Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

CIBERDELINCUENTES APUNTAN A AMÉRICA LATINA CON UN SOFISTICADO ESQUEMA DE PHISHING

10 / 04 / 2024

CONTENIDO

INTRODUCCIÓN

En un escenario digital marcado por la constante evolución de las amenazas cibernéticas, América Latina emerge como un objetivo destacado para los ciberdelincuentes. Una nueva campaña de phishing ha puesto de manifiesto la sofisticación de las tácticas utilizadas, revelando una serie de ataques dirigidos a sistemas Windows en la región. Con correos electrónicos cuidadosamente diseñados y archivos maliciosos camuflados como facturas legítimas, los perpetradores están desplegando una red compleja de engaños para comprometer la seguridad de los usuarios. Esta creciente amenaza no solo es un recordatorio de la importancia de la seguridad cibernética, sino también un llamado a la acción para fortalecer las defensas y proteger la integridad de los datos en un entorno digital cada vez más peligroso.

CIBERDELINCUENTES APUNTAN A AMÉRICA LATINA CON UN SOFISTICADO ESQUEMA DE PHISHING

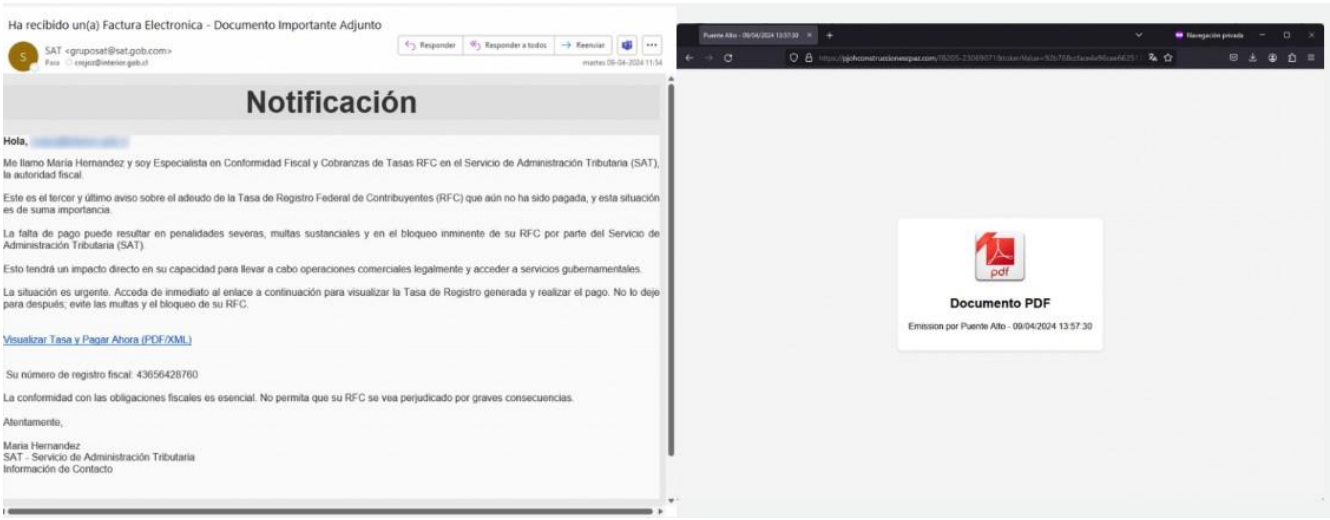
A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_04_10_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	10/04/2024
Es día cero (0 day):	No

RESUMEN

América Latina emerge como un objetivo prioritario para los ciberdelincuentes. Una nueva campaña de phishing ha puesto en alerta a expertos en seguridad cibernética, revelando tácticas cada vez más sofisticadas dirigidas a sistemas Windows en la región.

La estrategia empleada por los atacantes implica un enfoque meticuloso y multifacético. Los correos electrónicos de phishing, disfrazados como facturas legítimas, contienen archivos adjuntos ZIP que, al ser extraídos, conducen a una serie de descargas maliciosas. Estas descargas incluyen archivos HTML que, al ser accedidos desde direcciones IP geolocalizadas en América Latina, desencadenan una cadena de eventos que culminan en la instalación de scripts de PowerShell y la ejecución de programas diseñados para recolectar información del sistema comprometido.



Conexiones con Campañas Previas

Expertos en seguridad han identificado similitudes entre esta campaña y ataques anteriores, como las perpetradas por el malware Horabot. Este patrón sugiere una evolución constante de las estrategias utilizadas por los ciberdelincuentes para dirigirse a usuarios de habla hispana en la región.

El Contexto Global

Esta nueva oleada de ataques no es un caso aislado. En un panorama global, otros vectores de ataque están en constante evolución. Desde campañas de publicidad maliciosa hasta la distribución de troyanos de acceso remoto alojados en plataformas populares como Dropbox, los ciberdelincuentes están aprovechando cualquier oportunidad para infiltrarse en sistemas vulnerables.

Las Amenazas Emergentes

Además de las tácticas tradicionales de phishing, los expertos han identificado nuevas amenazas emergentes en la región. Desde la utilización de falsos instaladores de software hasta la implementación de malware programado en Golang, los ciberdelincuentes están adoptando enfoques cada vez más

sofisticados para eludir los sistemas de seguridad y comprometer la integridad de los datos y la privacidad de los usuarios.

Conclusiones

Ante esta creciente amenaza, es imperativo que las empresas y los usuarios refuercen sus medidas de seguridad cibernética. La concientización, la educación y la implementación de soluciones de seguridad robustas son fundamentales para mitigar el riesgo y protegerse contra las cada vez más complejas tácticas utilizadas por los ciberdelincuentes. En un mundo digitalmente interconectado, la prevención es la mejor defensa contra las crecientes amenazas que acechan en el horizonte cibernético.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20240410_1_Horabot

NOTICIA COMPLETA

https://devel.group/blog/ciberdelincuentes-apuntan-a-america-latina-con-un-sofisticado-esquema-de-phishing/

CONTACTOS DE SOPORTE

Correo electrónico: cert@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://www.devel.group/reporta-un-incidente