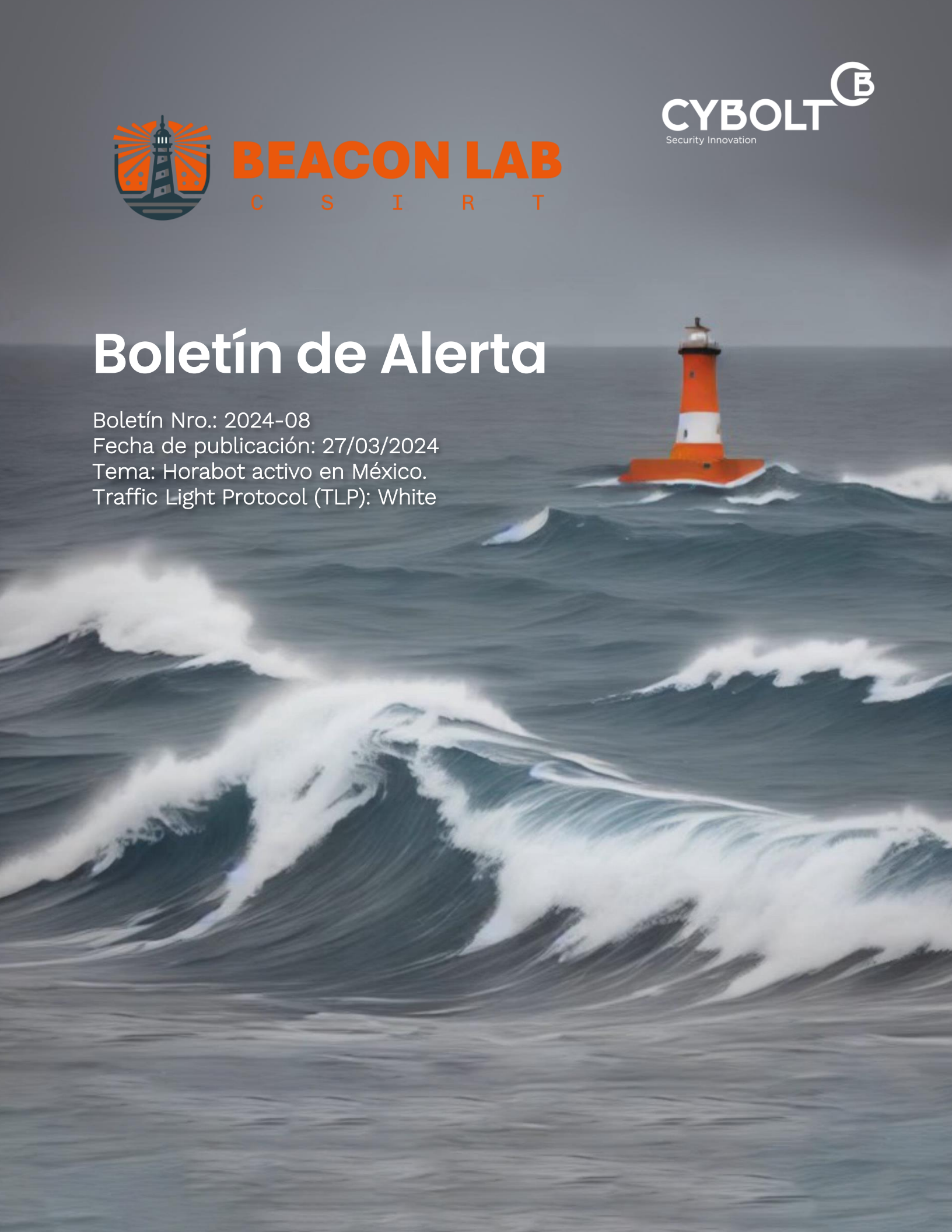
BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-08
Fecha de publicación: 27/03/2024
Tema: Horabot activo en México.
Traffic Light Protocol (TLP): White



Boletín de Alerta

Descripción

En los últimos días, se ha observado un incremento de actividad de **Horabot** en México, una campaña de **phishing**. Se estima que **Horabot** ha estado en progreso desde el mes de noviembre del 2020, dicha campaña, parece sólo estar dirigida a usuarios **hispanohablantes** localizados en Uruguay, Brasil, Venezuela, Argentina, Guatemala, Panamá y predominantemente en México.

