SERVICIO DE INTELIGENCIA SOBRE AMENAZAS [SIA]

AÑO 2020

WWW.COREONEIT.COM
@COREONEIT

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

¿QUÉ ES EL SERVICIO DE INTELIGENCIA SOBRE AMENAZAS [SIA]?

Es una combinación de información de amenazas existentes en la red con el análisis e inteligencia del grupo de especialistas de CORE ONE IT, quienes analizan exhaustivamente todo tipo de amenazas informáticas y desarrollan una serie de recomendaciones adaptadas a cada tipo de cliente.

ALCANCE

Se personaliza de acuerdo al tipo de infraestructura y entorno de red del cliente basado en los tipos de dispositivos, modelos y fabricantes, con el fin de recibir solo información relevante y que pudiera afectar de manera directa o indirecta, la continuidad del negocio.

DEFINICIONES

•Riesgo: Probabilidad que una amenaza particular explote una vulnerabilidad particular de un sistema.

•Amenaza: Es la causa potencial de un incidente no deseado, el cual puede resultar en un daño a un sistema de información u organización.

•Ataque: Acción de tratar de traspasar controles de seguridad en un sistema. Un ataque puede ser activo, resultando en la modificación de datos, o pasivo, resultando en la divulgación de información. El hecho de que un ataque sea realizado no significa que será exitoso, el grado de éxito depende de la vulnerabilidad del sistema o actividad y de la eficiencia de las medidas existentes.

•Vulnerabilidad: Debilidad en los procedimientos de seguridad de un sistema, en el diseño del sistema, en la implementación, en los controles internos, y que puede ser explotada para violar la política de seguridad del sistema.

•API: Interfaz de Programación de Aplicaciones (Application Programming Interface, por sus siglas en inglés). Conjunto de subrutinas, funciones y procedimientos de una biblioteca para ser utilizado por otro software

•Malware: también llamado badware, código maligno, software malicioso, software dañino o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

•Ransomware: Es un tipo especial de malware que amenaza con destruir los documentos y otros archivos de las víctimas.

•Troyano: Software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo.

•ISP: Proveedor de servicios de Internet (Internet Service Provider, por sus siglas en inglés)

•Keylogger: Software de vigilancia, el cual cuenta con la capacidad de grabar cada tecla pulsada en el sistema en un archivo, usualmente cifrado.

•BSOD: Blue Screen Of Death, “pantalla azul de la muerte”; se refiere a la pantalla mostrada por el sistema operativo de Windows cuando éste no puede recuperarse de un error del sistema.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

REGUS, COMPAÑÍA DE COWORKING, SUFRE BRECHA DE DATOS MASIVA

Por increíble que parezca, los descuidos del factor humano siguen siendo la principal causa de incidentes relacionados con la seguridad y protección de datos de usuarios y empleados.

El más reciente error se presentó en la firma Regus, cuyo personal de ventas fue sometido a una investigación sobre rendimiento laboral. Este parecía un proceso convencional, hasta que la información personal recolectada durante este ejercicio fue ingresada en una hoja de cálculo y publicada en Trello, una plataforma de gestión de proyectos.

Para sorpresa del personal de recursos humanos de Regus, un periodista de Telegraph encontró la hoja de cálculo, la cual contenía nombres, direcciones y el resultado de la evaluación de los empleados de la compañía. La hoja de cálculo incluso contenía los datos de algunas de las personas que colaboraron en la investigación haciéndose pasar por clientes potenciales.

Por su parte, la compañía emitió un comunicado mencionando: "Los miembros de nuestro equipo están al tanto de que son monitoreados con fines de capacitación. Hemos recibido un reporte preocupante en referencia a un acceso externo a estos datos, incidente que derivó en la publicación de esta información en una plataforma pública", afirma el equipo de protección de datos de la compañía.

Regus notificó de inmediato al equipo de Trello, que removió el material expuesto de inmediato. No obstante, los problemas no terminarán aquí, pues el incidente deberá ser notificado a la Oficina de la Comisionada de Información (ICO) de Reino Unido, actualmente dirigida por Elizabeth Denham.

Finalmente, Applause, compañía contratada para llevar a cabo la evaluación del personal de Regus, emitió un comunicado mencionando: "Hemos realizado una auditoría interna para descartar la posible presencia de algún software de terceros operando sigilosamente en nuestras redes. Al no encontrar indicios de actividad maliciosa, concluimos que el incidente se produjo debido a un descuido".

