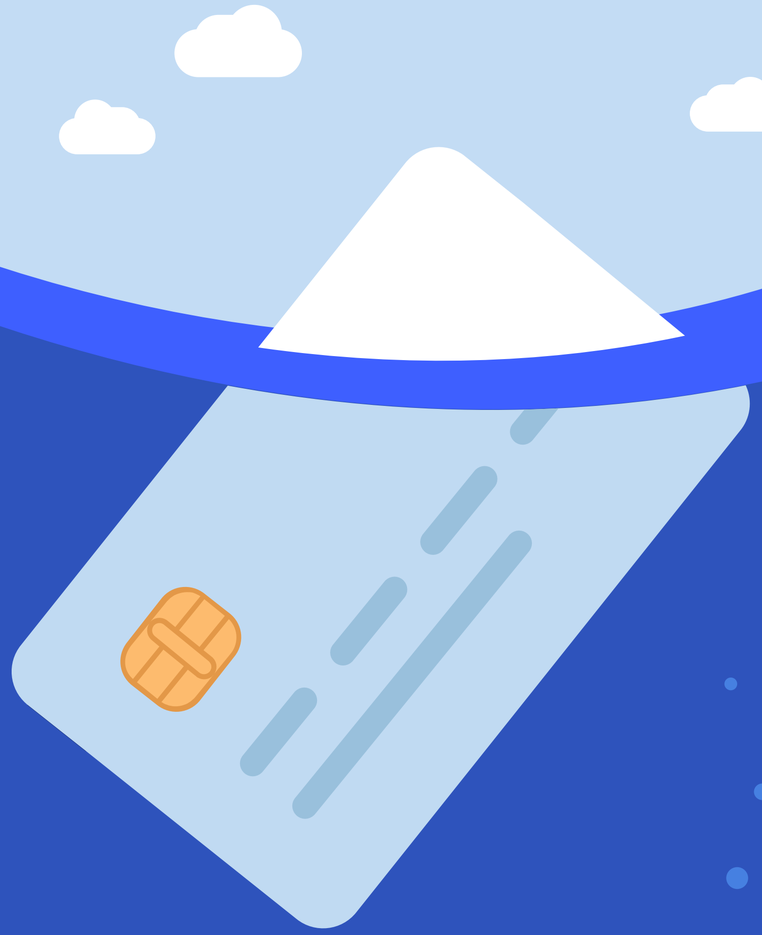
NordVPN®

La punta del iceberg: el análisis de 6 millones de tarjetas robadas



Introducción

Los sistemas digitales, como las tarjetas de pago, implican riesgos inherentes de seguridad y privacidad, pero nuestra vida cotidiana se basa en la ficción de que son totalmente fiables. ¿Cuáles son los riesgos reales de que le roben los datos de tu tarjeta? ¿Qué otra información está al alcance de los hackers? ¿Cómo podemos mitigar esos riesgos?

El robo de tarjetas es un problema global. El Informe Nilson 2020 mostró que provocó pérdidas por valor de 28 650 millones de dólares en todo el mundo, con más de un tercio de las pérdidas centradas en Estados Unidos. El sitio web Statista descubrió que casi el 7% de las ventas con tarjeta en EE.UU. eran fraudulentas, y predijo que las pérdidas mundiales totales alcanzarán alrededor de 32 960 millones de dólares en 2023.

La tecnología desempeña un papel fundamental en el fraude y el robo de tarjetas. Como mostramos en la investigación de NordVPN sobre ataques de fuerza bruta, los ordenadores pueden utilizarse para adivinar los detalles de las tarjetas. La información de pago puede filtrarse como resultado de vulneraciones de datos y hackeos de sistemas. Los delincuentes ni siquiera necesitan hacer ellos mismos el trabajo sucio: la web oscura alberga prósperos mercados de datos que proceden de las tarjetas robadas.

En este informe presentamos nuestra investigación sobre la venta de tarjetas de pago en la dark web. Nuestras conclusiones se basan en un conjunto de datos de casi 6 millones de tarjetas en ocho grandes mercados. Examinamos los antecedentes de cómo se robaron las tarjetas y otros datos personales, detallando los métodos de nuestro estudio. Analizamos la distribución de las tarjetas robadas por países, junto con los tipos de tarjetas disponibles y sus precios. También ampliamos la investigación existente examinando la conexión entre los datos de las tarjetas robadas y otros datos personales, intentando determinar cuántos datos de tarjetas son pirateados, filtrados o robados en lugar de utilizar métodos de fuerza bruta.

Por último, comparamos estos resultados con los datos disponibles sobre población y penetración de tarjetas para formar un índice de riesgo para distintos países. Utilizamos nuestros resultados para ofrecer recomendaciones a usuarios y empresas sobre cómo prevenir el robo de datos de tarjetas y otra información personal.

