BlindEagle flying high in Latin America

GReAT ⋮⋮ 8/19/2024

Authors

- Expert GReAT

BlindEagle, also known as “APT-C-36”, is an APT actor recognized for employing straightforward yet impactful attack techniques and methodologies. The group is known for their persistent campaigns targeting entities and individuals in Colombia, Ecuador, Chile, Panama and other countries in Latin America. They have been targeting entities in multiple sectors, including governmental institutions, financial companies, energy and oil and gas companies, among others.

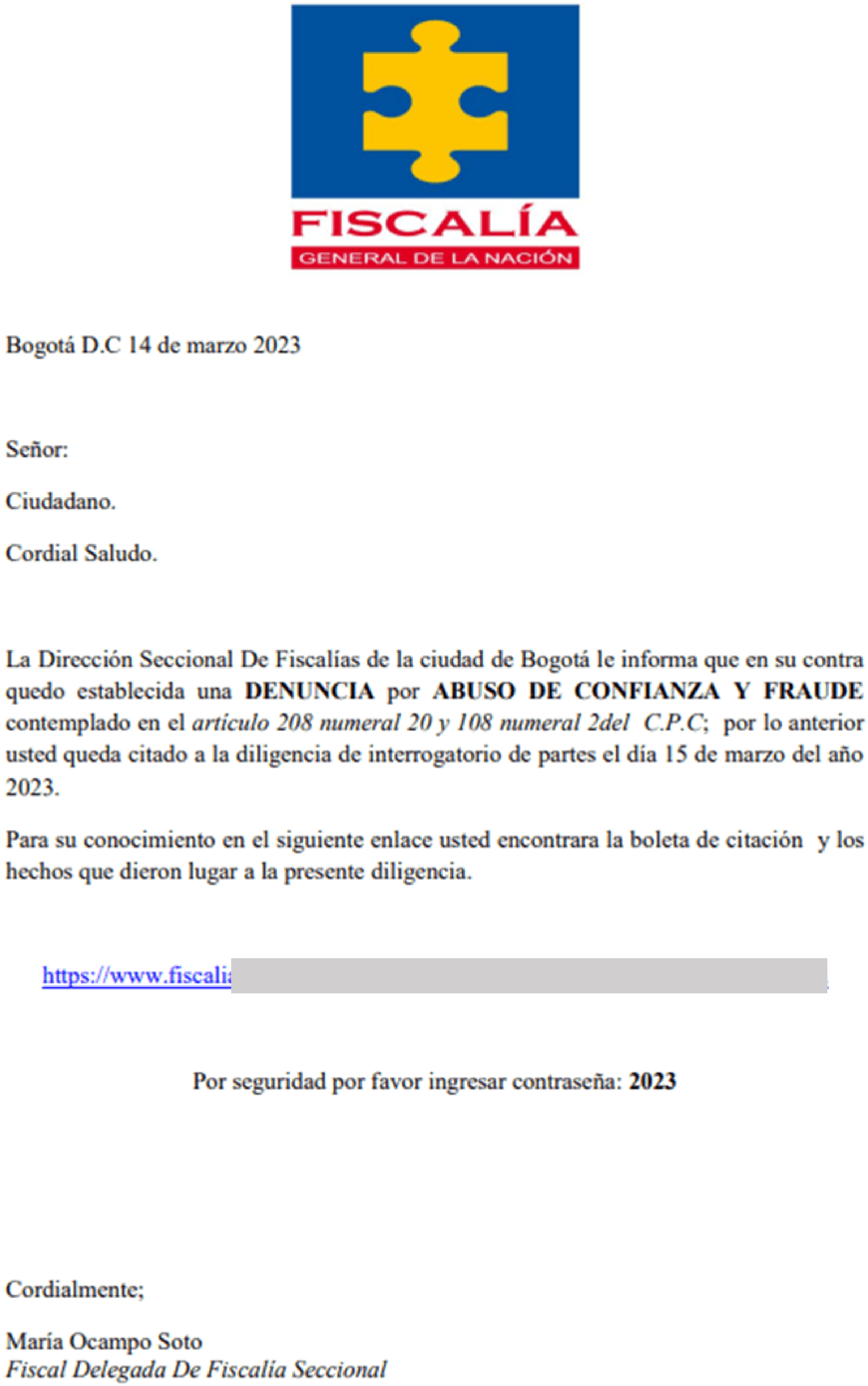
BlindEagle has demonstrated adaptability in shaping the objectives of its cyberattacks and the versatility to switch between purely financially motivated attacks and espionage operations.