A pesar de que la cantidad de información personal comprometida en este incidente no es realmente elevada, especialistas en protección de datos del Instituto Internacional de Seguridad Cibernética (IICS) señalan el preocupante número de incidentes de exposición de información provocados por simples descuidos del personal a cargo de la gestión de estas implementaciones. En los casos más serios, estos incidentes pueden llegar a filtrar información altamente sensible de cientos de miles, o incluso millones de usuarios de servicios y plataformas en línea.

FUENTES:

Notificas de Seguridad Informatica. (2020). Regus, compañía de coworking, sufre brecha de datos masiva. Enero, 21, de Seguridad Informatica Sitio web: https://noticiasseguridad.com/hacking-incidentes/regus-compania-de-coworking-sufre-brecha-de-datos-masiva/

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

GOOGLE, YAHOO, MICROSOFT, INTEL, IBM, SONY, HONDA, TOYOTA, ENTRE OTRAS, SUFREN POR VULNERABILIDADES CRÍTICAS EN OPENCV

Las fallas de seguridad en las tecnologías más usadas pueden traer consecuencias desastrosas para múltiples desarrolladores o compañías diferentes. Un equipo de análisis de vulnerabilidades de Cisco Talos ha reportado la presencia de dos fallas de desbordamiento de búfer en Open Source Computer Vision (OpenCV), una biblioteca de programación aplicada a la visión por computadora en tiempo real.

Este es un reporte de seriedad considerable, pues esta biblioteca es utilizada por algunas de las compañías tecnológicas más importantes del mundo, incluyendo Google, Microsoft, Intel, IBM, Toyota, Yahoo, entre otras, principalmente para proyectos relacionados con tecnología de reconocimiento facial, robótica, sensores de movimiento, entre otras aplicaciones.

La primera falla, identificada como CVE-2019-5063, fue hallada en la función de persistencia estructural de datos de OpenCV v4.1.0, explotable usando un archivo JSON especialmente diseñado para provocar un desbordamiento de búfer, lo que podría generar daños posteriores.

Acorde a los expertos en análisis de vulnerabilidades, cuando se analiza un archivo XML que contiene una referencia a una entidad de carácter potencial y encuentra el caracter "&", la API sigue extrayendo caracteres alfanuméricos hasta encontrar un punto y coma (;); si la cadena no coincide con ninguna de las cadenas en la instrucción de cambio, los datos se copian al búfer tal como son.

Este escenario permite a los actores de amenazas crear archivos XML especialmente diseñados para desencadenar el desbordamiento de búfer, acción que puede funcionar como vector de ataque inicial para llevar a cabo otras acciones maliciosas, como la ejecución de código en el sistema objetivo.

En cuanto a la segunda vulnerabilidad, identificada como CVE-2019-5064, también está presente en la característica de persistencia estructural de datos, y podría ser explotada empleando un archivo JSON especialmente diseñado.

Ambas vulnerabilidades ya han sido reportadas a los desarrolladores. Después de recibir el reporte, OpenCV mencionó que la versión 4.2.0, lanzada durante los últimos días de 2019, ya cuenta con las correcciones para estas dos fallas, por lo que se recomienda a los programadores que usan esta biblioteca actualizar a esta versión a la brevedad.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

Este nuevo año comenzó con múltiples compañías lanzando importantes actualizaciones de seguridad; apenas hace unos días, especialistas en análisis de vulnerabilidades del Instituto Internacional de Seguridad Cibernética (IICS) reportaron el lanzamiento de una actualización masiva en Oracle para corregir casi 400 fallas de seguridad halladas en más de 90 productos diferentes.

FUENTES:

Noticias de Seguridad Informatica. (2020). Google, Yahoo, Microsoft, Intel, IBM, Sony, Honda, Toyota, entre otras, sufren por vulnerabilidades críticas en OpenCV. Enero, 20, de noticiasseguridad Sitio web: https://noticiasseguridad.com/vulnerabilidades/google-yahoo-microsoft-intel-ibm-sony-honda-toyota-entre-otras-sufren-por-vulnerabilidades-criticas-en-opencv/

VULNERABILIDAD ZERO-DAY EN INTERNET EXPLORER ESTÁ SIENDO EXPLOTADA DE MANERA ACTIVA

El Centro de Respuesta de Seguridad de Microsoft publicó una advertencia de seguridad en la que informa acerca de la existencia de una vulnerabilidad zero-day en Internet Explorer que está siendo utilizada por cibercriminales de manera activa para llevar adelante ataques. El fallo, catalogado como CVE-2020-0674, aún no fue parcheado, pero la compañía aseguró que está trabajando en ello.