Puntos clave

En el momento de nuestra investigación, los mercados de la dark web tenían los datos de 6 millones de tarjetas de pago robadas, de las cuales 2,5 millones estaban a la venta por más de 18,5 millones de dólares en total. Si se compran, estos datos de tarjetas de pago pueden reportar a los delincuentes mucho más de lo que pagaron originalmente por ellos.

Las tarjetas estadounidenses son el principal objetivo: más de la mitad de las tarjetas de pago descubiertas procedían de Estados Unidos.

Los rusos fueron los menos propensos a encontrar sus datos en los mercados de la dark web analizados.

Más del 60% de las tarjetas se vendieron junto con otros datos personales de la víctima, como su dirección, número de teléfono, dirección de correo electrónico, fecha de nacimiento o número de la Seguridad Social.

Las tarjetas se venden por una media de 7 dólares, pero muchas se filtran gratuitamente.

Antecedentes y contexto

El fraude con tarjetas suele dejar indefensa a la víctima, en gran parte porque es casi imposible saber cómo le han robado los datos de su tarjeta. Incluso los profesionales de la seguridad corren peligro. Pero estos ataques de fuerza bruta (adivinar los datos, confirmarlos en sitios web con menos controles de seguridad y luego explotarlos o venderlos en la dark web, como se detalla en nuestra investigación anterior) son solo una forma de obtener los datos de las tarjetas de pago. Los métodos más directos de pirateo y robo pueden hacer que las víctimas se sientan aún más vulnerables y se apoderen de algo más que los datos de las tarjetas.

El robo de identidad se ha descrito como "el delito por excelencia de la era de la información". Si una filtración de datos o un pirateo informático expone no solo los datos de tu tarjeta, sino también tu dirección y otra información personal, puede dar lugar a más casos de usurpación de identidad. Cualquiera puede ser víctima de un robo de identidad, y puede llevar años deshacer el daño. Una vez que el atacante ha obtenido el nombre, la dirección postal y la dirección de correo electrónico de la víctima, puede incluso abusar de métodos legales (como utilizar el derecho de acceso del GDPR para obtener más información personal) para llevar adelante el plan de robo de identidad o cometer otras actividades maliciosas.

Además, mientras que el fraude con tarjetas de crédito tiende a afectar a las personas más adineradas (lo que hace que en la cultura popular se presente como un "delito sin víctimas" porque las víctimas son privilegiadas y las compañías de tarjetas de crédito suelen reembolsar los cargos fraudulentos), otras formas de usurpación de identidad, como el robo de cuentas bancarias, suelen afectar a los más desfavorecidos.

En este estudio, nos centramos en los casos en los que los datos de la tarjeta se venden en la red oscura junto con otra información personal. Esto sube la apuesta, proporcionando un valor adicional (uso de la información para el fraude de identidad), pero también causa un daño adicional a la víctima (más información expuesta y mayor riesgo de robo de identidad). Estos paquetes de información proceden de brechas de ciberseguridad (hackeos, filtraciones, robos) que podrían evitarse con medidas de protección adecuadas. Pero para protegernos, primero debemos entender cómo pueden robarse los datos de las tarjetas y otra información.

Tarjetas de crédito y robo de datos

Hemos dividido los diferentes métodos de robo en una serie de categorías según el tipo de ataque utilizado:

- **Métodos tradicionales**
  - Físico
  - Social
- **Métodos de hackeo**
  - Dispositivos
  - Sistemas

Hemos dividido aún más estas categorías por escala:

- **Pequeña escala:** Tendencias para operar individualmente.
- **Escala mediana:** Menos específica, puede ser a largo plazo con el potencial de escalar.
- **Gran escala:** Se puede automatizar fácilmente o afectar a un gran número de personas a la vez.

Por supuesto, estos métodos de robo pueden superponerse y a menudo lo hacen. Un método puede incluso llevar a otro — por ejemplo, una brecha de datos que filtran direcciones de correo electrónico puede conducir a un intento de suplantación de identidad a gran escala. El phishing en sí mismo abarca tanto los intentos sociales como los métodos digitales automatizados.

	Tradicional		Hackeo	
	Físico	**Social**	**Dispositivos**	**Online**
Pequeña escala	Perdida o robo de tarjeta Dumpster diving	Shoulder surfing/ copiado Fraude familiar o "amistoso"	RFID Wifi pública	Hacking de cuenta bancaria online
Escala mediana	Skimmer de tarjetas	Llamadas telefónicas fraudulentas	POS malware	
Gran escala		Phishing	Malware en dispositivos	Fuerza bruta Robo de formularios Robo de datos

Examinaremos cada uno de estos métodos para robar datos de tarjetas.

