PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 10 de febrero de 2024

036-2024-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°036	Fecha: 10-02-2024
		Página: 4 de 8

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	El nuevo troyano Coyote apunta a 61 bancos brasileños con un ataque impulsado por Nim		
Tipo de Ataque	Troyanos	Abreviatura	Troyanos
Medios de propagación	USB, Disco, Red, Correo, Navegacion de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. **ANTECEDENTES**:

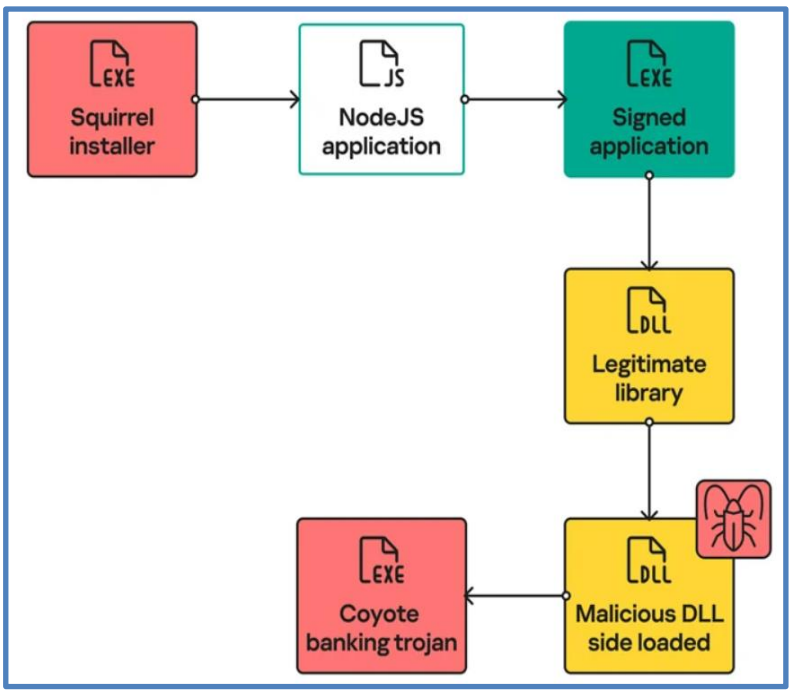
Los desarrolladores de malware troyano bancario están siempre buscando formas ingeniosas de distribuir sus implantes e infectar a las víctimas. En una investigación reciente, encontramos un nuevo troyano bancario, denominado Coyote, que está atacando actualmente 61 instituciones bancarias brasileñas. Lo que llama la atención es la sofisticada cadena de infección, que utiliza varias tecnologías avanzadas que lo diferencian de los troyanos bancarios conocidos.

2. **DETALLES:**

La empresa rusa de ciberseguridad Kaspersky informó en un informe del jueves que Coyote utiliza el instalador Squirrel para su distribución, aprovechando Node.js y un lenguaje de programación multiplataforma relativamente nuevo llamado Nim como cargador para terminar su proceso de infección.

SQuirreL es un cliente SQL gráfico multiplataforma. Se trata de una aplicación implementada en Java, que te permite gestionar cualquier base de datos compatible con JDBC.

Coyote se distingue de otros troyanos bancarios similares por su uso del código abierto Squirrel framework para la instalación y actualización de aplicaciones en Windows. También rompe con la norma al sustituir Delphi, el lenguaje habitual entre el malware bancario, por lenguajes de programación menos populares como Nim, dirigido específicamente a Latinoamérica.



En el desglose de Kaspersky de la cadena de ataque, un ejecutable instalador de Squirrel sirve como plataforma de lanzamiento para una aplicación Node.js construida con Electron. Esto ejecuta un cargador basado en Nim que inicia la ejecución de la carga maliciosa Coyote a través de Carga lateral de DLL.

Una biblioteca maliciosa de vínculos dinámicos, etiquetada como «libcef.dll», se carga lateralmente utilizando un ejecutable legítimo llamado «obs-browser-page.exe», que también forma parte del proyecto Node.js. Es importante señalar que el libcef.dll original es un elemento del Chromium Embedded Framework (CEF).

Coyote, una vez ejecutado, "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", contactando posteriormente a un servidor controlado por el actor para obtener directivas de la siguiente etapa.

Coyote tiene la capacidad de llevar a cabo una gran variedad de comandos, incluyendo la toma de capturas de pantalla, registro de pulsaciones de teclas, terminación de procesos, mostrar falsas superposiciones, mover el cursor del ratón a un lugar determinado e incluso apagar el sistema. También puede bloquear el sistema con un engañoso mensaje «Trabajando en actualizaciones…» mientras realiza actividades dañinas en segundo plano.

