Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

# HORABOT: EL MALWARE QUE APUNTA DIRECTAMENTE A LATINOAMÉRICA

*12/ 05 / 2025*

# CONTENIDO

INTRODUCCIÓN ..... 3

RESUMEN ..... 5

NOTICIA COMPLETA ..... 7

CONTACTOS DE SOPORTE ..... 8

# INTRODUCCIÓN

En un panorama digital cada vez más amenazante, una nueva campaña de malware está causando alarma en América Latina. Se trata de Horabot, una amenaza sigilosa que combina ingeniería social, scripts avanzados y técnicas de evasión para robar información sensible. Detectado por FortiGuard Labs, este malware se propaga principalmente a través de correos electrónicos falsos que simulan ser facturas legítimas en español.

Su objetivo: engañar a los usuarios para que abran archivos adjuntos maliciosos, iniciando así una cadena de infección que termina con el robo de credenciales, contactos y datos bancarios. Horabot no solo afecta al usuario individual, sino que también utiliza su cuenta de correo para seguir propagándose en redes personales y corporativas.

Lo más preocupante es que está diseñado específicamente para atacar a países de habla hispana, con un enfoque marcado en Latinoamérica. Esta amenaza demuestra cómo los ciberdelincuentes adaptan sus técnicas a contextos culturales y lingüísticos para lograr mayor efectividad. En este artículo, te explicamos cómo funciona Horabot, por qué es tan peligroso y qué puedes hacer para protegerte.

# HORABOT: EL MALWARE QUE APUNTA DIRECTAMENTE A LATINOAMÉRICA

A continuación, se encuentra en cuadro de identificación de la amenaza.

| | |
|---|---|
| **ID de alerta:** | DSOC-CERT_2025_05_12_1 |
| **Clasificación de alerta:** | Noticia |
| **Tipo de Impacto:** | Alta |
| **TLP (Clasificación de información):** | **CLEAR** |
| **Fecha de publicación:** | 12/05/2025 |
| **Es día cero (0 day):** | No |

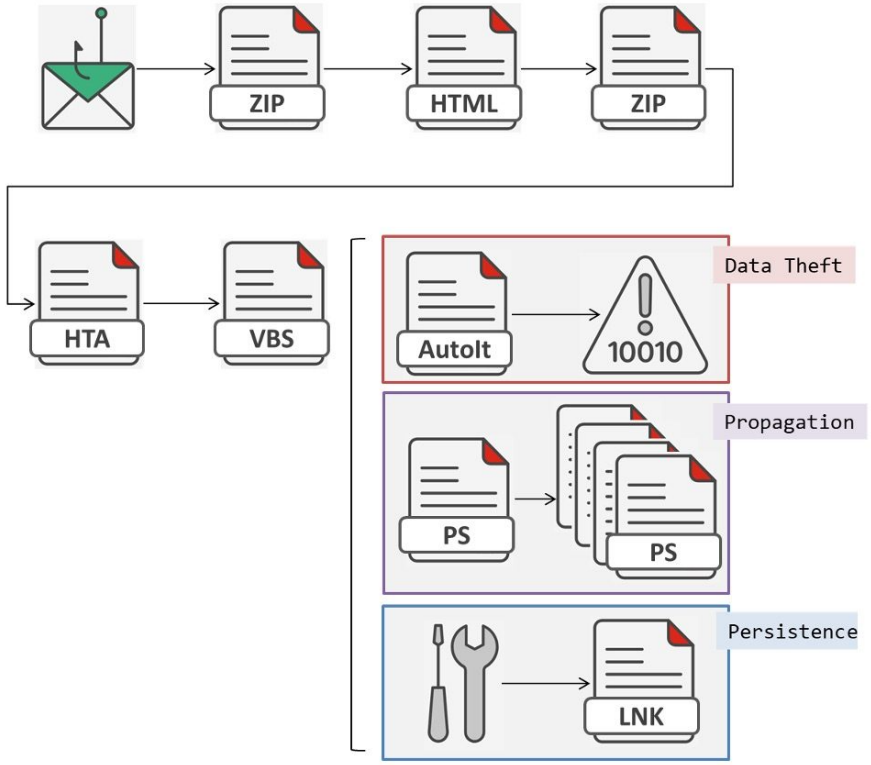
## RESUMEN

En los últimos meses, se ha identificado una creciente amenaza cibernética dirigida principalmente a usuarios de habla hispana en Latinoamérica. Se trata de **Horabot**, una campaña de phishing altamente sofisticada que busca robar credenciales, distribuir troyanos bancarios y propagarse silenciosamente por redes personales y corporativas.

**¿Qué es Horabot?**
Horabot es una familia de malware que se propaga a través de correos electrónicos falsos que simulan ser facturas o documentos financieros. Están escritos en español y aparentan provenir de fuentes legítimas, principalmente de México. El objetivo es que el usuario descargue y abra un archivo adjunto malicioso, lo que inicia la infección.