Pero ¿Qué es "Phishing"?

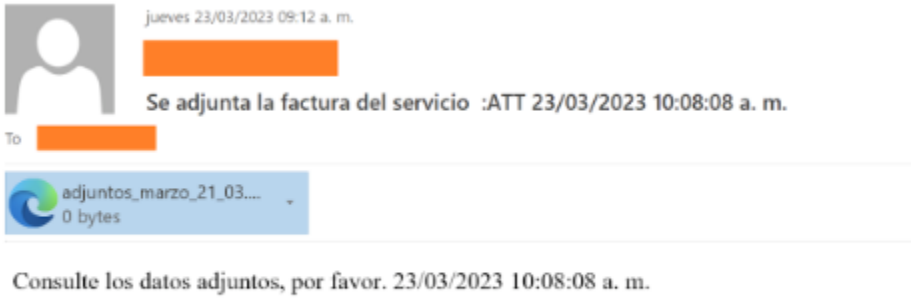
Es la práctica en la cual un atacante se contacta con una víctima por medios como el teléfono, correo electrónico, texto, o sitios falsos en internet, fingiendo ser una institución legitima. El objetivo principal del phishing es hacer que la víctima otorgue datos sensibles o que realicen acciones deseadas por el atacante, por ejemplo, la ejecución de programas maliciosos.

Cabe recalcar que existen varios tipos de phishing, el más común es aquel que está dirigido a muchísimas personas, con la esperanza de que alguna víctima caiga. El "Spear-phishing" es un ataque altamente dirigido a una víctima, la diferencia es que esteres es mucho más personalizado para hacerle creer a la víctima que es legítimo, por ejemplo, que la víctima esté esperando un correo de su jefe que tenga adjunta una presentación, el tacante, puede enviar su "spear-phishing", haciéndole creer que es el jefe, y adjuntando una "presentación", que en realidad sería un programa malicioso.

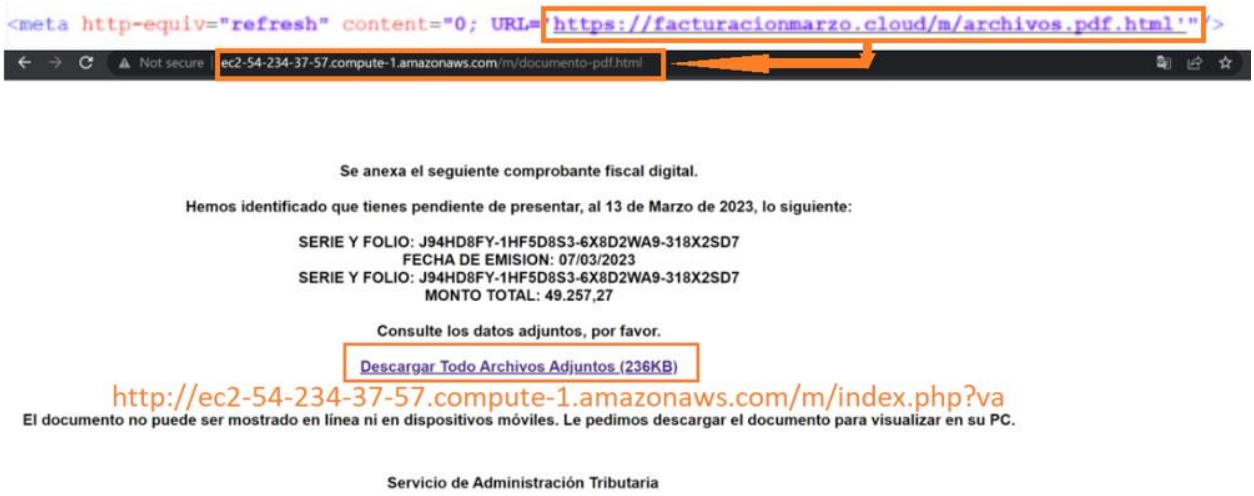
¿Qué hace la campaña Horabot?

