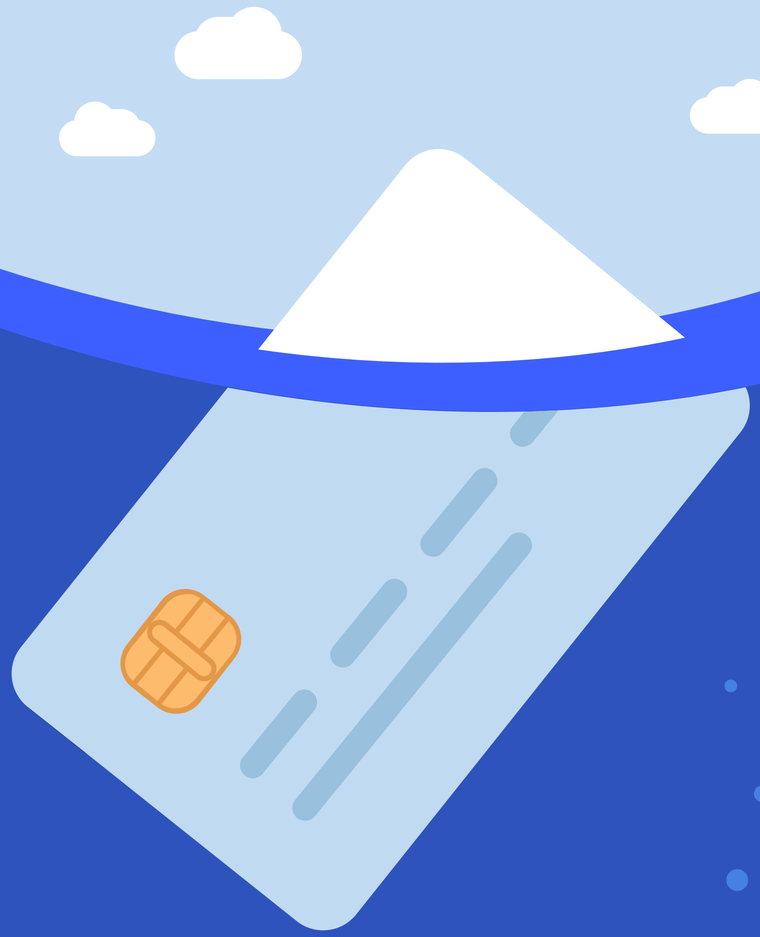
NordVPN®

La partie visible de l'iceberg : 6 millions de cartes volées analysées



Présentation

Les systèmes numériques comme les cartes de paiement entraînent des risques de sécurité et de confidentialité inévitables, et pourtant notre vie quotidienne repose sur l'idée qu'ils sont totalement fiables. Alors quels sont les risques réels de vol des données de votre carte de crédit ? Quelles autres données sont à la portée des pirates informatiques ? Comment atténuer ces risques?

Le vol de carte est un problème mondial. Le Rapport Nilson 2020 a montré que les pertes engendrées dans le monde entier s'élevaient à 28,65 milliards de dollars (26,03 milliards d'euros), plus d'un tiers des pertes étant concentrées aux États-Unis. Statista a constaté que près de 7% des ventes par carte aux États-Unis étaient frauduleuses, prédisant que le total des pertes mondiales atteindra environ 32,96 milliards de dollars (29,92 milliards d'euros) d'ici à 2023.

La technologie est un élément déterminant dans la fraude et le vol de cartes. La recherche de NordVPN sur les attaques par force brute montre que les ordinateurs peuvent être utilisés pour deviner le numéro d'une carte de crédit. Les données de paiement sont susceptibles d'être divulguées à la suite d'une violation de données ou d'un piratage de système. Les criminels n'ont même pas besoin s'occuper eux-mêmes du sale boulot. Le Dark Web héberge des marketplaces florissantes pour les données de cartes volées.

Dans cette étude, nous présentons nos recherches sur les cartes de paiement vendues sur le Dark Web. Nos conclusions s'appuient sur une base de données de près de 6 millions de cartes provenant des huit principaux marchés. Nous examinons le contexte dans lequel les cartes et autres données personnelles ont été volées, en détaillant les méthodes de notre enquête. Nous avons analysé la répartition des cartes volées par pays, ainsi que les types de cartes disponibles et leur prix. En complément des recherches existantes, nous avons examiné le lien entre les données de cartes volées et d'autres informations personnelles, en essayant de déterminer combien de données de cartes sont piratées, divulguées ou volées plutôt que des attaques par force brute.

