CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Operación Pulpo Rojo

Fecha: 06/01/2023

Problemática: Campaña de malware dirigida a organismos de alto perfil de Ecuador y países de la región

Correlativo: AC-0008

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

El equipo de investigación de ESET Latinoamérica compartió detalles de una campaña de malware dirigida a organizaciones de alto perfil que se llevó adelante entre finales de junio y primeros días de julio de 2022. Denominada Operación Pulpo Rojo, esta campaña maliciosa registró actividad en varios países de América Latina, pero de acuerdo a los sistemas de ESET se concentró principalmente en Ecuador, apuntando a organismos gubernamentales, organizaciones del sector de la salud y compañías privadas de distintas industrias. Los países a los que afectó la campaña se encuentran Perú 3%, Estados Unidos 3%, Guatemala 2%, Colombia 1% y Basil 1%.

SITUACIÓN

La naturaleza del incidente corresponde a un conocido troyano de acceso remoto (RAT) Remcos. Si bien Remcos es un software legítimo que fue desarrollado para monitorear y administrar remotamente dispositivos, desde hace unos años que viene siendo utilizado también por ciberdelincuentes en distintas campañas maliciosas que buscan espiar y robar información de los equipos de sus víctimas. Los operadores detrás de la Operación Pulpo Rojo utilizaron distintos servicios gratuitos para alojar sus códigos maliciosos, como Google Drive o la plataforma Discord, pero se destacó por el uso de diferentes técnicas para evitar ser detectados, ya sea por una solución de seguridad, como también por una víctima que vea un comportamiento anómalo en su equipo. La forma de infectar a las víctimas fue a través de correos de phishing

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	Preventiva

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	Alta	Alta	Alta

RECOMENDACIONES

Considere implementar:

1. Servicios de Antivirus/Antimalware.
2. Herramientas de Prevención de Intrusiones en la red (IDS)
3. Herramientas de Detección y Respuesta de Amenazas de Puntos Finales (EDR)
4. Herramientas de Detección y Respuesta Extendidas (XDR)

Es importante:

1. Actualizar regularmente los sistemas operativos, el hardware y el software de los dispositivos.
2. Llevar a cabo una rutina periódica de actualización y parcheo de los sistemas operativos y programas ofimáticos.
3. Implementar planes de recuperación ante desastres de TI que contengan procedimientos para realizar y probar regularmente copias de seguridad de

DICCIONARIO DE DATOS

1. Infostealer: Nombre genérico de programas informáticos maliciosos del tipo troyano, que se introducen a través de internet en un ordenador con el propósito de obtener de forma fraudulenta información confidencial.
2. Endpoint Detection and Response-EDR (Detección y Respuesta de Amenazas de Puntos Finales): Tecnología de ciberseguridad que monitorea continuamente un "punto final" para mitigar amenazas cibernéticas maliciosas
3. Extended Detection and Response - XDR (Detección y Respuesta Extendidas): Tecnología de ciberseguridad que monitorea y mitiga las amenazas de ciberseguridad
4. Cifrado: Operación o función matemática utilizada en combinación con una clave que se aplica a un texto en claro y permite obtener un texto cifrado (o descifrarlo) garantizando la confidencialidad e integridad de la información contenida.
5. Malware: Es un programa malicioso que tiene como característica principal su alto grado de dispersabilidad, es decir, lo rápidamente que se propaga.
6. Ransomware: Es un tipo de malware que impide y/o secuestra el acceso a archivos del sistema infectado, en ocasiones cifrándolos, y coacciona al usuario para pagar un rescate a cambio de su liberación.

REFERENCIAS

1. Documentación alerta ESET https://www.welivesecurity.com/la-es/2022/08/30/campana-malware-dirigida-organismos-alto-perfil-ecuador/
2. https://attack.mitre.org/techniques/T1486/
3. https://attack.mitre.org/techniques/T1566/