La pérdida o robo de tarjeta es quizás el método más simple utilizado, implicando la pérdida física de la propia tarjeta. Las víctimas tienden a ser alertadas de este método antes que los demás de esta lista.

Dumpster diving ha sido descrito como "tecnología sin hacking." Puede consistir en la búsqueda de datos personales, extractos bancarios o tarjetas de crédito antiguas en la basura doméstica, o en el asalto a las instalaciones de eliminación de residuos de las empresas en busca de documentos confidenciales que contengan grandes conjuntos de datos de clientes. Puede implicar ingeniería social, como cuando conduce al robo de identidad o cuando se utilizan métodos de comportamiento para obtener acceso no autorizado a residuos confidenciales.

Shoulder surfing o copiado es otra forma de no hacking tecnológico. Consiste en mirar por encima del hombro de alguien en el tren o en una cafetería concurrida para observar su contraseña, número de tarjeta u otra información. También incluye a los empleados de ventas que copian los datos de la tarjeta mientras cobran. ste método de robo de datos es de muy baja tecnología, pero es popular y eficaz para los delincuentes a pequeña escala.

Familia o fraude "amigable" a menudo ocurre cuando aquellos que están cerca de nosotros abusan del acceso a nuestra información personal y tarjetas físicas, pero fraude "amigable" también puede ser cometido por consumidores deshonestos — por ejemplo, al realizar compras que se cobran más tarde a través de la tarjeta de crédito del consumidor. Esta práctica acaba costando el dinero del vendedor, lo que puede ser particularmente perjudicial para las pequeñas empresas en línea.

El skimming de tarjetas involucra a criminales añadiendo un dispositivo adicional a un cajero automático para copiar los datos de la tarjeta de la víctima. A pesar de haber estado ahí durante décadas, los dispositivos de skimming de tarjetas son fáciles de perder si estás ocupado o no los estás buscando activamente. Diferentes tipos de skimmers de cartas tienen niveles diferentes de oculción, y algunos son bastante sofisticados al alterar el cajero automático.

Las **llamadas telefónicas fraudulentas** son uno de los ejemplos anteriores de ingeniería social. En este tipo de llamadas, el estafador se hace pasar por su banco u otra organización de confianza para engañarle y conseguir que revele información sensible. Los gobiernos publican a menudo consejos y una lista con las formas de denunciar las llamadas telefónicas fraudulentas.

Phishing es un método conocido de ataque, mezclando contras más tradicionales con técnicas digitales (como correos basura o sitios falsos) para engañar a las víctimas a fin de que comuniquen sus datos de acceso, información de cuenta o número de tarjeta. El phishing manipula la vulnerabilidad cognitiva activa que juegan con nuestras expectativas. Hay pasos que puedes tomar si te convertes en víctima, pero es mejor actuar rápidamente.

RFID implica hackear un pago realizado con una tarjeta física en una proximidad cercana. Un pago sin contacto puede ser copiado y repetido para hacer pagos en otros países. Los bancos han dado pasos para frenar los ataques RFID.

Wifi pública plantea graves problemas de seguridad, especialmente cuando se trabaja junto a dispositivos desconocidos y posiblemente maliciosos. El público parece ser consciente de al menos algunos de estos riesgos, en los que los usuarios retornan a diferentes patrones de comportamiento para la protección. Por ejemplo, mucha gente tiende a evitar la banca en línea cuando está en una Wifi pública — pero todavía siguen en otros sitios (como plataformas de redes sociales) que podrían filtrar información importante y resultar en fraude de identidad o crédito.

El hacking de cuentas bancarias online tiende a afectar a aquellos en grupos ya marginados. Los crecientes vínculos entre bancos y empresas emergentes de tecnología fintech crean riesgos adicionales en ciberseguridad. Las instituciones pueden promover medidas de protección en forma de riesgo percibido, interfaces promocionadoras de seguridad, confianza institucional. y tranquilizaciones (como las garantías de devolución del dinero), aunque no necesariamente mitigan el impacto potencial más largo y los efectos del robo de identidad.

Malware POS involucra infectar dispositivos punto de venta (POS) en tiendas con virus que envían datos de tarjetas a hackers. Estos ataques van desde apuntar a tiendas específicas hasta hacks a gran escala cuando se ponen en peligro suficientes dispositivos POS en una tienda grande. Por ejemplo, en 2013 la cadena de distribución Target fue víctima de este tipo de ataque. La amenaza del malware es especialmente prominente ahora que las tiendas están avanzando hacia POS basados en tabletas y teléfonos, con los criminales que continúan mejorando los métodos para evitar la detección.