Enfin, nous avons comparé ces résultats avec les données disponibles sur la population et le taux de pénétration des cartes afin d'établir un classement des risques pour les différents pays. Les résultats obtenus nous permettent de proposer des recommandations aux utilisateurs et aux entreprises sur la manière de prévenir le vol des données de cartes et d'autres informations à caractère personnel.

Principales observations

Au moment de nos recherches, les marketplaces du Dark Web proposaient les données de 6 millions de cartes de paiement volées, dont 2,5 millions étaient à vendre pour plus de 18,5 millions de dollars (16,81 millions d’euros) au total. Une fois achetées, ces données de cartes de paiement peuvent rapporter aux criminels une somme bien plus importante que celle qu'ils ont payée à l'origine.

Les cartes américaines sont la cible la plus importante : plus de la moitié des cartes de paiement détectées provenaient des États-Unis.

Les Russes seraient la population la moins touchée par le risque de voir ses données sur les marketplaces du Dark Web étudiées.

Plus de 60 % des cartes ont été vendues avec d'autres informations personnelles concernant la victime, telles que son adresse, son numéro de téléphone, son adresse email, sa date de naissance ou son numéro de sécurité sociale.

Les cartes se vendent en moyenne 7 dollars (6,36€), mais beaucoup sont publiées gratuitement.

Contexte

La fraude à la carte laisse souvent la victime désemparée, en grande partie parce qu'il est presque impossible de savoir comment les données de sa carte ont été volées. Même les professionnels du secteur de la sécurité sont exposés à des risques. Mais ces attaques par force brute qui consistent à deviner le numéro de carte, à le confirmer sur des sites Web où les contrôles de sécurité sont moindres, puis à l'exploiter ou à le vendre sur le Dark Web, comme nous l'avons expliqué dans nos précédentes études, ne sont qu'un moyen parmi d'autres d'obtenir le numéro de carte de paiement. Des méthodes plus directes de piratage et de vol peuvent rendre les victimes encore plus vulnérables et obtenir bien plus que les détails de leur carte.

L'usurpation d'identité a été décrite comme "la quintessence du crime de l'ère de l'information". Si une violation de données ou un piratage expose vos données de carte, mais également votre adresse et d'autres informations personnelles, les cas d'usurpation d'identité risquent de se multiplier. Tout le monde peut être victime d'une usurpation d'identité et il faut parfois des années pour réparer les dégâts. Une fois que le pirate a obtenu le nom, l'adresse personnelle et email de la victime, il peut même abuser de méthodes légales (telles que l'utilisation du droit d'accès à des informations plus personnelles prévu par la RGPD) pour poursuivre son projet de vol d'identité ou commettre d'autres activités malveillantes.

Il faut également souligner que si la fraude à la carte de crédit a tendance à toucher les personnes les plus aisées (ce qui lui vaut d'être présentée comme un "crime sans victime" dans la culture populaire car les victimes sont privilégiées et les sociétés de cartes de crédit remboursent souvent les frais frauduleux), d'autres formes d'usurpation d'identité, comme le vol de compte bancaire, touchent souvent les personnes défavorisées.

Dans cette étude, nous nous concentrons sur les cas où les détails de la carte sont vendus sur le Dark Web avec d'autres informations personnelles. Cette situation multiplie les enjeux en apportant une valeur ajoutée (utilisation des informations en vue d'une usurpation d'identité), mais elle cause également un préjudice supplémentaire à la victime (davantage d'informations exposées et un risque accru d'usurpation d'identité). Ces ensembles d'informations sont issus de violations de la cybersécurité (piratages, fuites, vols) qui pourraient être évitées grâce à des mesures de protection appropriées. Pour se protéger, il convient d'abord de comprendre comment les données des cartes et d'autres informations peuvent être volées.