Según explicó en el comunicado, se trata de una vulnerabilidad que radica en la forma en que el motor de scripting maneja objetos en memoria dentro de Internet Explorar. En este sentido, un atacante podría corromper la memoria para ejecutar código de manera arbitraria.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

En caso de que un atacante logre explotar de manera exitosa el fallo obtendría los mismos permisos que el usuario en curso, por lo que, si el usuario inició sesión como administrador, el atacante también contará con esos permisos y podría llegara tomar control del sistema afectado para instalar programas, modificar o borrar información o incluso crear nuevas cuentas, explicó Microsoft.

Dicho esto, un cibercriminal podría crear un sitio especialmente diseñado para explotar la vulnerabilidad a través de este navegador y convencer al usuario de que visite el sitio, por ejemplo, a través de un correo electrónico, agrega el comunicado.

Todas las versiones de Windows son afectadas por esta zero-day. En algunos casos, el impacto del fallo es considerado moderado, mientras que en varias versiones de Windows 10 el fallo en Internet Explorer 11 es considerado crítico. Para más detalle de las versiones del navegador y del sistema operativo afectados consultar aquí. Cabe destacar que Windows 7, que desde hace unos días quedó sin soporte, también es afectado por el fallo.

La compañía reveló que está al tanto de la existencia de ataques que han estado intentando explotar este fallo, pero según publican algunos medios, no se sabe si Microsoft esperará al próximo mes para enviar el parche junto con el paquete mensual de actualizaciones o si hará una excepción.

Este mes también se reportó la existencia de otra vulnerabilidad zero-day que afectaba a un navegador como Firefox y que, según explicó Mozilla, también ha estado siendo utilizada por actores maliciosos para llevar adelante dirigidos. A diferencia del fallo en Explorer, la vulnerabilidad en Firefox ya fue parcheada en la última actualización disponible.

FUENTES:

Juan Manuel Harán. (2020). Vulnerabilidad zero-day en Internet Explorer está siendo explotada de manera activa. Enero, 20, de Eset Sitio web: https://www.welivesecurity.com/la-es/2020/01/20/vulnerabilidad-zero-day-internet-explorer-explotada-activa/

NETSKOPE ASEGURA LA NUBE DE LOS PROVEEDORES DE VIDEOJUEGOS

Netskope se adentra en el mundo de los videojuegos asegurando la nube de los proveedores. Prueba de ello es el acuerdo que acaba de alcanzar con el proveedor de software de juegos online, Microgaming, para que emplee la solución Netskope Security Cloud como eje central de su estrategia de seguridad informática de cinco años, diseñada para respaldar la migración de las principales aplicaciones de negocio hacia la nube.

Netskope Security Cloud proporciona visibilidad y protección de datos y frente a amenazas en tiempo real cuando se accede a servicios cloud, sitios web o aplicaciones privadas desde cualquier lugar y sin importar el dispositivo. Con la intención de migrar a la nube con Office 365, Microgaming seleccionó la solución CASB de Netskope junto con la solución de Web Proxy de nueva generación (NG-SWG) para mapear cada transacción web y cloud, lo que le ha permitido entender la actividad del usuario a través de todos los servicios SaaS e IaaS, y cualquier sitio web.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

Netskope también unifica la administración de políticas de Microgaming a través de la nube y el tráfico web desde una única plataforma cloud nativa.

Netskope Security Cloud proporciona visibilidad y protección de datos y frente a amenazas en tiempo real cuando se accede a servicios cloud.

A este respecto, la Gerente de Seguridad de Información de Microgaming, Samantha Hoffmann, comenta: «Era evidente que nuestros flujos de trabajo organizacionales mejorarían considerablemente con Office 365, sin embargo, no podíamos realizar ese movimiento mientras nuestra infraestructura de seguridad de web-proxy tradicional fuese incapaz de proporcionar una visión del tráfico cloud. Hemos logrado migrar a la nube porque Netskope Security Cloud nos ha proporcionado la visibilidad y el control total que necesitábamos».

Visibilidad y control de la información.

Efectivamente, Netskope proporciona a Microgaming controles en tiempo real entre los usuarios y la nube, la protección de la información confidencial y la capacidad para controlar el Shadow IT.

