El malware 'Coyote' comienza su búsqueda, aprovechándose de 61 aplicaciones bancarias

Brasil, el centro mundial de malware troyano bancario, ha producido una de sus herramientas más avanzadas hasta el momento. Y como muestra la historia, Coyote pronto podría expandir su territorio.

Imagen de Nate Nelson, escritor colaborador

Nate Nelson, escritor colaborador

8 de febrero de 2024

Lectura de 4 minutos

FUENTE: DESIGN PICS INC A TRAVÉS DE UNA FOTO DE STOCK DE ALAMY

Los investigadores han descubierto un novedoso troyano bancario al que denominaron "Coyote", que busca credenciales para 61 aplicaciones bancarias en línea diferentes.

"Coyote", detallado por Kaspersky en un análisis de hoy, se destaca tanto por su amplio enfoque en aplicaciones del sector bancario (la mayoría, por ahora, en Brasil), como por su sofisticado entrelazamiento de diferentes componentes rudimentarios y avanzados: una plataforma abierta relativamente nueva. instalador fuente llamado Squirrel; NodosJ; un lenguaje de programación desconocido llamado "Nim"; y más de una docena de funcionalidades maliciosas. En general, representa una evolución notable en el próspero mercado de malware financiero de Brasil y podría significar grandes problemas para los equipos de seguridad en el futuro si amplía su enfoque.

"Han estado desarrollando troyanos bancarios durante más de 20 años; comenzaron en el año 2000", dice Fabio Assolini, jefe del Equipo de Análisis e Investigación Global de América Latina (GReAT) de Kaspersky, sobre los desarrolladores de malware brasileños. "En 24 años de desarrollar y eludir nuevos métodos de autenticación y nuevas tecnologías de protección, han sido muy creativos y ahora se puede ver con este nuevo troyano".

Puede que por ahora sea una amenaza para los consumidores centrada en Brasil, pero como se mencionó, hay razones claras para que las organizaciones estén conscientes de Coyote. Por un lado, como advierte Assolini, "las familias de malware que tuvieron éxito en abordar el mercado brasileño en el pasado también se han expandido en el extranjero. Es por eso que las corporaciones y los bancos deben estar preparados para enfrentarlo".

Y otra razón para que los equipos de seguridad presten atención a la aparición de nuevos troyanos bancarios es su historial de evolución hacia troyanos de acceso inicial y puertas traseras totalmente desarrollados; Este fue el caso de Emotet y Trickbot, por ejemplo, y más recientemente, QakBot y Ursinif.

Coyote tiene una funcionalidad adicional para seguir su ejemplo: puede ejecutar una variedad de comandos, incluidas directivas para tomar capturas de pantalla, registrar pulsaciones de teclas, finalizar procesos, apagar la máquina y mover el cursor. También puede congelar completamente la máquina con una superposición falsa de "Trabajando en actualizaciones...".

El troyano Coyote se ejecuta con Squirrel y Nim

Hasta ahora, en sus ataques, Coyote se comporta como cualquier otro troyano bancario moderno: cuando se activa una aplicación compatible en una máquina infectada, el malware hace ping a un servidor de comando y control (C2) controlado por el atacante y muestra una superposición de phishing adecuada en la computadora de la víctima. pantalla para capturar la información de inicio de sesión de un usuario. Sin embargo, Coyote se destaca más por cómo combate posibles detecciones.

La mayoría de los troyanos bancarios utilizan instaladores de Windows (MSI), señaló Kaspersky en su publicación de blog, lo que los convierte en una señal de alerta fácil para los defensores de la ciberseguridad. Es por eso que Coyote opta por Squirrel, una herramienta legítima de código abierto para instalar y actualizar aplicaciones de escritorio de Windows. Utilizando Squirrel, Coyote intenta enmascarar su cargador de etapa inicial malicioso como un empaquetador de actualizaciones perfectamente honesto.

>Su cargador de etapa final es aún más exclusivo, ya que está escrito en un lenguaje de programación relativamente específico llamado "Nim". Este es el primer troyano bancario que Kaspersky identifica utilizando Nim.

"La mayoría de los antiguos troyanos bancarios estaban escritos en Delphi, que es bastante antiguo y se utiliza en muchas familias. Así que, con el paso de los años, la detección del malware Delphi se volvió muy buena y la eficiencia de las infecciones se fue desacelerando con el paso de los años. " explica Assolini. Con Nim, "tienen un lenguaje más moderno para programar con nuevas funciones y una baja tasa de detección por parte del software de seguridad".

Los troyanos bancarios brasileños son un problema global

Si Coyote tiene que hacer tanto para distinguirse, es porque la quinta nación más grande del mundo se ha convertido en los últimos años en el principal centro mundial de malware bancario.

Y por mucho que aterroricen a los brasileños, estos programas también tienen la costumbre de cruzar masas de agua.

"Estos chicos tienen mucha experiencia en el desarrollo de troyanos bancarios y están ansiosos por expandir sus ataques a todo el mundo", subraya Assolini. "Ahora mismo podemos encontrar troyanos bancarios brasileños atacando a empresas y personas en lugares tan lejanos como Australia y Europa. Esta semana, un miembro de mi equipo encontró una nueva versión de uno en Italia".

Para demostrar el futuro potencial de una herramienta como Coyote, Assolini señala Grandoreiro, un troyano similar que hizo importantes incursiones en México y España, pero también mucho más allá. A finales del otoño pasado, dice, había llegado a un total de 41 países.

Sin embargo, una consecuencia de ese éxito fue un mayor escrutinio por parte de las autoridades. En un paso para interrumpir el flujo libre de ciberseguridad para este tipo de malware, la policía brasileña tomó una medida inusual: ejecutó cinco órdenes de arresto temporales al año.

d 13 órdenes de registro e incautación para los arquitectos detrás de Grandoreiro en cinco estados brasileños.

"El problema en Brasil es que no tienen muy buena aplicación de la ley local para castigar a estos atacantes. Funciona mejor cuando tienes una entidad fuera del país aplicando cierta presión, como ocurrió con Granadoreiro, cuando la policía y los bancos en España estaban presionando a la policía federal brasileña para que capture a estos tipos", dice Assolini.

Entonces, concluye, "están mejorando, pero queda un largo camino por recorrer, porque muchos cibercriminales todavía están libres [en Brasil] y cometen muchos ataques en todo el mundo".