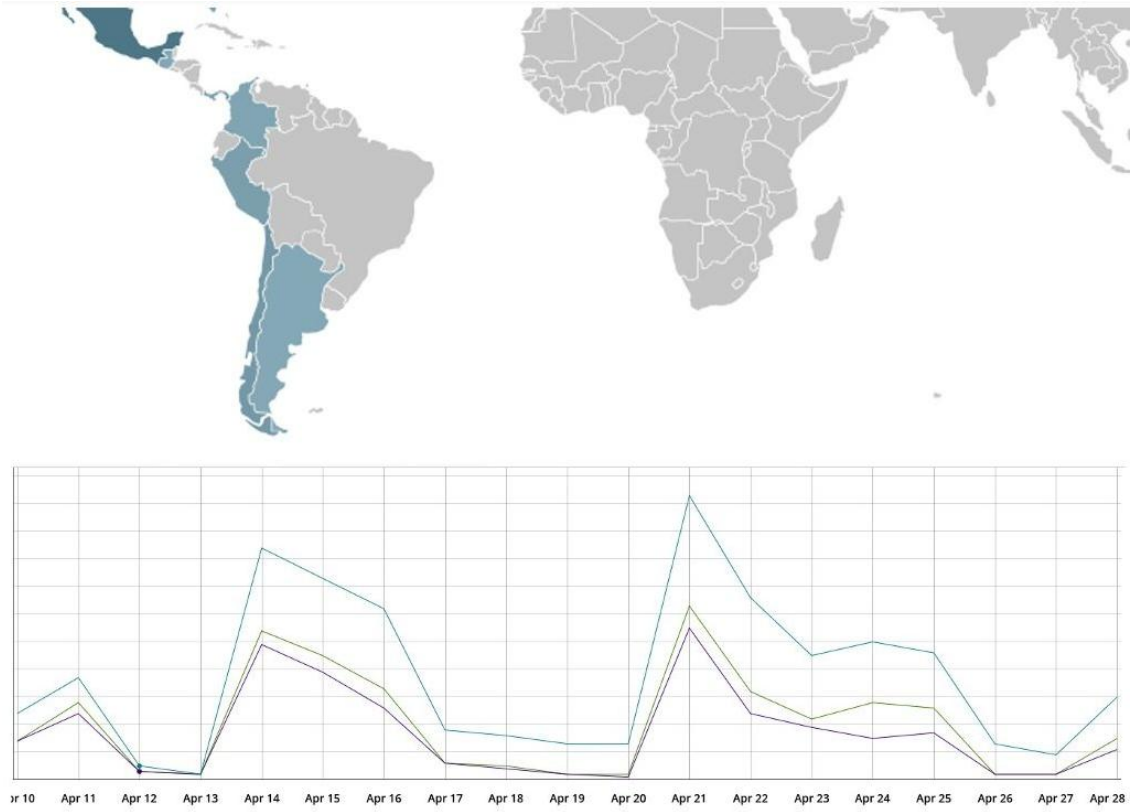
**¿Cómo infecta a sus víctimas?**
Todo empieza con un correo que contiene un archivo ZIP. Dentro hay un archivo HTML con código oculto en Base64. Al abrirlo, se descarga otro archivo que ejecuta un complejo conjunto de scripts (VBScript, AutoIt y PowerShell) diseñados para:

- Detectar si el equipo tiene antivirus o si está en una máquina virtual.
- Robar datos del sistema, como nombre del usuario, IP y versión de Windows.
- Descargar otros archivos maliciosos desde servidores remotos.
- Ejecutar un troyano bancario que roba credenciales, cookies y datos del navegador.
- Usar Outlook para reenviar automáticamente correos de phishing a contactos del usuario, propagándose aún más.
-



**¿Por qué es preocupante para Latinoamérica?**

Según la telemetría de FortiGuard, los principales países afectados hasta ahora son **México, Guatemala, Colombia, Perú, Chile y Argentina**. Al estar el malware especialmente diseñado en español, y utilizando ingeniería social basada en documentos financieros, resulta especialmente efectivo en nuestra región.




**¿Cómo protegerse?**

1. No abras archivos adjuntos sospechosos, especialmente si no esperabas recibirlos.
2. Verifica la fuente del correo. Aunque parezca legítima, revisa el dominio del remitente.
3. Mantén actualizado tu antivirus y sistema operativo.
4. Educa a tu equipo y compañeros sobre los riesgos del phishing.

**Conclusión**

Horabot no es un malware cualquiera. Es una campaña dirigida y sofisticada que utiliza herramientas legítimas del sistema operativo para operar sin ser detectado. Su capacidad para propagarse y robar información lo convierte en una amenaza real, especialmente para usuarios y empresas en Latinoamérica. Estar informados y preparados es la mejor defensa ante esta nueva ola de ciberataques.

## NOTICIA COMPLETA

https://devel.group/blog/horabot-el-malware-que-apunta-directamente-a-latinoamerica/

## INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/a11eed001a7a062e86f47f59061514bea59ea027/20250512_Horabot

# CONTACTOS DE SOPORTE


**Correo electrónico:** soporte@develsecurity.com

**Teléfonos directos:**

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

**Sitio Web:** https://devel.group/