There is evidence that the group has been active since at least 2018. At GReAT, we have been closely tracking their campaigns. This blog aims to give an introduction to the group, detail its TTPs, and provide insights into their recent operations.

The eagle goes phishing

The spreading method used by BlindEagle is via phishing emails. Depending on the type of cyberoperation they conduct, it could be spear phishing (used in targeted espionage attacks) or more generalized phishing (particularly used in financial attacks).

The phishing emails typically impersonate governmental institutions, such as Colombia’s National Directorate of Taxes and Customs, Ministry of Foreign Affairs or Office of the Attorney General, among others. Spam campaigns impersonating financial and banking entities are also common.



FISCALÍA
GENERAL DE LA NACIÓN

Bogotá D.C 14 de marzo 2023

Señor:

Ciudadano.

Cordial Saludo.

La Dirección Seccional De Fiscalías de la ciudad de Bogotá le informa que en su contra quedo establecida una **DENUNCIA** por **ABUSO DE CONFIANZA Y FRAUDE** contemplado en el *artículo 208 numeral 20 y 108 numeral 2del C.P.C*; por lo anterior usted queda citado a la diligencia de interrogatorio de partes el día 15 de marzo del año 2023.

Para su conocimiento en el siguiente enlace usted encontrara la boleta de citación y los hechos que dieron lugar a la presente diligencia.

https://www.fiscali[redacted]

Por seguridad por favor ingresar contraseña: **2023**

Cordialmente;

María Ocampo Soto
Fiscal Delegada De Fiscalía Seccional

Phishing impersonating the Attorney General's Office

The campaigns involve sending deceptive emails containing a notification about an issue that requires immediate action by the user. Each email contains a link in its body that appears to lead to the official website of the entity being impersonated, and an attached file (particularly PDF or Word documents). The attached document mirrors the email's message, contains the same URL and, in some cases, adds extra details and a heightened sense of urgency to make the phishing attempt sound more convincing. The links usually point to DDNS services and redirect victims to public repositories or sites owned by the attackers where they host malware implants, also known as "the initial dropper".

A distinctive aspect of the malware delivery is geolocation filtering. The group often uses URL shorteners that are capable of geographical detection and redirection. That means that, if a connection is detected to be coming from a country which is not among the group's targets, the attack is called off, and the victim is redirected to the site of the organization the attackers are impersonating. This geographical redirection prevents new malicious sites from being flagged, and thwarts hunting and analysis of these attacks.

How the eagles attack

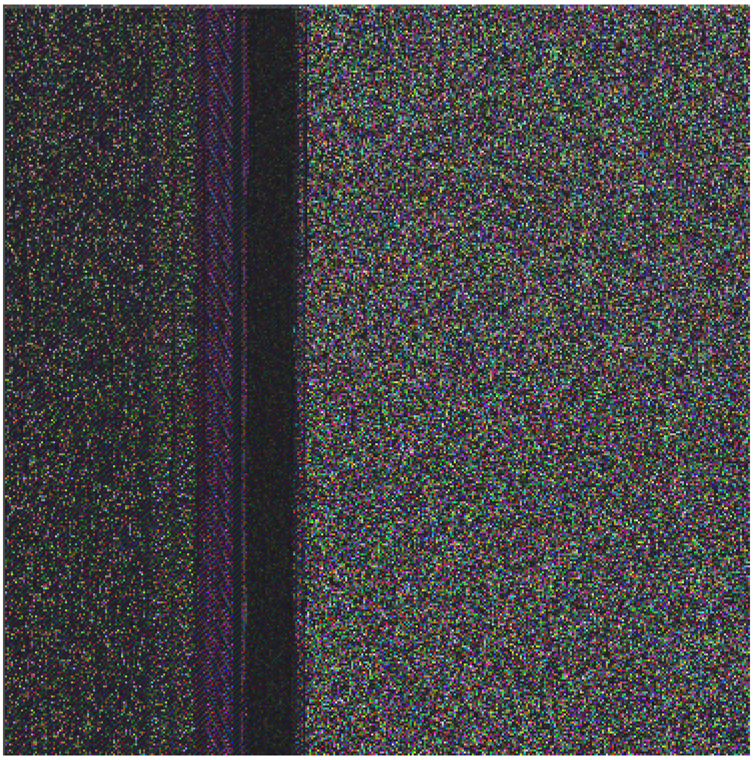
Once an email is delivered, it paves the way for the group's final malicious implant. BlindEagle is well known for using publicly available or open-source Remote Access Trojans (RATs), with the primary goal of spying on victims and stealing financial information. The group constantly switches from one RAT to another, using different tools in different campaigns. We have observed BlindEagle running operations using njRAT, LimeRAT, BitRAT and AsyncRAT, among others. They usually modify the samples to add customization them and new capabilities.