El malware en dispositivos es un problema común con una gran "economía sumergida" de malware como servicio. El malware presente en el dispositivo puede extraer datos directamente, husmear en otras apps (actuando como un "fantasma en el navegador") o comprometer la seguridad del dispositivo personal o de la empresa para enviar datos a los delincuentes.

La **fuerza bruta** fue explorada en detalle en un estudio anterior de NordVPN. Un ataque de fuerza bruta implica probar varias combinaciones para adivinar los detalles de la carta. Estos ataques se hacen más fáciles por el hecho de que las tarjetas de determinados países, los emisores de tarjetas y los bancos siguen ciertos patrones. Las suposiciones pueden ser comprobadas rápidamente en masa en sitios con laxa seguridad de pago.

El **secuestro de formularios** es una forma recientemente descubierta de ataque basada en web que utiliza JavaScript malicioso y otras técnicas para tomar el control de los formularios en línea y filtrar los datos a hackers. El secuestro de formularios es difícil de detectar y puede explotar una amplia gama de otras vulnerabilidades en sitios web y navegadores. Se hace más común en el período previo al periodo de vacaciones de invierno a medida que aumenta la compra online.

Las v**ulneraciones de datos** son un gran riesgo de reputación para las empresas y un riesgo real para sus clientes. El informe PwC de 2015 al gobierno del Reino Unido descubrió que no solo aumentó el número de incidentes en comparación con el año anterior, sino que también su escala y costo se duplicaron, hasta el punto de que para las grandes empresas se las debería considerar una "certeza cercana". Si bien algunas infracciones de alto perfil sí hacen que las noticias, la situación a menudo está mal representada y sin contexto. Los usuarios a menudo terminan incorrectamente culpando a sus propios hábitos en lugar de a la organización o hackers incumplidos. y a menudo subestiman los efectos potenciales para ellos personalmente, incluso cuando conocen los riesgos generales. Las herramientas fáciles de usar son esenciales cuando se trata de concienciar al público y actuar después de una infracción. Por ejemplo, las notificaciones de vuleración de contraseña pueden evitar ataques de autocompletado de credenciales, limitar los efectos del robo de identidad que resulta de las filtraciones de información personal.

La tabla anterior intenta poner cada tipo de ataque discutido en su categoría apropiada. Este estudio se centrará en los tipos destacados porque implican técnicas de hacking digital más directas y puede (hasta cierto punto) ser mitigado usando el comportamiento y herramientas adecuadas.

Es importante destacar que todos los tipos de ataques anteriores pueden conducir al robo de tarjetas de pago, así como a casos más amplios de fraude de identidad. Cuando se filtra más información junto con los detalles de la tarjeta, es más fácil para los piratas informáticos (y para los que venden los datos) causar más daño a largo plazo a sus víctimas.

Métodos

Para estudiar el alcance del robo de tarjetas en línea, hemos trabajado con un conjunto de detalles de millones de tarjetas para la venta en la dark web.
En particular, examinamos las tarjetas que vinieron empaquetadas con otra información personal para determinar cuántas fueron robadas o hackeadas en lugar de simplemente brutas forzadas.

Recopilación de datos

Los datos fueron compilados en colaboración con investigadores independientes especializados en investigación de incidentes de ciberseguridad. Evaluaron ocho mercados clave en la dark web para recuperar los detalles de más de 6 millones de tarjetas, incluyendo los detalles del tipo de tarjeta (crédito o débito) y otros datos personales vinculados. Los datos recibidos por NordVPN de estos investigadores de terceros no contenían ninguna información relacionada con un individuo identificable (como nombres, información de contacto u otra información personal). El estudio no determinó el número exacto ni analizó la totalidad de los datos de las tarjetas de pago vendidos en toda la dark web — NordVPN solo examinó el conjunto de datos estadísticos proporcionados por investigadores independientes.

Limpieza de datos

Dada la naturaleza de los mercados web oscuros, no todos los vendedores de web oscuros podrían ser instalados en categorías de datos o etiquetas estándar. Para crear un conjunto de datos consistente, excluimos las entradas con datos incompletos o incompatibles. Estos registros excluidos representan menos de 1,5 % del total fijado — alrededor de 3500 fueron excluidos debido a errores en la carga de los datos y otros 8.000 debido a un etiquetado inadecuado. Esto nos dejó con un conjunto de datos de 5,953,651 tarjetas.