Netskope identificó inmediatamente 700 aplicaciones cloud no autorizadas que se estaban utilizando dentro de Microgaming y el Índice de Confianza en la Nube (CCI) de Netskope ha servido para proporcionar una evaluación continua de las credenciales de seguridad de cualquier aplicación en la nube. En lo que respecta específicamente a Office 365, Netskope proporciona visibilidad de los datos en reposo (en particular los datos que podrían compartirse), audita el tráfico de la herramienta de colaboración de equipos y permite la gestión del acceso a la nube empresarial desde dispositivos no gestionados.

Por su parte, Grant Reynolds, Director Regional de Ventas de Netskope, explica: «Microgaming seleccionó a Netskope después de una licitación pública, y ahora hemos completado una rápida y exitosa implementación. Actualmente seguimos colaborando; además de ayudar a Microgaming a mejorar las reglas de DLP utilizando su nueva infraestructura, nuestro equipo de Customer Success está trabajando con el grupo de seguridad informática de la empresa para respaldar sus planes en torno a la experiencia de los empleados, la gestión de recursos, el tiempo de actividad, el número de incidentes de seguridad y el buen funcionamiento del proceso de reparación».

FUENTES:

Manuel Navarro. (2020). Netskope asegura la nube de los proveedores de videojuegos. Enero, 21, de mkm publicaciones Sitio web: https://revistabyte.es/seguridad-informatica/netskope-security-cloud-videojuegos/

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

EL MALWARE LIBMINER SE APROVECHA DE LA MINERÍA DE CRIPTOMONEDAS BASADA EN CONTENEDORES

La compañía especializada en soluciones de seguridad y cumplimiento en la nube, Qualys ha identificado en un reciente análisis algunas instancias de dockers que ejecutan un malware denominado LibMiner.

LibMiner tiene la capacidad de implementar y ejecutar Cryptominer. Utiliza una técnica única para el movimiento lateral a través de los contenedores así como de los sistemas Linux, ejecutándose en servidores Redis desprotegidos e iniciando la extracción en ellos. El malware tiene la capacidad de proteger su terminación, lo que hace imposible obtener el control sobre el mismo.

LibMiner tiene la capacidad de implementar y ejecutar Cryptominer.

Hoy en día, parece que entrega de Cryptominers sigue siendo la fuente de ingresos favorita de los cibercriminales.

Los atacantes han cambiado su enfoque para apuntar a los contenedores docker mal configurados y desprotegidos e instalar este tipo de amenaza para conseguir el máximo beneficio. De cara al futuro, es muy probable que veamos ataques generalizados en este sentido.

FUENTES:

MNR. (2020). El malware LibMiner se aprovecha de la minería de criptomonedas basada en contenedores. Enero, 21, de revista byte Sitio web: https://revistabyte.es/seguridad-informatica/el-malware-libminer/

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

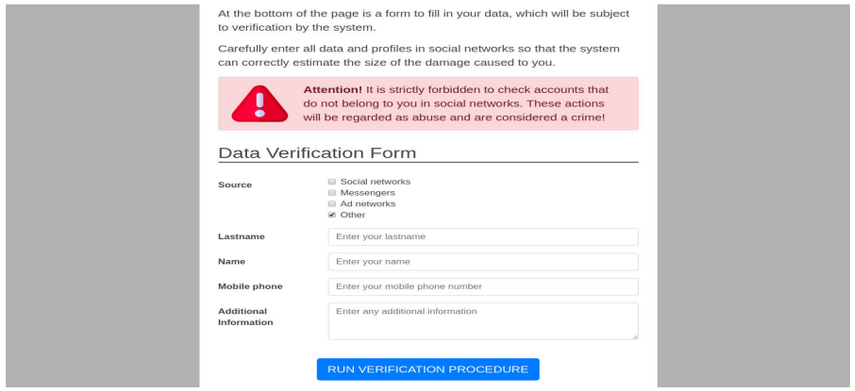
VÍCTIMAS DE BRECHAS DE DATOS SON HACKEADAS OTRA VEZ. NUEVO VECTOR DE ATAQUE

Un estudio elaborado por expertos en hacking ético de la firma Kaspersky detalla una nueva forma de engañar a miles de usuarios de Internet aprovechándose de las recientes noticias sobre brechas de datos y multas millonarias que las compañías responsables reciben de las autoridades de protección de la información.