To deploy the final implant, the group uses a multi-stage process that is consistently similar across their campaigns. Unlike the final payload, the tools they use at the intermediate stages are custom built. The initial dropper, downloaded from malicious links, is typically a compressed file that tricks the victim by pretending to be an official document from the government or financial entity being spoofed in the phishing attack. We have observed the use of popular compression formats like ZIP, but also older and less known formats, such as LHA and UUE. Many threat actors exploit these lesser-known formats to deceive their victims into opening the file, taking advantage of their lack of knowledge about these formats.

The victim is persuaded to extract and run the files within the archive allegedly to solve the issue mentioned in the phishing email. The extracted files are typically Visual Basic Scripts that use WScript, XMLHTTP objects, or PowerShell commands to contact another server to download a malicious artifact for the next stage. The server address is usually hardcoded in the VBS file.

During the monitored campaigns, we have observed various server options chosen by BlindEagle, including servers controlled by the group and public infrastructure, such as image hosting sites, text storage sites like Pastebin, CDN services like Discord or developer platforms like GitHub repositories.

As the second-stage artifact, the threat actor employs various files, with the most common types being text files, images and .NET executables. These are usually encoded or obfuscated.



Steganography used in a BlindEagle campaign

The text files often contain a payload encoded in base64, ASCII or a combination of both. For images, the group has explored using steganography techniques to hide similarly encoded malicious code. The executable files typically masquerade as legitimate and contain the next malicious payload within their resource section.

In the next phase, the malicious code is extracted if needed and decoded by the initial dropper, yielding an intermediate file that, judging by the campaigns we have monitored, can be either a DLL or a .NET injector. This file calls yet another malicious server, whose address is, too, hardcoded in the executable, to download the final payload: the open-source RAT.

