2025-08-29
level: high
tags:
  - attack.t1608 # Stage Capabilities
  - attack.t1074.001 # Data Staged - Local Data Staging
  - attack.t1115 # Clipboard Data
  - attack.t1056.001 # Keylogging
logsource:
  product: windows
  category: file_event
detection:
  castlerat_logs:
    TargetFilename|endswith:
      - '\AppData\Local\Temp\MuuuuuhGer3'
      - '\AppData\Local\Temp\PluhhSuk3'
      - '\AppData\Local\Temp\AsdDsaHaha3'
      - '\AppData\Local\Temp\ChuChuka'
      - '\AppData\Local\Temp\GagikMaraguiSS'
      - '\AppData\Local\Temp\LowUshrSudujes'
      - '\AppData\Local\Temp\RarnuiKarta'
      - '\AppData\Local\Temp\GrazGraznii'
      - '\AppData\Local\Temp\GiveGvein3'
      - '\AppData\Local\Temp\BeruiowdgsouiHTR'
      - '\AppData\Local\Temp\GDSongdsgndohSDU'
  condition: castlerat_logs
falsepositives:
  - Unlikely
```

Appendix F: Snort Rules

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"CastleLoader Malware Outbound
Checkin"; flow:established,to_server; content:"GET"; http_method; urilen:82,norm;
content:"|2F|service|2F|settings|2F|"; http_uri; fast_pattern; content:"Cache-Control|3A
20|no-cache|0D 0A|Connection|3A 20|Keep-Alive|0D 0A|Pragma|3A 20|no-cache|0D
0A|User-Agent|3A 20|"; http_header; depth:79; content:"Host|3A 20|"; http_header;
distance:0; content:!"Accept"; http_header;
pcre:"/User\x2dAgent[^\x0d]+\x0d\x0aHost\x3a\x20[^\x0d]+\x0d\x0a\x0d\x0a/";
reference:url,https://catalyst.prodaft.com/public/report/understanding-current-castleloade
r-campaigns/overview; classtype:trojan-activity; sid:52460302; rev:1; metadata:author
MGUT, created_at 2025-07-24, mitre_tactic_id TA0011, mitre_tactic_name
Command-And-Control;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"CastleLoader Malware Outbound
Payload Request"; flow:established,to_server; content:"GET"; http_method;
content:"|2F|service|2F|download|2F|"; http_uri; fast_pattern; content:"Cache-Control|3A
20|no-cache|0D 0A|Connection|3A 20|Keep-Alive|0D 0A|Pragma|3A 20|no-cache|0D
0A|User-Agent|3A 20|"; http_header; depth:79; content:"Host|3A 20|"; http_header;
distance:0; content:!"Accept"; http_header;
pcre:"/User\x2dAgent[^\x0d]+\x0d\x0aHost\x3a\x20[^\x0d]+\x0d\x0a\x0d\x0a/";
reference:url,https://catalyst.prodaft.com/public/report/understanding-current-castleloade
r-campaigns/overview; classtype:trojan-activity; sid:52460303; rev:1; metadata:author
MGUT, created_at 2025-07-24, mitre_tactic_id TA0011, mitre_tactic_name
Command-And-Control;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"CastleLoader Malware Stager
Outbound Payload Request"; flow:established,to_server; content:"GET"; http_method;
content:"|2F|service|2F|download|2F|"; http_uri; depth:18; fast_pattern; content:".bin";
http_uri; content:"User-Agent|3A 20|GoogeBot|0D 0A|"; http_header;
reference:url,https://catalyst.prodaft.com/public/report/understanding-current-castleloade
r-campaigns/overview; classtype:trojan-activity; sid:52460304; rev:1; metadata:author
MGUT, created_at 2025-08-12, mitre_tactic_id TA0011, mitre_tactic_name
Command-And-Control;)
```

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Possible CastleRAT Python Malware
Outbound Request To IP Geo Location Service ip-api"; flow:established,to_server;
content:"GET"; http_method; urilen:19,norm; content:"|2F|line|2F 3F|fields|3D|16385";
http_uri; depth:19; fast_pattern; content:"Connection|3A 20|Keep-Alive|0D 0A|Host|3A
20|www.ip-api.com|0D 0A 0D 0A|"; http_raw_header; depth:48;