Hemos ordenado los datos por país donde se emitió la tarjeta. Esto dio lugar en un principio a más de 200 categorías, que hemos reducido centrándonos en los países que tenían más de 1000 tarjetas en su conjunto de datos. Esto se debió a que un gran número de países sólo tenían un puñado de tarjetas que sesgaban los datos a la hora de realizar comparaciones internacionales. Esto nos dejó con 98 países para la comparación, una lista que generalmente refleja a las poblaciones de los países. Los datos de los países restantes se doblaron en la categoría de “ningún/otro país” para mantenerlos presentes en el conjunto.

Extracción de datos

De nuestro conjunto de datos, extraemos la siguiente información, separada por países:

- **Cuenta**
- **Precio medio**
- **Tarjeta**
  - Tipo: crédito, débito, otro
  - Compañía: Visa, Mastercard, Amex, otra
- **Información adicional**
  - Domicilio
  - Número de la Seguridad Social
  - DoB
  - Número de teléfono
  - Dirección de email

Luego calculamos el porcentaje de las tarjetas que se obtuvieron por medio de piratería, robo o violaciones de datos. Esto se basó en el número que contiene una o más piezas de información (dirección de casa, SSN, DoB, número de teléfono o dirección de correo electrónico). El resto puede haber sido bruto forzado, ya que sólo contienen los datos de la tarjeta. Sin embargo, el porcentaje de tarjetas hackeadas es una estimación conservadora — es probable que al menos algunos detalles de la tarjeta clasificados como “fuerza bruta” también fueran resultado de robo o incumplimiento. Mientras tanto, el porcentaje de tarjetas brutas forzadas representa el máximo número posible de instancias de fuerza bruta (es muy poco práctico forzar bruta otras piezas de información además de los detalles de la tarjeta).

Comparamos los datos de la tarjeta estadística entre países con estadísticas de población de las Naciones Unidas y el número de tarjetas en circulación por país o región de Visa, Mastercard y American Express. Usando la información de abajo, creamos un índice de riesgo para comparar las posibilidades de que ciudadanos de diferentes países encuentren sus datos de tarjeta en la dark web:

Número de tarjetas en el conjunto de datos (N)
Población (P)
Número de tarjetas en circulación por persona (C)
El porcentaje de tarjetas robadas por hacking (H)

La variable final se añadió para explicar el riesgo adicional de que ciertos países fueran mayores objetivos para los piratas informáticos. Los ataques brutos de las fuerzas pueden afectar potencialmente a todos los países, mientras que las violaciones graves y los hacks tienden a centrarse en negocios específicos. ubicaciones, u otras entidades vinculadas a países específicos. El índice de riesgo se calculó utilizando la siguiente fórmula:

$$RI = \frac{N}{P * C} * H$$

Con estos tipos de datos, pudimos analizar los patrones y diferencias de los países.

Resultados

Nuestro estudio demuestra que se está robando un gran número de datos de tarjetas junto con otros datos personales sensibles, lo que supone un riesgo significativo de fraude de identidad. Los detalles de millones de tarjetas se filtran de forma gratuita en los oscuros mercados de la web. El precio promedio de las tarjetas de 2,5 millones disponibles para la venta fue de $7,01, con el conjunto estudiado de datos de detalles robados por $18,5 millones.

La tabla al final de esta sección muestra los primeros 20 países por las siguientes mediciones clave: número de tarjetas, precio medio, y porcentaje de tarjetas con información adicional (requisito mínimo para tarjetas hackeadas) así como los índices de riesgo más altos y más bajos.

Tarjetas

De nuestro conjunto de datos que contenía casi 6 millones de tarjetas, más de la mitad procedían de los Estados Unidos (3.461.444 tarjetas, o 58,1%). Esto tiene sentido, considerando que Estados Unidos tiene una mayor tasa de penetración de cartas, una población considerable y una economía fuerte. Luego fueron India (3,7%), el Reino Unido (2,8%) y México (2. %), seguido por Brasil, China, Francia e Italia — una mezcla de países con poblaciones altas y economías fuertes o reputación política.

De los 2,5 millones de tarjetas vendidas en los mercados web oscuros, las tarjetas de Dinamarca ordenaban el precio medio más alto a 11,54 dólares por tarjeta. A esto le siguieron tarjetas de Japón, Portugal y Ucrania, por término medio, más de 11 dólares.

Curiosamente, las tarjetas de Estados Unidos eran comparativamente más baratas: 6,86 dólares, cayeron justo por debajo del costo promedio total de 7,01 dólares. Las tarjetas de Argentina y Nueva Zelanda eran las más baratas, con un promedio de menos de 2,50 dólares. Teniendo en cuenta la cantidad de daños que se pueden causar con los datos de la tarjeta robada y cualquier información personal incorporada, se trata de una cantidad sorprendentemente pequeña, sugerir que el uso de tarjetas robadas podría ser relativamente escalable incluso por aquellos que han obtenido los detalles de segunda mano de la dark web.