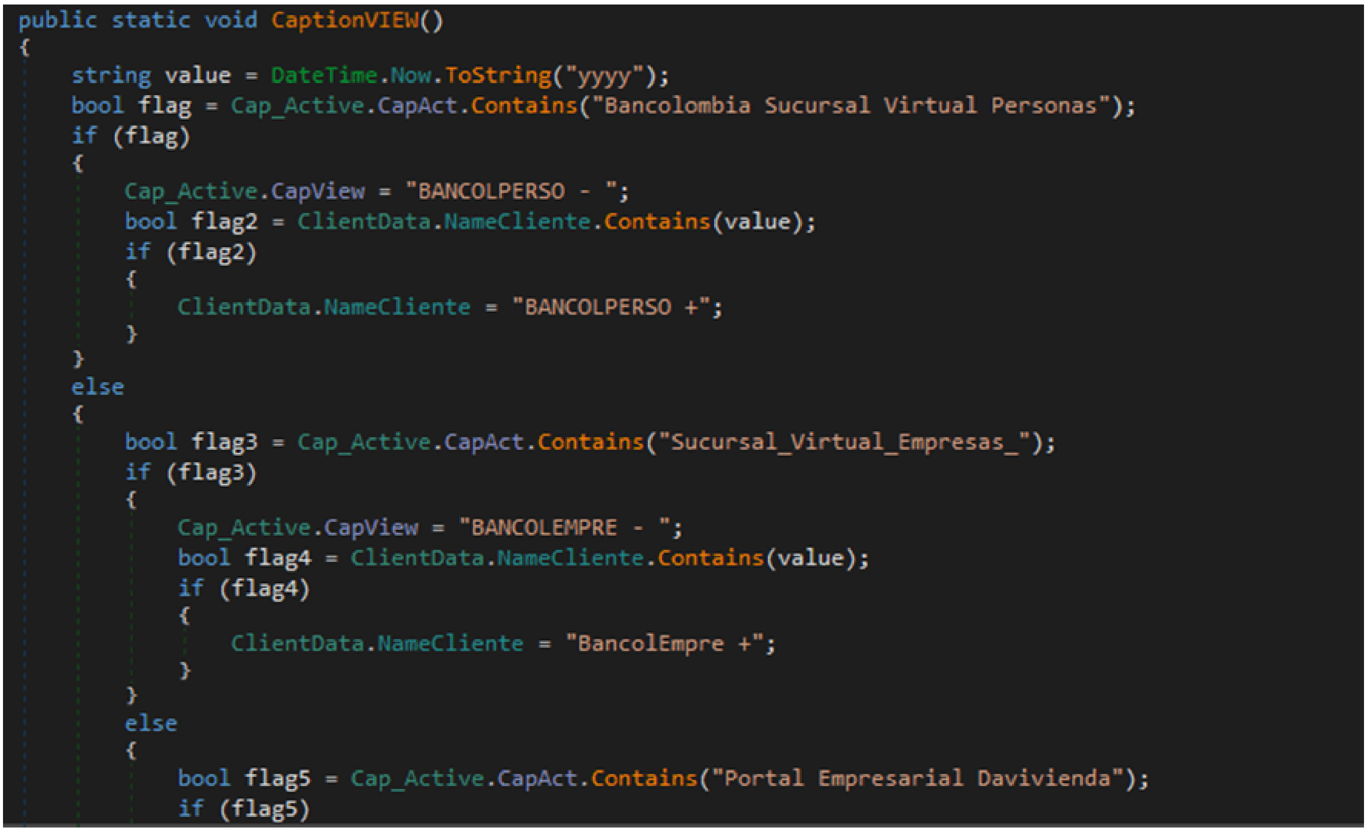
During this intermediate phase, the group often uses process injection techniques to execute the RAT in the memory of a legitimate process, thereby evading process-based defenses. The group's preferred technique is process hollowing. This technique consists in creating a legitimate process in a suspended state, then unmapping its memory, replacing it with a malicious payload, and finally resuming the process to start execution.

Cyber-espionage or a financial attack: Actually, both

BlindEagle uses open-source RATs as the final link in their attack chain, which they modify in a way that suits their campaign objectives. This approach gives them the flexibility to adapt their malware with minimal efforts, as they do not need to develop implants from scratch. We have observed a wide variety of RATs used by the group, with notable examples including AsyncRAT, njRAT, Lime-RAT, Quasar RAT and BitRAT.

The group demonstrates great adaptability between campaigns. For example, in some of its financial attacks, the threat actor utilized a modified version of the Quasar RAT, a malware primarily used for espionage but in this case, repurposed as a banking Trojan to specifically target customers of financial institutions in Colombia.

The group modified the RAT by adding functionality to capture information from the victim’s browser to intercept credentials for banking services. After execution, the malware monitored newly opened browser windows. If the titles of any of these windows returned a match with a list of strings relating to ten Colombian financial entities, the RAT initiated keylogging to capture the login credentials for these entities’ online services.



```
public static void CaptionVIEW()
{
    string value = DateTime.Now.ToString("yyyy");
    bool flag = Cap_Active.CapAct.Contains("Bancolombia Sucursal Virtual Personas");
    if (flag)
    {
        Cap_Active.CapView = "BANCOLPERSO - ";
        bool flag2 = ClientData.NameCliente.Contains(value);
        if (flag2)
        {
            ClientData.NameCliente = "BANCOLPERSO +";
        }
    }
    else
    {
        bool flag3 = Cap_Active.CapAct.Contains("Sucursal_Virtual_Empresas_");
        if (flag3)
        {
            Cap_Active.CapView = "BANCOLEMPRE - ";
            bool flag4 = ClientData.NameCliente.Contains(value);
            if (flag4)
            {
                ClientData.NameCliente = "BancolEmpre +";
            }
        }
        else
        {
            bool flag5 = Cap_Active.CapAct.Contains("Portal Empresarial Davivienda");
            if (flag5)
```