Cartes de crédit et vol de données

Les différentes méthodes de vol ont été classées en plusieurs catégories selon le type d'attaque utilisé :

- **Méthodes traditionnelles**
  - Physique
  - Social
- **Méthodes de piratage**
  - Appareils
  - Système

Nous avons divisé ces catégories en fonction de l'échelle :

- **Petite échelle :** Fonctionne souvent à titre individuel.
- **Moyenne échelle :** Moins ciblée, peut être à long terme avec la possibilité de passer à l'échelle supérieure.
- **Grande échelle :** Peut être facilement automatisé ou affecte un grand nombre de personnes à la fois.

Bien entendu, ces méthodes de vol sont susceptibles de se superposer, et c'est d'ailleurs souvent le cas. Bien entendu, ces méthodes de vol sont susceptibles de se superposer, et c'est d'ailleurs souvent le cas. La notion de phishing recouvre à la fois les pratiques sociales et les méthodes numériques automatisées.

	Traditionnelle		Piratage	
	Physique	**Social**	**Appareils**	**En ligne**
Petite échelle	Perte ou vol de la carte Fouille des poubelles	Shoulder surfing / copie Arnaque à l'amitié	Puce RFID Wi-Fi public	Piratage de compte bancaire en ligne
Échelle moyenne	Écrémage de cartes (skimming)	Appels téléphoniques frauduleux	Logiciel malveillant POS	
Grande échelle		Hameçonnage ou phishing	Logiciels malveillants sur les appareils	Force brute Vol de formulaire Fuite de données

Nous allons maintenant examiner chacune de ces méthodes de vol de données de cartes.

La perte ou le vol de la carte est peut-être la méthode utilisée la plus simple, impliquant la perte physique de la carte. Les victimes se rendent généralement compte de son efficacité plus tôt, par rapport aux autres méthodes citées dans cette liste.

La **fouille des poubelles** a été décrite comme “no tech hacking”, autrement dit : sans aucun piratage informatique. Cette démarche peut consister à rechercher des données personnelles, des relevés bancaires ou d’anciennes cartes de crédit dans les ordures ménagères, ou à faire une descente dans les installations d’élimination des déchets des entreprises pour y trouver des documents sensibles contenant des ensembles plus importants de données sur les clients. Elle peut impliquer de l’ingénierie sociale, par exemple lorsqu’elle conduit à un vol d’identité ou lorsque des comportements inappropriés sont utilisés pour obtenir un accès non autorisé à des déchets confidentiels.

Surveillance rapprochée (Shoulder surfing)/copie est une autre forme de “no tech hacking”. Cette pratique signifie que l’on regarde par-dessus l’épaule d’une personne dans le train ou dans un café très fréquenté pour observer son mot de passe, son numéro de carte ou d’autres informations. Il s’agit également des employés de commerce qui copient les données des cartes lorsqu’ils encaissent les paiements. Cette méthode de vol de données est très peu sophistiquée, mais elle est populaire et efficace pour les criminels à petite échelle.

Une escroquerie en milieu familial ou “amical” se produit souvent lorsque des proches abusent de l’accès aux informations personnelles et aux cartes physiques, mais une escroquerie “amicale” peut également être perpétrée par des consommateurs malhonnêtes. Par exemple, en effectuant des achats qui sont ensuite refacturés via la carte de crédit du consommateur. Cette pratique finit par coûter de l’argent au vendeur, ce qui peut être particulièrement dommageable pour les PME qui vendent leurs produits en ligne.

L’écrémage de carte ou le skimming est une technique qui consiste à ajouter un dispositif supplémentaire à un distributeur automatique de billets pour copier les données de la carte de la victime. Bien qu’ils existent depuis des décennies, les dispositifs d’écrémage de cartes sont peu visibles si vous êtes occupé ou si vous ne les cherchez pas activement. Les différents types de skimmers ont des niveaux de discrétion variables, et certains sont très sophistiqués en ce qui concerne l’altération du distributeur automatique de billets.

Les appels téléphoniques frauduleux sont l’un des premiers exemples d’ingénierie sociale. Lors de ces appels, l’escroc se fait passer pour votre banque ou une autre organisation de confiance afin de vous inciter à révéler des informations sensibles. Les gouvernements publient souvent des conseils et des listes de signalements en cas d’appels téléphoniques frauduleux.