Durante una reciente investigación sobre políticas de recolección de datos, los expertos encontraron un sitio web llamado Fondo de Protección de Datos Personales (por sus siglas en inglés, Personal Data Protection Found), presuntamente creado por la Comisión de Comercio de E.U.

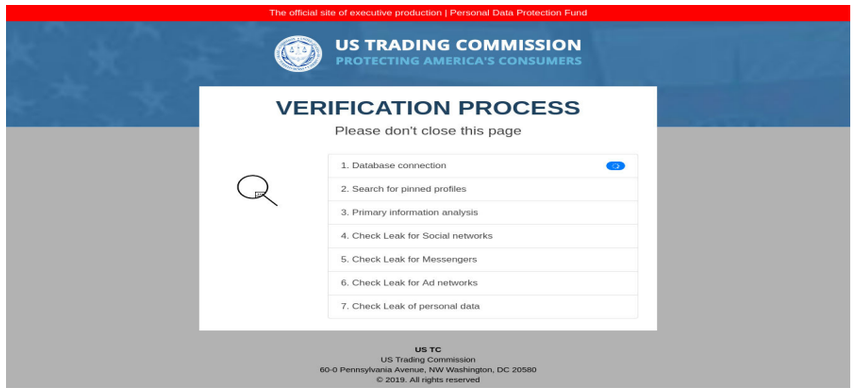
En el sitio web, de apariencia legítima, se afirma la existencia de un fondo para víctimas de brechas de datos de todo, supuestamente creado gracias a las multas que reciben las compañías. Además, se invita a los visitantes a registrarse para solicitar una compensación por estos incidentes.

Acorde a los expertos en hacking ético, el sitio también ofrece a los usuarios una función para verificar si su información personal se ha visto comprometida en algún incidente reciente. Para esto, los usuarios deben ingresar al sitio web su nombre completo, número de teléfono y nombre de usuario en algunas plataformas de redes sociales.



Como era de esperarse, esta es una nueva variante de estafa que trata de aprovecharse de los usuarios preocupados por la seguridad de sus datos en línea. Para corroborar esta suposición, los investigadores de Kaspersky ingresaron al sitio web los datos de un ciudadano llamado fghfgh fghfgh. Después ingresar estos datos falsos, el sitio web arrojó una respuesta sorpresiva: Los datos del inexistente ciudadano fghfgh fghfgh fueron "filtrados". No sólo eso, sino que el sitio web afirmó que, debido a que los archivos personales de la falsa víctima fueron expuestos, fghfgh fghfgh tenía derecho a recibir una compensación de 2 mil 500 dólares.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"



The report was prepared specifically for **fghfgh fghfgh (ID: 3480324)** automatically and verified by the executive officer **Jamie Raskin.**

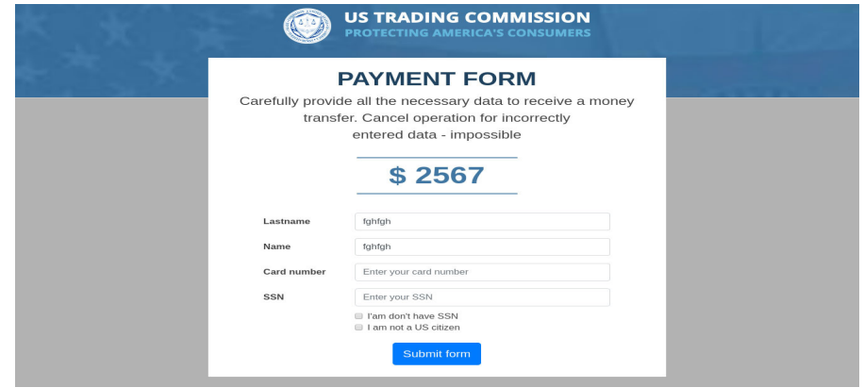
The audit showed that most of **your data repeatedly appeared in information leaks.** The largest percentage of data was transferred to third parties **between October and December 2018.** The main content of the data transfer was photo and video materials. The greatest damage is estimated from the **transfer of your contact information to numerous advertising companies.**