Información adicional

Más de la mitad (51,5%) de las tarjetas venían con direcciones, mientras que un número significativo venía con números de teléfono (39,8%) y direcciones de correo electrónico (28,7%). Las tarjetas de mayor tamaño vienen con una fecha de nacimiento (2,5%) o un número de Seguro Social (1,8 %) — sin embargo, esta información adicional expondría a la víctima a un riesgo significativamente mayor de fraude de identidad.

En total, el 62,8% (casi dos tercios) de las tarjetas venían con alguna forma de información adicional, indicando hacking, mientras que hasta 37,2% fueron adivinados a través de ataques de fuerza bruta (recuerde, este es un límite superior para ataques de fuerza bruta y un límite inferior para los hacks). Esto significa que la mayoría de los detalles de la tarjeta robada fueron obtenidos por uno de los métodos de hacking que se discutieron anteriormente.

Los números varían según el país. Cabe destacar que los registros sin información válida sobre el país siguieron una tendencia inversa, ya que casi todas las entradas solo contenían datos de la tarjeta (92,4%). En general, los países con más tarjetas en el conjunto de datos tenían tasas más altas de tarjetas con información adicional, con la excepción de China (que posiblemente se saltó la tendencia debido a la falta de integración con los sistemas de información globales y a la naturaleza cerrada de Internet, las plataformas de compra online y las plataformas bancarias chinas).

Casi el 90 por ciento de las tarjetas de la India tenían datos adicionales, exponiendo a las víctimas indias a cuestiones más amplias de fraude de identidad. Por lo general, los países europeos y los países más desarrollados económicamente tenían tasas más altas de información adicional. mostrando una correlación suelta entre el valor percibido de la víctima y los intentos de hacking.

Índice de riesgo

Usando el cálculo descrito anteriormente, creamos un índice de riesgo para 98 países. Nuestro índice tiene en cuenta la probabilidad de que una de sus tarjetas esté en la web oscura así como los riesgos adicionales que plantea su venta con información adicional.

Los países con el índice de riesgo más alto (y por lo tanto el mayor riesgo) fueron Malta, Australia y Nueva Zelanda. Esto se debe potencialmente a su asociación con la UE o la anglosfera, al tiempo que tienen poblaciones más pequeñas en comparación con su peso financiero y político. Estados Unidos ocupaba el puesto 5, mientras que Singapur y Hong Kong ocupaban el puesto noveno y décimo respectivamente.

En el otro extremo del espectro, Rusia tenía la menor puntuación de riesgo y China era la tercera de la última. Esto coincide con las hipótesis predominantes en cuanto a la ubicación de operaciones de piratería informática a gran escala y al objetivo de los países angloeuropeos. Otros países más bajos en el índice de riesgo tendieron a tener economías más pequeñas (con la excepción de Alemania, que era el 15 del pasado).

El índice de riesgo no necesariamente se correlaciona con el número de tarjetas en el conjunto de datos, mostrar la importancia de tener en cuenta el tamaño de la población, la penetración de tarjetas y otros factores para evaluar el riesgo. También está el caso de Alemania. que a pesar de una economía fuerte y una población considerable para un país europeo, tenía una calificación de riesgo muy baja. Esto puede deberse a factores políticos y de comportamiento, tales como una mayor atención a las regulaciones así como mayores medidas de seguridad y privacidad implementadas para individuos y organizaciones.

Top 20 países por diferentes categorías de datos

País	Tarjetas	%
EEUU	3461444	58,1
India	218053	3,7
Reino Unido	164143	2,8
México	156613	2,6
Brasil	144297	2,4
China	114765	1,9
Canadá	97552	1,6
Francia	97032	1,6
Italia	78676	1,3
Australia	65350	1,1
España	60173	1
Sudáfrica	46737	0,8
Turquía	41803	0,7
Chile	30079	0,5
Alemania	26558	0,4
Malasia	22504	0,4
Argentina	16792	0,3
Perú	13968	0,2
Dinamarca	12468	0,2
Noruega	12055	0,2

País	Precio medio
Dinamarca	$11,54
Japón	$11,07
Portugal	$11,07
Ucrania	$11,02
Eslovenia	$10,83
Vietnam	$10,74
Eslovaquia	$10,64
Chile	$10,55
Arabia Saudí	$10,55
Tailandia	$10,27
Singapur	$10,20
Filipinas	$10,00
Mauritania	$9,98
Hungría	$9,71
Francia	$9,42
Uganda	$9,04
Camerún	$8,98
Italia	$8,90
Rusia	$8,62
Brasil	$8,47

