| | |
|---|---|
| Alerta de seguridad informática | 2CMV23-00427-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing-Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 28 de julio de 2023 |
| Última revisión | 28 de julio de 2023 |

PARA EL CORRECTO USO Y DIVULGACIÓN DE ESTE DOCUMENTO LEER ACÁ

## Resumen


El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) ha identificado una nueva campaña de phishing con malware, que se difunde a través de email suplantando a la empresa mexicana Magus SA. de CV. con una falsa cotización de productos.

Si la víctima interactúa con el fichero malicioso sufrirá la explotación de una vulnerabilidad en Microsoft Office que permite ejecutar código de forma remota en el sistema. Esta vulnerabilidad refiere a un mal manejo de los objetos en la memoria por parte del antiguo editor de ecuaciones de Office (EQNEDT32.EXE).

El archivo Excel maliciosa transporta un malware llamado Agent Tesla, un troyano de acceso remoto (RAT) diseñado para sustraer información de sus víctimas. Para eso, registra lo que se digita en el equipo infectado (función keylogger), toma capturas de pantalla, visualiza y copia lo que hay en el portapapeles, y extrae contraseñas y cookies de múltiples navegadores web, VPN (como Open VPN y Nord VPN) y también de Microsoft Outlook.

# Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

## SHA256

| Indicador | Relación |
|---|---|
| 860be34105da8de5e28d2501b10aa7aac1932c8e028ff107a74858b9f04af001 | Nueva Orden.xlsx.malz |
| 71e00f9e4d1b0ed0f6125950c172a29b1a8b3d422762b539fd14355b2834d1d3 | stage_2.exe.malz |
| 7a2f296746c0ef1567faa12e7fe1902c4d74efda27045a5e4593fa91943dff9b | download.exe.malz |
| b0c79c0f087b28e30cf4126ad4766ac21723ef5c41cb3aba8e04eb4c68e88558 | universo_vbs.jpeg.malz |
| 5a60dc7db48a0e7c248937c62c3edce2101fb507186b595b5a52ab75cb4480d0 | Vbs Online.vbs.malz |
| 1eae83fc3a1539d80cb03b6ece9091a1c33c44fd3f97a89beec2b62ffe07dcb9 | cococococ.vbs |

## URL-Dominio

| Dominio | Relación |
|---|---|
| http://45.88.66[.]43/Vbs%20Online.vbs | Configuración Malware |
| http://45.88.66[.]43/WHEEHEHEHEH.txt | Configuración Malware |
| https://cdn.pixelbin[.]io/v2/red-wildflower-1b0af4/original/universo_vbs.jpeg | Configuración Malware |

## MITRE ATT&CK

| Descripción | ID |
|---|---|
| Acceso Inicial (Mediante Phishing) | T1566.002 |
| Descubrimiento (Consulta del Registro) | T1012 |
| Descubrimiento (Información del Sistema) | T1082 |
| Ejecución (Explotación para ejecución en cliente) | T1203 |
| Acceso a credenciales (credenciales en archivos) | T1081 |
| Colección (Datos del sistema local) | T1005 |
| Colección (Colección Email) | T1114 |

## Imagen del Mensaje


CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.07.31 12:30:40 -04'00'