Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

COYOTE BANKING TROJAN: UNA AMENAZA SILENCIOSA A TRAVÉS DE ARCHIVOS LNK

03 / 02 / 2025

CONTENIDO

INTRODUCCIÓN

Coyote Malware es un troyano bancario sofisticado que ha expandido su alcance a 1,030 sitios web y 73 instituciones financieras en Brasil, utilizando archivos LNK maliciosos y comandos PowerShell para ejecutar cargas útiles. Capaz de realizar keylogging, capturas de pantalla, superposiciones de phishing y evasión de entornos virtuales, representa una amenaza crítica para la ciberseguridad financiera. Devel Group recomienda fortalecer la concienciación del usuario, restringir PowerShell, implementar EDR avanzados, segmentar redes, monitorear continuamente y mantener sistemas actualizados para mitigar su impacto.

COYOTE BANKING TROJAN: UNA AMENAZA SILENCIOSA A TRAVÉS DE ARCHIVOS LNK

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

ID de alerta:	DSOC-CERT_2024_02_03_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	03/02/2025
Es día cero (0 day):	No

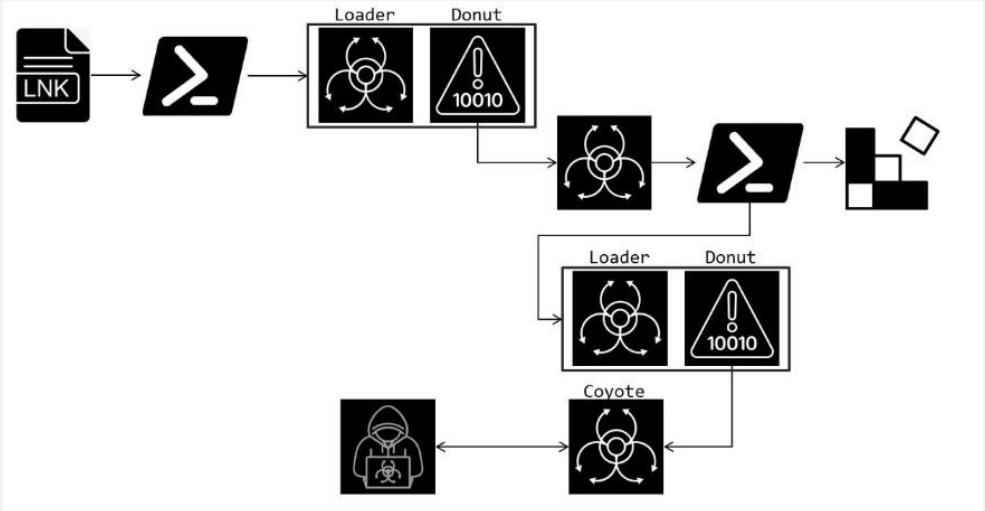
RESUMEN

Coyote Malware, un troyano bancario previamente documentado, ha ampliado su alcance, afectando a 1,030 sitios web y 73 instituciones financieras, principalmente en Brasil. Este malware, identificado inicialmente por Kaspersky en 2024, ha evolucionado en sus tácticas, técnicas y procedimientos (TTPs), representando una amenaza creciente para la ciberseguridad financiera en la región.

DETALLES TÉCNICOS

- **Vector de Infección:** El ataque comienza con un archivo LNK malicioso que ejecuta comandos PowerShell para descargar cargas útiles desde servidores remotos.

- **Cadena de Infección:** Utiliza un script PowerShell para lanzar un loader que ejecuta un payload intermedio. Se detectó el uso de Donut, una herramienta que descifra y ejecuta payloads MSIL.



- **Persistencia:** Modifica el registro de Windows en 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' para establecer persistencia.
- **Funcionalidades Maliciosas:**
  - Keylogging
  - Captura de pantalla
  - Superposición de ventanas de phishing (phishing overlays)
  - Recolección de información del sistema y software de seguridad instalado
  - Evasión de entornos sandbox y máquinas virtuales