A version of Quasar RAT modified to steal financial credentials

When it comes to espionage campaigns, the group turns to Trojans like njRAT. Modified versions of this malware allow them to capture sensitive information from their victims through keylogging and application monitoring. Additionally, the RAT exfiltrates system information and screenshots to C2 servers and can create RDP sessions or even install additional plugins. In one of the recent campaigns we have detected, the group modified this RAT to add the capability to install plugins sent from the C2 in the form of .NET assemblies or other binary files.

Improving flight precision

The group has always been known for using simple yet highly effective tactics and techniques: straightforward phishing, basic encoding and obfuscation methods, and the use of publicly available malware. However, during the latest campaigns, we have observed changes in the group’s techniques, reinforcing the idea of “adapt or perish”.

In May this year, for instance, the group conducted a new espionage campaign targeting Colombia. During this operation, BlindEagle employed an infection process featuring artifacts with strings and variable names entirely in Portuguese (instead of Spanish they had predominantly used before) and utilized Brazilian image hosting sites. Although not definitive, these elements could hint at the involvement of third parties with the group, either through collaboration or outsourcing to increase their attack capacity.

More recently, in June, we observed an espionage campaign that also targeted Colombia in which the group introduced a new technique into their arsenal. The campaign followed all the group's usual TTPs, but this time, added a DLL sideloading twist and a new modular malware loader dubbed "HijackLoader".

The attack was initiated through phishing emails impersonating Colombia's judicial institutions and containing malicious PDF or DOCX files masquerading as a demand notice or a court summons. The victims were tricked into opening the attached files and clicking embedded links to download fictitious lawsuit documents, allegedly to resolve the previously mentioned legal issues. These documents were actual legitimate executable files signed by ASUS or IObit. They invoked malicious DLLs through sideloading, ultimately executing a version of HijackLoader that injected the spy RAT: in this case, AsyncRAT.

Victims

Since its inception, BlindEagle has been conducting persistent campaigns targeting entities and individuals, particularly in Colombia and other Latin American, countries such as Ecuador, Chile and Panama.

In the espionage campaigns we observed in May and June this year, the group primarily targeted individuals and organizations in Colombia, which accounted for 87% of the detected victims. These attacks involved entities across various sectors, notably government, education, health and transportation.

Tactics, techniques and procedures (TTPs)

Although the group's toolset varies greatly, as do their goals, they employ a range of tactics, techniques, and procedures that are consistently used across their various campaigns. Below are some key TTPs that frequently recur:

- Phishing impersonating governmental entities as the spreading method. In some campaigns, particularly those involving financial attacks, the group impersonates banking institutions.
- Attached PDFs and DOCX files containing embedded links.
- URL shortener services employed for geolocation filtering.
- Dynamic DNS services utilized for resolving the addresses of servers hosting the group's malicious artifacts.
- Public infrastructure used to host some of the malicious artifacts (image hosting services, pastebin sites, GitHub repositories and the Discord CDN, among others).
- Process hollowing applied for injecting malicious code into legitimate processes during intermediate stages of the attack.
- VBS scripts and .NET assemblies employed as intermediate artifacts.
- Open-source RATs used as the final payload in the attack.

Conclusions

As simple as BlindEagle's techniques and procedures may appear, their effectiveness allows the group to sustain a high level of activity. By consistently executing cyber-espionage and financial credential theft campaigns, BlindEagle remains a significant threat in the region.

Additionally, the group is exploring alternative strategies within their infection processes and adding new techniques to their arsenal to sustain their operations and maintain their impact. BlindEagle continues to fly high, and we will maintain vigilant monitoring of their activity.

IoCs

18eb0a413b80a548d2b615e11fc580cd
53231da42b6f19d2a6b59700f822be6a
69d218a3cd86a194d8fbc22c487096bc
7b72f2775b7bf33c9778533480d34e04