reference:url,https://tria.ge/250808-w4hpeaxtcw; classtype:trojan-activity; sid:52460315;
rev:1; metadata:author MGUT, created_at 2025-08-24, mitre_tactic_id TA0011,
mitre_tactic_name Command-And-Control;)
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"Possible CastleRAT C Variant
Malware Outbound Request To IP Geo Location Service ip-api"; flow:established,to_server;
content:"GET"; http_method; urilen:20,norm; content:"|2F|line|2F 3F|fields|3D|147457";
http_uri; depth:20; fast_pattern; content:"Connection|3A 20|Keep-Alive|0D 0A|Host|3A
```

```
20|www.ip-api.com|0D 0A 0D 0A|"; http_header; depth:48;
reference:url,https://tria.ge/250822-vwt7ssxly9; classtype:trojan-activity; sid:52460316;
rev:1; metadata:author MGUT, created_at 2025-08-24, mitre_tactic_id TA0011,
mitre_tactic_name Command-And-Control;)
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"Possible CastleRAT C Variant
Malware Outbound Request To IP Geo Location Service ip-api"; flow:established,to_server;
content:"GET"; http_method; urilen:20,norm; content:"|2F|line|2F 3F|fields|3D|147505";
http_uri; depth:20; fast_pattern; content:"Connection|3A 20|Keep-Alive|0D 0A|Host|3A
20|www.ip-api.com|0D 0A 0D 0A|"; http_header; depth:48;
reference:url,https://tria.ge/250814-wyqstsyjx3; classtype:trojan-activity; sid:52460317;
rev:1; metadata:author MGUT, created_at 2025-08-24, mitre_tactic_id TA0011,
mitre_tactic_name Command-And-Control;)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"CastleRAT Malware Outbound Handshake";
flow:established,to_server; dsize:20; stream_size:server,=,1; content:"|02 56 77 8E A5 83
D7 05 02 C2 1E D9 70 5A 47 E5 11 92 B5 5A|"; fast_pattern; depth:20;
reference:url,https://tria.ge/250808-w4hpeaxtcw; classtype:trojan-activity; sid:52460307;
rev:1; metadata:author MGUT, created_at 2025-08-18, mitre_tactic_id TA0011,
mitre_tactic_name Command-And-Control;)
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"CastleRAT Malware Outbound Handshake";
flow:established,to_server; dsize:20; stream_size:server,=,1; content:"|BF CF 04 82 45 DF
4F 09 55 5E 0B 15 9F E2 91 A0 68 51 1E 87|"; fast_pattern; depth:20;
reference:url,https://tria.ge/250814-wyqstsyjx3; classtype:trojan-activity; sid:52460308;
rev:1; metadata:author MGUT, created_at 2025-08-18, mitre_tactic_id TA0011,
mitre_tactic_name Command-And-Control;)
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"CastleRAT Malware Outbound Handshake";
flow:established,to_server; dsize:20; stream_size:server,=,1; content:"|6B 13 5C 08 BD 49
59 75 79 62 4E EA 2F DE 57 F4 6E 08 8B 6B|"; fast_pattern; depth:20;
reference:url,https://tria.ge/250219-nsbsqazpep; classtype:trojan-activity; sid:52460309;
rev:1; metadata:author MGUT, created_at 2025-08-18, mitre_tactic_id TA0011,
mitre_tactic_name Command-And-Control;)
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"CastleRAT Malware Outbound Handshake";
flow:established,to_server; dsize:20; stream_size:server,=,1; content:"|56 EA 59 DB 6B DD
36 81 42 01 C6 84 DF 5A 6B E8 38 14 8D 07|"; fast_pattern; depth:20;
reference:url,https://tria.ge/250505-wmbvjabk3t; classtype:trojan-activity; sid:52460310;
rev:1; metadata:author MGUT, created_at 2025-08-18, mitre_tactic_id TA0011,
mitre_tactic_name Command-And-Control;)
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"CastleRAT Malware Outbound Handshake";
flow:established,to_server; dsize:20; stream_size:server,=,1; content:"|A8 CF 1E 1D BA 27
49 FB 63 38 F4 52 A7 9C 39 CF 4A 85 E5 5B|"; fast_pattern; depth:20;