"La incorporación de Nim como cargador añade complejidad al diseño del troyano", afirmó Kaspersky. "Esta evolución destaca la creciente sofisticación dentro del panorama de amenazas y muestra cómo los actores de amenazas se están adaptando y utilizando los últimos lenguajes y herramientas en sus campañas maliciosas".

IOCs de Referencia:

Basado en host (hash MD5):

- 03eacccb664d517772a33255dff96020
- 071b6efd6d3ace1ad23ee0d6d3eead76
- 276f14d432601003b6bf0caa8cd82fec
- 5134e6925ff1397fdda0f3b48afec87b
- bf9c9cc94056bcdae6e579e724e8dbbd

Lista de dominios C2:

- atendesolucao[.]com
- servicoasso[.]com
- dowfinanceiro[.]com
- centralsolucao[.]com
- traktinves[.]com
- diadaacaodegraca[.]com
- segurancasys[.]com

3. RECOMENDACIONES:

- Descargar e instalar únicamente aplicaciones de software de fuentes conocidas y confiables
- Implementar potentes soluciones antivirus y antimalware para detectar y eliminar archivos ejecutables maliciosos.
- Capacitar a los usuarios sobre las mejores prácticas de ciberseguridad.

Fuente de Información:	• hxxps://thehackernews.com/2024/02/new-coyote-trojan-targets-61-brazilian.html • hxxps://hackarizona.org/es/el-troyano-coyote-lanza-un-ataque-con-nim-contra-61-bancos-brasilenos/ • hxxps://securelist.lat/coyote-multi-stage-banking-trojan/98404/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°036	Fecha: 10-02-2024
		Página: 6 de 8

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Detección de falso servicio del correo electrónico de Microsoft		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que actores de amenazas vienen realizando una campaña de Phishing, activando un falso servicio del correo electrónico de la compañía Microsoft (Outlook, Hotmail, etc.), con la finalidad de obtener las credenciales de acceso (correos y contraseñas) de los usuarios de la compañía tecnológica.

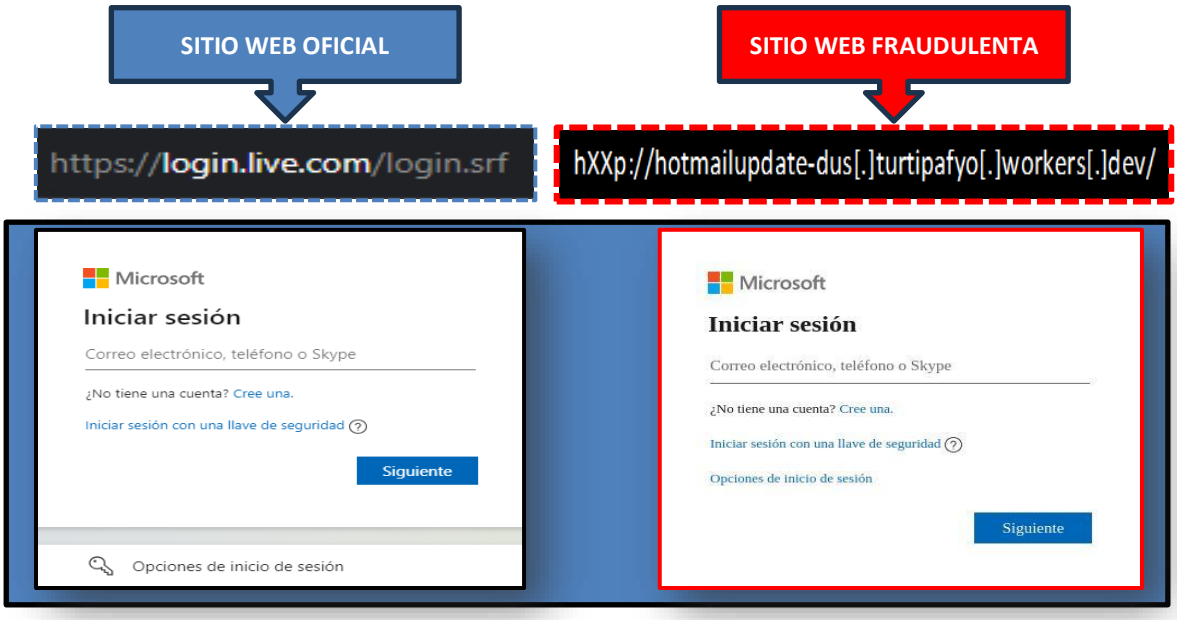
2. DETALLES:

El proceso del Phishing es el siguiente:

Solicita el correo electrónico de la víctima, para acceder al servicio en la web de la compañía Microsoft (Outlook, Hotmail, etc.)