Técnica MITRE ATT&CK	Descripción	ID MITRE
Command and Scripting Interpreter: JavaScript	Tras la ejecución de Squirrel, una aplicación NodeJS se ejecuta y ejecuta código JavaScript ofuscado.	T1059.006
User Execution: Malicious File	El cargador inicial está disfrazado como un actualizador Squirrel.	T1204.002
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	El valor de registro se agrega a la clave HKCU\Environment\UserInitMprLogonScript (antes de verificar su existencia). El valor agregado en el caso que observamos: "obs-browser-page.exe" es para establecer la persistencia.	T1547.001
Hijack Execution Flow: DLL Side-Loading	El troyano se carga a través de la carga lateral de una DLL de una dependencia de los ejecutables de Chrome y OBS Studio (libcef.dll).	T1574.002
System Binary Proxy Execution	Uso de Squirrel para crear paquetes de instalación y actualizaciones ocultando el vector de infección en un actualizador.	T1218
Obfuscated Files or Information	El troyano utiliza ofuscación de cadenas con cifrado AES. La aplicación NodeJS ejecuta código JavaScript ofuscado.	T1027
Reflective Code Loading	NIM se utiliza para cargar la etapa final, que descomprime el ejecutable .NET y lo ejecuta en la memoria mediante CLR.	T1620

Masquerading: Match Legitimate Name or Location	Coyote oculta su cargador inicial presentándolo como un empaquetador de actualizaciones.	T1036.001
Code Signing	Uso de aplicación firmada con biblioteca legitima.	T1553.002
Execution Guardrails	Una vez que el malware verifica que efectivamente la conexión es con el atacante, procede a enviar la información recopilada de la máquina infectada y las aplicaciones bancarias al servidor.	T1480.001
System Information Discovery	La información enviada a C2 incluye: Nombre de la máquina, GUÍA, Aplicación(nes) bancaria(s) que se están utilizando.	T1082
Application Windows Discovery	El troyano monitorea todas las aplicaciones abiertas en el sistema de la víctima y espera a que se acceda a la aplicación bancaria o al sitio web específico.	T1010
Input Capture: Keylogging	El troyano tiene la capacidad de realizar registros de teclas.	T1056.001
Screen Capture	El troyano tiene la capacidad de tomar capturas de pantalla.	T1113
Encrypted Channel	El troyano establece comunicación con su servidor C2 utilizando canales SSL con un esquema de autenticación mutua.	T1573
Traffic Signaling	El atacante envía un paquete de respuesta que contiene acciones específicas. Para procesar estas acciones, el atacante transmite una cadena con un delimitador aleatorio. Cada posición de la cadena se convierte en una lista, en la que la primera entrada representa el tipo de comando.	T1205
System Shutdown/Reboot	El troyano tiene la capacidad de apagar el sistema comprometido.	T1529

IMPACTO

- Expansión del objetivo a 1,030 sitios y 73 entidades financieras, incluyendo plataformas de criptomonedas y servicios hoteleros.
- Potencial para robo masivo de credenciales, fraude financiero y acceso no autorizado a sistemas críticos.

RECOMENDACIONES DE MITIGACIÓN

1. **Fortalecimiento de la Concientización del Usuario:** Capacitar a los colaboradores para identificar correos electrónicos y archivos adjuntos sospechosos, especialmente aquellos que contienen archivos LNK.
2. **Restricciones de PowerShell:** Implementar políticas de restricción para el uso de PowerShell, permitiendo solo scripts firmados y monitoreando su ejecución.
3. **Seguridad en el Endpoint:** Utilizar soluciones EDR avanzadas que detecten comportamientos anómalos, como la manipulación del registro y la ejecución de scripts no autorizados.
4. **Segmentación de Red:** Limitar el movimiento lateral del malware mediante la segmentación de la red y el uso de firewalls internos.
5. **Revisión de Logs y Monitoreo Continuo:** Implementar capacidades de monitoreo continuo para detectar patrones de comportamiento relacionados con la actividad del malware.
6. **Actualización y Parches:** Mantener los sistemas operativos y aplicaciones actualizados para mitigar vulnerabilidades explotables.

CONCLUSIÓN

Coyote Malware representa una amenaza sofisticada con un enfoque claro en el sector financiero. Su capacidad de adaptación y expansión requiere un enfoque integral de ciberdefensa, combinando tecnologías de detección avanzada, políticas de seguridad robustas y una cultura organizativa consciente de los riesgos cibernéticos.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20240203_CoyoteMalware

NOTICIA COMPLETA

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

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://devel.group/