reference:url,https://tria.ge/250822-vwt7ssxly9; classtype:trojan-activity; sid:52460311;
rev:1; metadata:author MGUT, created_at 2025-08-22, mitre_tactic_id TA0011,
mitre_tactic_name Command-And-Control;)
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"CastleRAT Malware Outbound Handshake";
flow:established,to_server; dsize:20; stream_size:server,=,1; content:"|0F 0D F7 66 4C B2
```

```
D5 12 BA 55 CC BB 2E 1B F4 AD C0 E0 7C A2|"; fast_pattern; depth:20;
reference:url,https://tria.ge/250822-rt355svtfs; classtype:trojan-activity; sid:52460312;
rev:1; metadata:author MGUT, created_at 2025-08-22, mitre_tactic_id TA0011,
mitre_tactic_name Command-And-Control;)
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"CastleRAT Malware Outbound Handshake";
flow:established,to_server; dsize:20; stream_size:server,=,1; content:"|74 6F D9 7F B5 48
F6 91 26 E0 16 5A 81 29 4F 35 21 6C 61 82|"; fast_pattern; depth:20;
reference:url,https://tria.ge/250813-a7c3fadl7z; classtype:trojan-activity; sid:52460313;
rev:1; metadata:author MGUT, created_at 2025-08-22, mitre_tactic_id TA0011,
mitre_tactic_name Command-And-Control;)
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"CastleRAT Malware Outbound Handshake";
flow:established,to_server; dsize:20; stream_size:server,=,1; content:"|61 57 7C E8 EE BE
56 71 B3 98 F4 A6 87 E3 0C 39 50 0C 29 41|"; fast_pattern; depth:20;
reference:url,https://tria.ge/250822-vwt7ssxly9; classtype:trojan-activity; sid:52460314;
rev:1; metadata:author MGUT, created_at 2025-08-22, mitre_tactic_id TA0011,
mitre_tactic_name Command-And-Control;)
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"Possible CastleRAT Python Malware
Outbound Request To IP Geo Location Service ip-api"; flow:established,to_server;
content:"GET"; http_method; urilen:19,norm; content:"|2F|line|2F 3F|fields|3D|16385";
http_uri; depth:19; fast_pattern; content:"Connection|3A 20|Keep-Alive|0D 0A|Host|3A
20|www.ip-api.com|0D 0A 0D 0A|"; http_raw_header; depth:48;
reference:url,https://tria.ge/250808-w4hpeaxtcw; classtype:trojan-activity; sid:52460315;
rev:1; metadata:author MGUT, created_at 2025-08-24, mitre_tactic_id TA0011,
mitre_tactic_name Command-And-Control;)
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"Possible CastleRAT C Variant
Malware Outbound Request To IP Geo Location Service ip-api"; flow:established,to_server;
content:"GET"; http_method; urilen:20,norm; content:"|2F|line|2F 3F|fields|3D|147457";
http_uri; depth:20; fast_pattern; content:"Connection|3A 20|Keep-Alive|0D 0A|Host|3A
20|www.ip-api.com|0D 0A 0D 0A|"; http_header; depth:48;
reference:url,https://tria.ge/250822-vwt7ssxly9; classtype:trojan-activity; sid:52460316;
rev:1; metadata:author MGUT, created_at 2025-08-24, mitre_tactic_id TA0011,
mitre_tactic_name Command-And-Control;)
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"Possible CastleRAT C Variant
Malware Outbound Request To IP Geo Location Service ip-api"; flow:established,to_server;
content:"GET"; http_method; urilen:20,norm; content:"|2F|line|2F 3F|fields|3D|147505";
http_uri; depth:20; fast_pattern; content:"Connection|3A 20|Keep-Alive|0D 0A|Host|3A
20|www.ip-api.com|0D 0A 0D 0A|"; http_header; depth:48;
reference:url,https://tria.ge/250814-wyqstsyjx3; classtype:trojan-activity; sid:52460317;
rev:1; metadata:author MGUT, created_at 2025-08-24, mitre_tactic_id TA0011,
mitre_tactic_name Command-And-Control;)
```

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

Learn more at recordedfuture.com