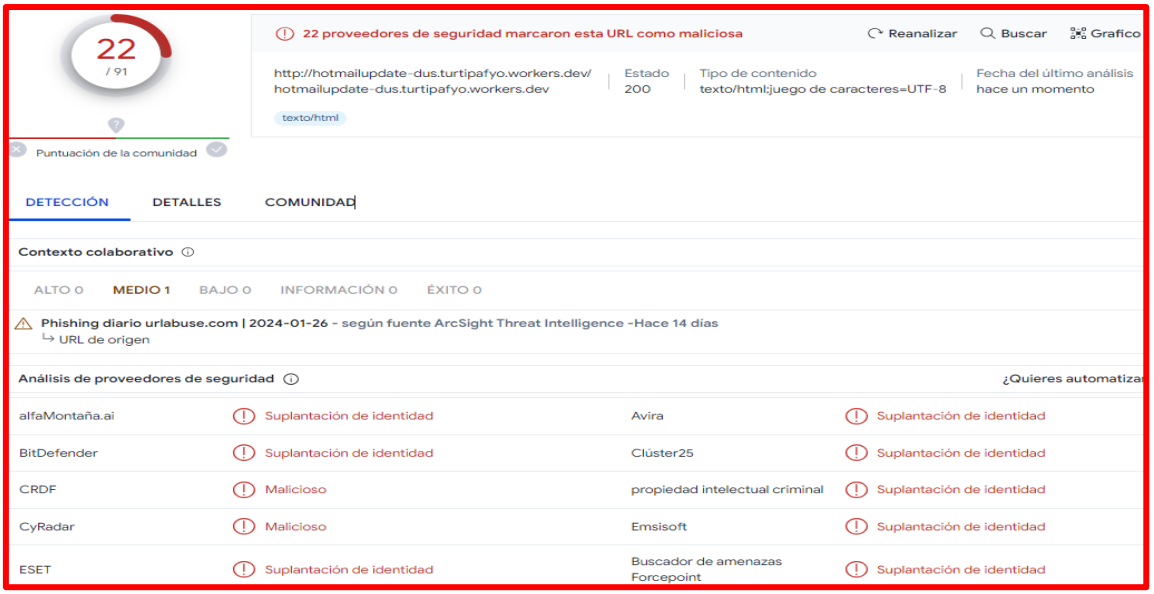
Requieren la contraseña de acceso para el servicio web de Microsoft, para luego dar clic en <Iniciar sesión>; sin embargo, después de unos segundos redirige al servicio del correo electrónico de la compañía Microsoft.

A. Comparación del sitio web oficial y fraudulento.



- Existe diferencias entre la URL original y la fraudulenta.
- La URL del sitio web fraudulento no el posee protocolo de seguridad de red (http)
- Existe una similitud entre ambas páginas en imagen, fondo y colores de ambos sitios web.

B. Proveedores de seguridad informática alertan como SUPLANTACIÓN DE IDENTIDAD - PHISHING.



C. Indicadores de compromiso (IoC)

- Dominio : workers[.]dev
- Servidor : Cloudflare
- SHA-256 : 21e33a95d1d2c06f77fd19b06e1e303e369eec4f7e1ff5a3ebaf1f4b64f3f603
- IP : 104[.]21[.]90[.]36

D. Apreciación de la información:

- La presente campaña de Phishing permite a los actores de amenazas obtener las credenciales de acceso del servicio del correo electrónico en la web de la compañía Microsoft (Outlook, Hotmail, etc.).
- La propagación del sitio web fraudulento se realiza mediante envió masivos de email, adjuntando enlaces de sitios web fraudulentos con la finalidad de obtener información sensible de las víctimas; asimismo, dicho enlace malicioso, es enviado a través de las plataformas digitales como el WhatsApp, Telegram, Messenger y mensajes de textos SMS.

3. RECOMENDACIONES:

- Verificar detalladamente las URL de los sitios web
- No abrir o descargar archivos sospechosos.
- No seguir las instrucciones de sitio web sospechoso.
- Mantener el antivirus actualizado.
- Descargar aplicaciones de fuentes confiables.
- Realizar las actualizaciones correspondientes desde fuentes originales.

Fuente de Información:	Análisis propio de redes sociales y fuente abierta.

Índice alfabético