2025

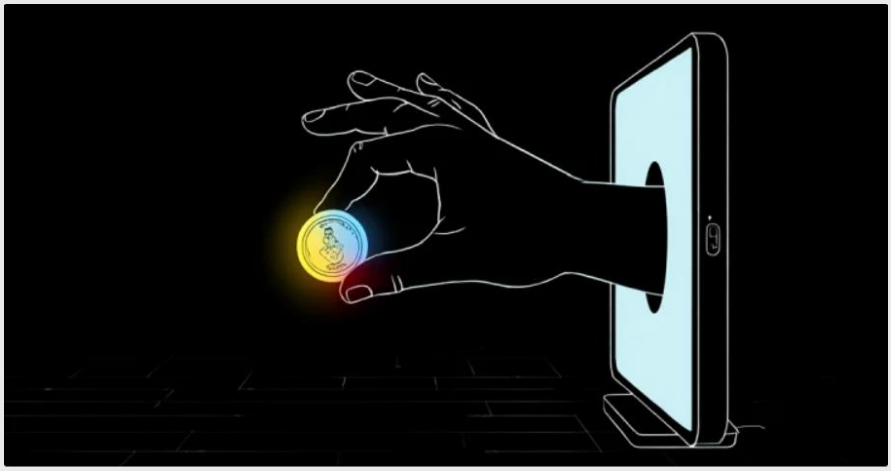
Cyber Threat and Intelligence Awareness Report

CryptoGen

the security focus company

CryptoGen | the security focus company

Blind Eagle Uses Proton66 Hosting for Phishing, RAT Deployment on Colombian Banks



ID : **0142**

Severity : **High**

CTIA Type : General

Date : **07 July 2025**

Time: **15:50 pm**

Executive Summary

The Latin American threat group **Blind Eagle** is carrying out a phishing and malware attack campaign against financial institutions in Colombia. The infrastructure of the Russian bulletproof hosting provider **Proton66** is used by the attackers, which results in the detection of an active threat cluster utilizing **Visual Basic Script (VBS)** files as the first step toward installation of **off-the-shelf Remote Access Trojans (RATs).**

The offense commences using the phishing of emails with **VBS** files. Once they are opened by a victim of this attack, they discreetly install remote-access tools like **AsyncRAT** and **Remcos** which enable the attackers to take control of the infected computer and extract valuable data. Although **VBS** itself appears outdated, it works well on Windows, and it is in the background silently. Attackers use it to download malware loaders, bypass antivirus tools, and blend into normal user activity. These scripts which are usually lightweight may only be an initial step in a series of stages with which attackers deploy or utilize **RATs**, data stealers or keyloggers.

The main targets are the banks of Colombia such as **Bancolombia**, **BBVA**, **Banco Caja Social**, and **Davivienda**. The hackers create fake websites that look like real bank web sites to trick users into entering their credentials. The attackers are hiding their actions by using some services such as **DuckDNS**, to create fake Website addresses to the same Proton66 server. So, antivirus programs have a hard time detecting them.

This is significant since these attacks may cause stolen bank passwords and personal information. They can be safe by being cautious about unexpected emails and files, not opening random script files, using long strong passwords with two-factor authentication, and updating their software. It is also possible to prevent the attacks by blocking suspicious websites and IP addresses connected to **Proton66** and **DuckDNS**.

Mitigation Strategies

- Keep all systems and software up to date, especially with patches addressing known vulnerabilities like CVE-2024-43451.
- Disable VBS execution where not needed via Group Policy.
- Use advanced email filtering to catch VBS attachments and phishing links.
- Conduct effective cyber security awareness training for the organization’s employees.
- Update SIEM, EDR and other endpoint security software with above mentioned IOCs.

References

- https://thehackernews.com/2025/06/blind-eagle-uses-proton66-hosting-for.html

Indicators of Compromise (IoCs)

IPs:

- 45.135.232[.]38

Domains:

- gfast.duckdns[.]org
- njfast.duckdns[.]org

Malware Tools:

- AsyncRAT
- Remcos RAT