Le phishing constitue une méthode d’attaque largement connue, mêlant des escroqueries plus traditionnelles à des techniques numériques (telles que les spams ou les faux sites) pour inciter les victimes à divulguer leurs identifiants de connexion, leurs informations de compte ou leur numéro de carte. Le phishing manipule les mécanismes de vulnérabilité cognitive qui répondent à nos attentes. Il existe des mesures à prendre si vous êtes victime, mais il est préférable d’agir rapidement.

Puce RFID : piratage d’un paiement effectué avec une carte physique à proximité. Un paiement sans contact peut être copié et relayé pour effectuer des paiements dans d’autres pays. Les banques ont pris des mesures pour limiter les attaques par RFID.

Le Wi-Fi public pose de sérieux problèmes de sécurité, en particulier lorsqu’il fonctionne avec des appareils inconnus et éventuellement malveillants. Le public semble être conscient d’au moins une partie de ces risques, les utilisateurs adoptent différents comportements pour se protéger. Par exemple, de nombreuses personnes ont tendance à éviter les services bancaires en ligne lorsqu’elles sont sur un réseau Wi-Fi public, mais elles vont quand même sur d’autres sites (comme les réseaux sociaux) qui pourraient laisser filtrer des informations importantes et entraîner des usurpations d’identité ou des arnaques à la carte de crédit.

Le piratage des comptes bancaires en ligne affecte généralement les personnes appartenant à des groupes déjà isolés. Les relations de plus en plus étroites entre les banques et les entreprises fintech émergentes créent des risques supplémentaires en matière de cybersécurité. Les institutions pourraient promouvoir des mesures de protection sous la forme de risques perçus, d’interfaces favorisant la sécurité, de confiance institutionnelle et de réassurances (comme les garanties de remboursement), bien qu’elles n’atténuent pas nécessairement l’impact et les effets potentiels à plus long terme de l’usurpation d’identité.

Le logiciel malveillant POS infecte les appareils de point de vente (POS) des magasins en y introduisant des virus qui envoient les données de la carte aux pirates informatiques. Ces attaques vont du ciblage de magasins spécifiques à des piratages à grande échelle, lorsqu'un nombre suffisant de terminaux de point de vente d'un grand magasin sont compromis. Par exemple, en 2013, la chaîne de magasins Target a été victime de ce type d'attaque. La menace des logiciels malveillants est d'autant plus importante que les magasins s'orientent vers des points de vente basés sur des tablettes et des téléphones, les criminels continuent d'améliorer leurs méthodes pour éviter d'être détectés.

Les logiciels malveillants installés sur les appareils constituent un problème courant, avec une importante "économie souterraine" basée sur l'utilisation de logiciels malveillants en tant que services. Les logiciels malveillants présents sur votre appareil peuvent récupérer des données directement, espionner d'autres applications (agissant comme un "fantôme dans le navigateur") ou compromettre la sécurité de votre appareil personnel ou d'entreprise pour renvoyer des données aux criminels.

Attaque par force brute : le phénomène a été examiné en détail dans une étude antérieure réalisée par NordVPN. Une attaque par force brute est une tentative de deviner les données de la carte en essayant plusieurs combinaisons. Ces attaques sont facilitées par le fait que les cartes de certains pays, émetteurs de cartes et banques suivent certains modèles. Les suppositions peuvent être rapidement vérifiées à grande échelle sur des sites dont la sécurité des paiements est laxiste.

Le **détournement de formulaire** est une forme récemment découverte d'attaque en ligne qui utilise des JavaScripts malveillants et d'autres techniques pour prendre le contrôle de formulaires en ligne et transmettre les données à des pirates informatiques. Le détournement de formulaires est difficile à détecter et permet d'exploiter un large éventail d'autres vulnérabilités présentes sur les sites Web et les navigateurs. Elle devient plus fréquente à l'approche des fêtes de fin d'année, avec l'augmentation des achats en ligne.