País	% hackeado
India	89,8
Eslovaquia	86,3
Arabia Saudí	82,8
Portugal	82
Ucrania	82
Chile	81,4
Hungría	79,2
Japón	78,9
Eslovenia	77,2
EEUU	76,8
Islandia	76,3
Francia	74,9
Bahrain	74,6
Dinamarca	74,1
Italia	73,3
Rusia	73,2
Iraq	72,9
Grecia	72,2
Suiza	72,1
Reino Unido	71,9

País	Índice de riesgo
Malta	1
Australia	0,91
Nueva Zelanda	0,84
Eslovenia	0,82
EEUU	0,79
Bahrain	0,79
Bahamas	0,78
Emiratos Árabes Unidos	0,78
Singapur	0,77
Hong Kong	0,77
Namibia	0,77
Qatar	0,74
Botswana	0,73
Chile	0,72
Puerto Rico	0,72
Suazilandia	0,72
Islandia	0,71
Turquía	0,71
Omán	0,71
Hungría	0,68

País	RI (más bajo)
Rusia	0
Pakistán	0,01
China	0,04
Bangladés	0,06
Venezuela	0,09
Ucrania	0,16
Indonesia	0,16
Egipto	0,18
Benín	0,18
Zimbabue	0,2
Paraguay	0,21
Iraq	0,26
Vietnam	0,26
Nigeria	0,27
Alemania	0,28
Marruecos	0,3
Colombia	0,31
Polonia	0,31
Mozambique	0,31
Túnez	0,32

Recomendaciones

Las empresas bancarias pueden reducir los riesgos a través de medios tecnológicos. pero esto los deja para lidiar con monitoreo invasivo y costoso de clientes y transacciones potencialmente fraudulentas. De la misma manera, los bancos y las tiendas en línea simplemente no pueden controlar las cuestiones más amplias asociadas con el robo de identidad y las vulneraciones de datos. A menudo depende del usuario protegerse contra estos riesgos incorporando herramientas de seguridad y privacidad online en la vida diaria.

Recomendamos leer nuestra guía sobre cómo protegerse contra el robo de identidad o probar estos pasos específicos y usar herramientas NordVPN contra amenazas específicas:

VPN para la banca electrónica

- Protege el tráfico de tu red, especialmente en la Wifi pública, para mantener tu información personal y financiera segura.

Protección contra amenazas

- Escanea en busca de malware durante las descargas para eliminar amenazas potenciales tanto de dispositivos POS personales como empresariales.
- Bloquea sitios web maliciosos que podrían filtrar tus datos o anuncios maliciosos que podrían intentar el secuestro de formularios.
- Combinada con VPN y otras herramientas de ciberseguridad, la Protección contra amenazas activada puede ayudar a protegerse de los intentos de phishing de los hackers para que las víctimas revelen información privada.

Dark web monitor

- Recibe alertas si tus credenciales aparecen en la web oscura tras un ataque de fuerza bruta o una vulneración de datos, lo que te avisa y evita que los delincuentes se adelanten.

NordPass

- Utiliza contraseñas únicas y complejas para proteger tus cuentas bancarias online y otras cuentas contra ataques de fuerza bruta y otros métodos de pirateo.

NordLayer

- Reduce el riesgo de infracciones para tu empresa y protege tus datos (y los de tus clientes) con una protección de red escalable y de varias capas, especialmente si tiene trabajadores remotos.

Debido a que existen diferentes formas de robar, piratería informática o filtración de datos de tarjetas o datos personales, es mejor adoptar un enfoque múltiple de la seguridad. Combina estas herramientas para reducir el riesgo general de que sus datos sean vendidos en la dark web y las consecuencias a largo plazo del robo de crédito e identidad.

Referencias

Benjamin, G. 2023. Mistrust Issues: How technology discourses quantify, extract and legitimise inequalities. Bristol: Bristol University Press.

Caballero, J., Grier, C., Kreibich, C. y Paxson, V. 2011. Measuring Pay-per-Install: The Commoditization of Malware Distribution. USENIX Security 11: 1-16.

Chothia, T., Garcia, F.D., de Ruiter, J., van den Breekel, J., Thompson, M. 2015. Relay Cost Bounding for Contactless EMV Payments. Financial Cryptography and Data Security: 1-18.

Copes, H., Kerley, K.R., Huff, R. y Kane, J. 2010. Differentiating identity theft: An exploratory study of victims using a national victimization survey. Journal of Criminal Justice 38(5): 1045-1052.

Crail, C. 2022. How to Spot a Credit Card Skimmer. Forbes.

Dharmavaram, V.G. 2021. Formjacking attack: Are we safe? Journal of Financial Crime 28(2).

