Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Boletín Informativo

.

10/mayo/2022

Contenido

Introducción

El siguiente boletín presenta información sobre vulnerabilidades descubiertas por el equipo de Devel Security, correspondiente a una campaña de malware mediante email.

MALWARE DETECTADO EN CORREOS MALICIOSOS.

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

ID de alerta:	DSOC-CERT_2022_05_10
Clasificación de alerta:	MALWARE
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**WHITE**
Fecha de publicación:	05/10/2022
Es día cero (0 day):	NO

RESUMEN

La campaña fue detectada el día 10 de mayo del año en curso, consta de direcciones de correo electrónico transportando archivos en formato .xlsx, con carga maliciosa que busca corromper su sistema operativo y muy probablemente abrir puertas traseras para el robo de información.

Mediante análisis se han encontrado los indicadores de compromiso del malware en cuestión, arrojando resultados que clasifican la amenaza con un nivel alto.

Resultados del análisis:

Security Vendors' Analysis

Avast	VBS:Malware-gen	AVG	VBS:Malware-gen
ClamAV	Doc.Downloader.Qbot-af43432fbcb8603...	Cyren	XF/Qbot.J.genIEldorado
F-Secure	Malware.W97M/Dldr.Quakbot.VE	Fortinet	VBA/Dloader.NF!tr
GData	Macro.Trojan-Downloader.Agent.BDH	Ikarus	Win32.Outbreak
Kaspersky	HEUR:Trojan.Script.Generic	McAfee	X97M/Downloader.oy
McAfee-GW-Edition	X97M/Downloader.oy	Microsoft	Trojan:Script/Sabsik.FL.Blml
Sophos	Troj/DocDl-AFYL	ZoneAlarm by Check Point	HEUR:Trojan.MSOffice.Generic

Como parte del trabajo realizado por el SOC de Devel Security los IOC de esta amenaza emergente ya se han cargado en los SIEM de nuestros clientes y se mantiene monitoreo constante para evitar vectores de ataque similares a este, que respondan a las mismas fuentes maliciosas detectadas.

Actualmente nuestro SOC se encuentra analizando las muestras obtenidas de este ataque para validar que no represente riesgos mayores (Como un ataque de Ransomware).

Recomendaciones

Se recomiendan las siguientes acciones:

- No descargar archivos adjuntos de correos electrónicos desconocidos.
- No ejecutar aplicativos desconocidos, sin recibir la aprobación de su departamento de IT.
- Validar si en la carpeta SPAM se encuentran correos Phishing, de ser así favor.
- Aplicar el bloqueo de los IOC según la plataforma y categoría a la que estos correspondan.
- Comunicarse a su SOC y solicitar monitoreo a la posible comunicación entre su red interna y las IPs adjuntas en los IOC.

Indicadores de compromiso

https://github.com/develgroup/SOC_IOCs/tree/main/20220510_01

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