Esta campaña involucra un ataque de varias etapas, inicia con un correo phishing que lleva a la ejecución de un script en Powershell que realiza una descarga automática de herramientas y ejecutables maliciosos.

El correo recibido por la campaña está escrito en español y se hace pasar por una notificación de factura, que incita al usuario a ingresar al archivo .html adjunto:



Al ingresar al archivo adjunto, nos redirigirá a una página web bajo el control del atacante, que nos incitará a dar click en un hipervínculo que nos descargará un archivo .rar.



Este archivo contendrá un batch file (.cmd) que procederá con la infección, descargando un script de powershell que descargará un archivo comprimido .zip que en su interior, tendrá varios archivos legítimos y algunos DLLs que se ejecutarán al cada vez que se encienda el dispositivo, además después de esto, se forzará un reinicio del dispositivo en los próximos 10 segundos, lo que obligará a que se ejecuten estos archivos DLL.

Al encenderse nuevamente el dispositivo, se descargarán y ejecutarán de otro servidor controlado por el atacante, dos scripts de powershell, uno que vuelve a descargar los DLLs y otro que será Horabot.

El objetivo de Horabot, es recolectar todas las direcciones de correo como sean posibles de nuestros contactos o buzones con los que hemos interactuado para poder extender el ataque a cuantos más víctimas se pueda, además, cabe recalcar que la

intención también es el robo de nuestros datos bancarios, que eventualmente serán capturados por el troyano que se instala en nuestros dispositivos.

Impacto

Cuando un usuario cae ante un phishing, este puede llegar a eludir varias defensas de seguridad que se hayan implementado en el perímetro, además de que esta acción sería encadenada por el consentimiento del usuario al dar clic en algún archivo o link malicioso adjunto en algún correo u otro medio de phishing. En el caso específico de Horabot, haría que nuestro dispositivo sea parte de una botnet, además de ser víctimas de troyano que puede robar nuestra información financiera.

Recomendaciones

- Contar con mecanismos de protección de correo, ya sea algún antispam o Email Security Gateway donde se limpien/revisen los contenidos de los correos
- Contar con estrategias permanentes de concientización de usuarios que les permita identificar cualquier tipo de correo sospechoso y actuar correctamente ante ellos (no hacer clic, reportarlo, etc.)
- Implementar reglas de detección y/o bloqueo de los indicadores de compromiso conocidos de esta botnet, algunos de los cuales pueden ser encontrados en la sección “Indicadores de compromiso” de este reporte.

Indicadores de compromiso (IoC)

En este apartado compartimos indicadores de compromiso acerca de Horabot, por un lado, podemos consultar los que ya existen en la inteligencia de TALOS de Cisco en el siguiente enlace: https://github.com/Cisco-Talos/IOCs/blob/main/2023/05/new-horabot-targets-americas.txt

Aunque también compartimos algunos indicadores recientemente compartidos por la comunidad de ciberseguridad:
Dominios:
- facturasm[.]cloud
- adbd[.]tech
- satventasfac[.]tech
- facturasmex[.]cloud
- facturasm[.]cloud
- archivosdwn[.]cloud
- facturas[.]co[.]in
- ca1.sytes[.]net
- ad2.gotdns[.]ch
- adbd[.]tech
- tths.ddns[.]net
- temporary[.]link
- facturas[.]co[.]in

Lista con IPs: Horabot IP addresses email senders - Pastebin.com

Referencias

- Phishing | What Is Phishing?
- ¿Qué es el spear phishing? Definición y riesgos (kaspersky.com)
- New Horabot campaign targets the Americas (talosintelligence.com)
- La nueva campaña de Horabot apunta a América Latina (cisco.com)

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com