Di Martino, M., Robyns, P., Weyts, W., Quax, P., Lamotte, W. y Andries, K. 2019. Personal Information Leakage by Abusing the GDPR "Right of Access". Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019): 371-385.

Gibbs, S. 2022. Scammers guessed my credit card number – and they could guess yours too. The Guardian.

Jarvis, K. y Milletary, J. 2014. Inside a Targeted Point-of-Sale Data Breach. Dell SecureWorks Counter Threat Unit™ Threat Intelligence 773.

Kahn, C. M. and Roberds, W. 2008. Credit and identity theft. Journal of Monetary Economics 55(2): 251-264.

Kaur, S. y Arora, S. 2020. Role of perceived risk in online banking and its impact on behavioral intention: trust as a moderator. Journal of Asia Business Studies 15(1).

Lake, P. y Behling, S. 2010. E-businesses at risk: a look at the impact and control of e-business fraud. Issues in Information Systems 11(1): 280-285.

Long, J. 2008. No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Syngress.

Maimon, D., Becker, M., Patil, S. y Katz, J. 2017. Self-protective behaviors over public Wifi networks. Learning from Authoritative Security Experiment Results (LASER 17): 69-76.

Mayer, P., Zou, Y., Schaub, F. and Aviv, A. 2021. "Now I'm a bit angry:" Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them. 30th USENIX Security Symposium (USENIX Security 21): 393-410.

Najaf, K., Mostafiz, M.I. and Najaf, R. 2021. Fintech firms and banks sustainability: Why cybersecurity risk matters? International Journal of Financial Engineering 8(2).

NCSC. 2021. Phishing Scams.

Nilson. 2020. Nilson Report 2020. Issue 1187.

NordVPN Blog. 2023. What is phishing and how to prevent it. NordVPN.

Referencias

NordVPN Research. 2021. No such thing as a personal device? NordVPN.
-- 2022. Analyzing 4 million payment card details found on the dark web. NordVPN.

Provos, N. 2008. The Ghost in the Browser and Other Frightening Stories About Web Malware. 17th USENIX Security Symposium.

PwC. 2015. 2015 Information Security Breaches Survey. HM Government.

Radu, A.I., Chothia, T., Newton, C.J.P., Boureanu I. y Chen, L. 2022. Practical EMV Relay Protection. IEEE Symposium on Security and Privacy: 1737-1756.

Scaife, N., Peeters, C. y Traynor, P. 2018. Fear the Reaper: Characterization and Fast Detection of Card Skimmers. 27th USENIX Security Symposium (USENIX Security 18): 1-14.

Song, X., Chen, C., Cui, B. y Fu, J. 2020. Malicious JavaScript Detection Based on Bidirectional LSTM Model. Applied Sciences 10(10): 3440.

Statista. 2020. Value of fraudulent payment card transactions worldwide from 2021 to 2027.
-- 2021. Fraud losses per 100 U.S. dollars of total card sales worldwide from 2010 to 2020.

Talukder, M.A.I., Shahriar, H. y Haddad, H. 2019. Point-of-Sale Device Attacks and Mitigation Approaches for Cyber-Physical Systems. In Cybersecurity and Privacy in Cyber Physical Systems. ImprintCRC.

Thomas, K., Pullman, J., Yeo, K., Raghunathan, A., Kelley, P.G., Invernizzi, L., Benko, B., Pietraszek, T., Patel, S., Boneh, D. y Bursztein, E. 2019. Protecting accounts from credential stuffing with password breach alerting. 28th USENIX Security Symposium (USENIX Security 19): 1556-1571.

UN. 2018. World Urbanization Prospects. Department of Economic and Social Affairs, Population Dynamics.

van der Heijden, A. and Allodi, L. 2019. Cognitive Triaging of Phishing Attacks. 28th USENIX Security Symposium (USENIX Security 19): 1309-1326.

Varmedja, D., Karanovic, M., Sladojevic, S., Arsenovic, M. and Anderla, A. 2019. Credit Card Fraud Detection - Machine Learning methods. 18 International Symposium INFOTEH-JAHORINA (INFOTEH 2019): 1-5.

Wieffering, T. 2021. Formjackers: Towards an Internet-scale Survey of Credit Card Skimming on the Web. TU Delft.

Wirth, A. 2019. Reviewing today's cyber threat landscape. Biomedical Instrumentation and Technology: 227-231.

Yu, L., Luo, B., Ma, J., Zhou, Z. and Liu, Q. 2020. You Are What You Broadcast: Identification of Mobile and IoT Devices from (Public) WiFi. 29th USENIX Security Symposium (USENIX Security 20): 55-72.

NordVPN®

2023