Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

CAMPAÑA MASIVA DE PHISHING GOLPEA AMÉRICA LATINA: VENOM RAT DIRIGIDO A MÚLTIPLES SECTORES

03 / 04 / 2024

CONTENIDO

INTRODUCCIÓN

La ciberseguridad se enfrenta a un desafío creciente y complejo con la reciente aparición de una importante campaña de phishing en América Latina. Impulsada por el grupo de amenazas TA558, esta campaña tiene como objetivo propagar el malware Venom RAT en diversos sectores, desde hoteles y finanzas hasta sectores gubernamentales. La sofisticación del ataque, que utiliza correos electrónicos de phishing como punto de entrada, subraya la urgencia de una respuesta coordinada y proactiva en la región. Este informe revela la naturaleza global de la amenaza, destacando la necesidad de que las organizaciones implementen medidas de seguridad robustas y estén alerta ante las tácticas en constante evolución de los ciberdelincuentes.

CAMPAÑA MASIVA DE PHISHING GOLPEA AMÉRICA LATINA: VENOM RAT DIRIGIDO A MÚLTIPLES SECTORES

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

ID de alerta:	DSOC-CERT_2024_04_03_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	03/04/2024
Es día cero (0 day):	No

RESUMEN

Una importante campaña de phishing ha sido desatada por el actor de amenazas conocido como TA558, dirigida a varios sectores en América Latina. La campaña tiene como objetivo desplegar Venom RAT, representando una seria amenaza para organizaciones en España, México, Estados Unidos, Colombia, Portugal, Brasil, la República Dominicana y Argentina.

Sectores Objetivo

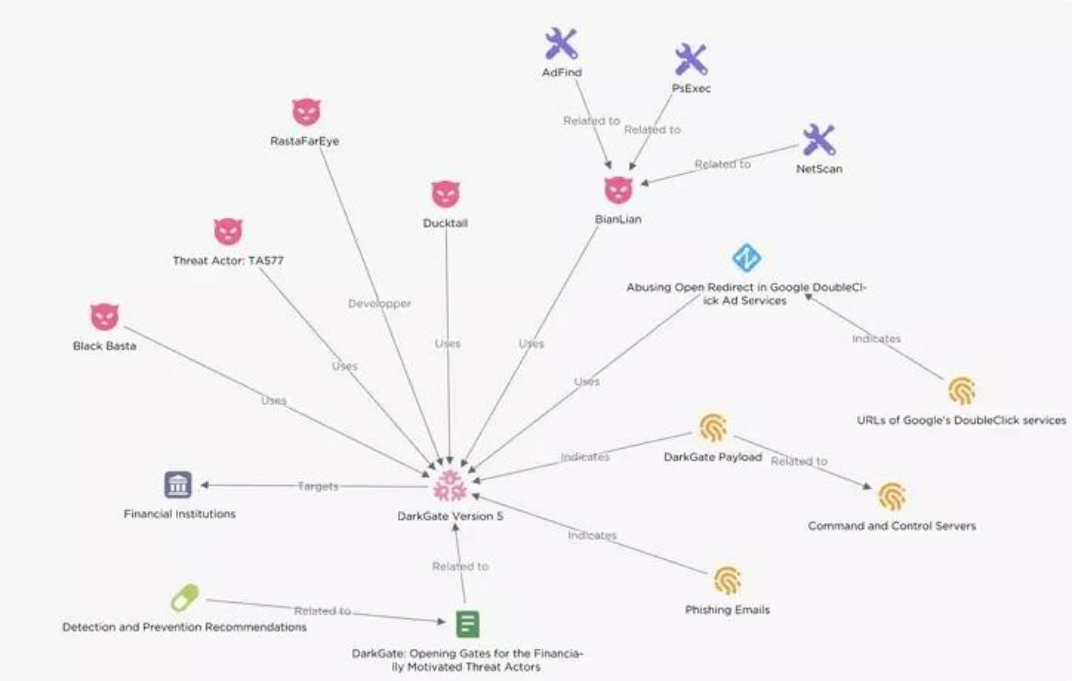
Los ataques de phishing se centran especialmente en industrias como hoteles, viajes, comercio, finanzas, manufactura, industrial y sectores gubernamentales. TA558 tiene un historial de despliegue de malware en la región LATAM, incluyendo Loda RAT, Vjw0rm y Revenge RAT, datando al menos desde 2018.

Vector de Ataque

El investigador de Perception Point, Idan Tarab, revela que los atacantes inician la cadena de infección a través de correos electrónicos de phishing. Una vez accedidos, los correos electrónicos descargan Venom RAT, un derivado de Quasar RAT. Venom RAT está equipado con funcionalidades para extraer datos sensibles y controlar remotamente sistemas comprometidos.

Tendencias Recientes en Amenazas Cibernéticas

Esta revelación coincide con el creciente uso del cargador de malware DarkGate por parte de actores de amenazas, especialmente después de la interrupción de las operaciones de QakBot por parte de las autoridades el año pasado. Además, las campañas de malvertising han estado en aumento, entregando variantes de malware como FakeUpdates, Nitrogen y Rhadamanthys.



Asaltos de Malvertising en Video

De particular preocupación es el cambio observado en las tácticas de malvertising, con ScamClub ahora centrado en asaltos de malvertising en video. Estos ataques aprovechan las plantillas de Servicio de Anuncios de Video (VAST) para redirigir a los usuarios a páginas fraudulentas, empleando sofisticadas técnicas de huellas digitales tanto del lado del cliente como del servidor.

Impacto Geográfico

La mayoría de las víctimas se concentran en Estados Unidos, seguido por Canadá, Reino Unido, Alemania y Malasia. Sin embargo, las organizaciones en todo el mundo deben permanecer vigilantes ante las amenazas cibernéticas en evolución, adoptando medidas de seguridad robustas para mitigar los riesgos de manera efectiva.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20240403_01_VenomRAT

NOTICIA COMPLETA

https://devel.group/blog/campana-masiva-de-phishing-golpea-america-latina-venom-rat-dirigido-a-multiples-sectores/

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