Below you can find a detailed scan report. **The amount of payment is final.**

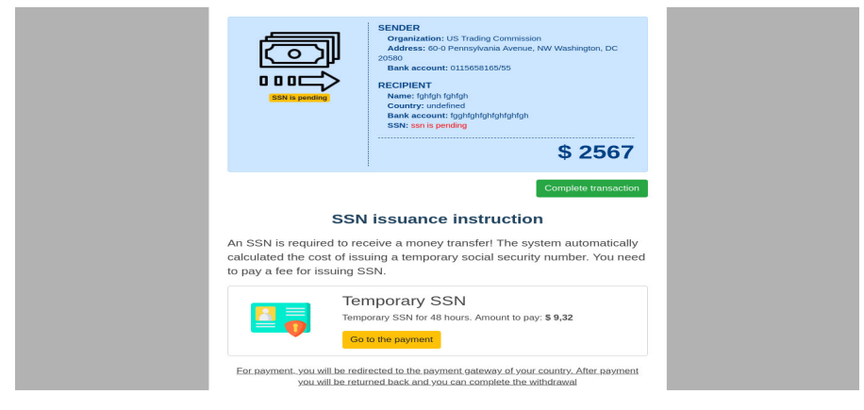
Source check	Status
Social networks	
use of personal information	not detected
the use of a photo\video materials	detected
using a phone number	not detected
Messengers	
use of personal information	not detected
the use of a photo\video materials	detected
using a phone number	not detected
Ad networks	
use of personal information	not detected
the use of a photo\video materials	detected
using a phone number	not detected
Additional check	
using your account contacts for promotional purposes	detected
	Total summ compensation
	$ 2567

Verification and certification of the calculation of compensation made by the employee

A diferencia de otras estafas en las que los criminales van directamente tras los datos de la tarjeta de crédito de la víctima, este sitio web menciona que la compensación no puede ser enviada a menos que la víctima ingrese su número de seguridad social, una clave de nueve dígitos emitida para cada ciudadano norteamericano y que se emplea para prácticamente cualquier trámite.

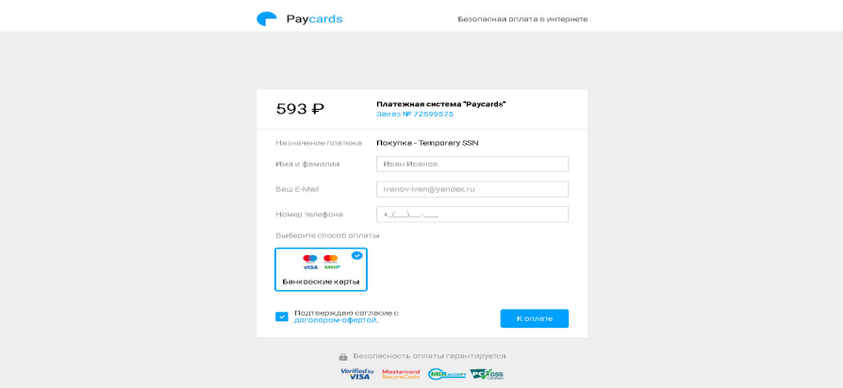


Los operadores de esta estafa contemplaron todos los posibles escenarios, pues incluso agregan al formulario una casilla con la opción "No tengo número de seguro social", mencionan los expertos en hacking ético. En este caso, el sitio web ofrece a los visitantes comprar un número de seguro social temporal por sólo 9 dólares.



SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

Si la víctima decide comprar un número de seguro social temporal, será redirigida a un formulario de pago. Si lo hace desde una dirección IP rusa, este formulario de pago aparece en ruso y el precio de compra se especifica en rublos. Esto es ridículo pues, ¿por qué una agencia del gobierno de EU solicitaría pagos en alguna divisa extranjera? La plataforma se dedica a la recolección de datos, además de robar cantidades mínimas, aunque se vuelven cifras considerables si se toma en cuenta el alcance potencial del sitio web.



Aunque esta estafa es obvia a los ojos de los usuarios familiarizados con el tema, miles de personas con pocos conocimientos están expuestas a los defraudadores. Como medida de prevención, los expertos en hacking ético del Instituto Internacional de Seguridad Cibernética (IICS) recomiendan ignorar cualquier ofrecimiento de dinero de esta clase. Consultar sitios legítimos, como Have I Been Pwned, también es una buena medida de seguridad para los usuarios preocupados por sus datos personales.

FUENTES:

Noticias de seguridad. (2020). Víctimas de brechas de datos son hackeadas otra vez. Nuevo vector de ataque. Enero, 20, de noticiasseguridad Sitio web: https://noticiasseguridad.com/seguridad-informatica/victimas-de-brechas-de-datos-son-hackeadas-otra-vez-nuevo-vector-de-ataque/