Les violations de données constituent un risque majeur pour la réputation des entreprises et un risque réel pour leurs clients. Selon le rapport 2015 de PwC au gouvernement britannique, non seulement le nombre d'incidents a augmenté par rapport à l'année précédente, mais leur ampleur et leur coût ont également doublé, à tel point que les grandes entreprises devraient les considérer comme une "quasi-certitude". Bien que certaines violations très médiatisées fassent la une des journaux, la situation est souvent mal décrite et mal comprise. Les utilisateurs finissent souvent par blâmer à tort leurs propres habitudes plutôt que l'organisation victime de la violation ou les pirates, et sous-estiment souvent les effets potentiels pour eux personnellement, même s'ils sont conscients des risques généraux. Des outils simples à utiliser sont essentiels lorsqu'il s'agit de sensibiliser le public et de l'inciter à agir à la suite d'une infraction. Par exemple, les notifications de violation de mot de passe peuvent prévenir les attaques de bourrage d'identifiants, limitant ainsi les effets de l'usurpation d'identité résultant des fuites d'informations personnelles.

Le tableau ci-dessus tente de classer chaque type d'attaque dans la catégorie appropriée. Cette étude se concentre sur les types mis en évidence car ils impliquent des techniques de piratage numérique plus directes et peuvent (dans une certaine mesure) être atténués en adoptant un comportement et des outils appropriés.

Il est important de souligner que tous les types d'attaques mentionnés ci-dessus peuvent conduire à un vol de carte de paiement ainsi qu'à des cas plus larges d'usurpation d'identité. Lorsque davantage d'informations sont divulguées en plus des numéros de cartes, il devient plus facile pour les pirates (et ceux à qui ils vendent les données) de causer des dommages à long terme à leurs victimes.

Méthodologie

Pour évaluer l’ampleur du vol de cartes en ligne, nous avons utilisé un ensemble de données provenant de millions de cartes en vente sur le Dark Web. Nous avons notamment examiné les cartes accompagnées d’autres informations personnelles afin de déterminer combien d’entre elles ont été piratées ou volées plutôt qu’obtenues par une attaque par force brute.

Collecte des données

Les données ont été rassemblées en partenariat avec des spécialistes indépendants de la recherche sur les incidents de cybersécurité. Ils se sont intéressés à huit grands marchés du Dark Web pour récupérer les données de plus de 6 millions de cartes, y compris le type de carte (de crédit ou de débit) et d’autres informations personnelles connexes. Les données que NordVPN a reçues de la part de ces chercheurs indépendants ne contenaient aucune information relative à une personne identifiée ou identifiable (comme des noms, des informations de contact ou d’autres informations personnelles). L’étude n’a pas déterminé le nombre exact ni analysé la totalité des détails de cartes de paiement vendus sur l’ensemble du Dark Web. NordVPN n’a examiné que l’ensemble des données statistiques fournies par des chercheurs indépendants.

Traitement des données

En raison de la nature des marchés du Dark Web, tous les vendeurs présents sur ce réseau ne peuvent pas être classés dans des catégories de données standard ou être étiquetés. Pour créer un ensemble de données cohérent, nous avons exclu les entrées dont les données étaient incomplètes ou incompatibles. Ces données retirées représentent moins de 1,5% de l’ensemble : environ 3 500 ont été retirées en raison d’erreurs pendant le chargement et 80 000 autres en raison d’un étiquetage inadapté. Nous disposons donc d’un ensemble de données de 5 953 651 cartes.

Nous les avons classées par pays où la carte a été émise. Nous avons ainsi obtenu plus de 200 catégories, que nous avons limitées en nous concentrant sur les pays dont l’ensemble de données contenait plus de 1 000 cartes. Cela s’explique par le fait qu’un grand nombre de pays ne possèdent qu’une poignée de cartes, ce qui fausse les données lorsqu’il s’agit d’établir des comparaisons internationales. Il nous reste donc 98 pays à comparer, une liste qui reflète généralement la population des pays. Les données des autres pays ont été regroupées dans la catégorie “pas de pays/autre pays” afin qu’elles restent présentes dans l’ensemble.

Extraction des données

Nous avons récupéré de notre base de données les informations suivantes, classées par pays :

- **Nombre**
- **Prix moyen**
- **Carte**
  - Type : crédit, débit, autre
  - Marque : Visa, Mastercard, Amex, autre
- **Informations supplémentaires**
  - Adresse du domicile
  - Numéro de sécurité sociale
  - Date de naissance
  - Numéro de téléphone
  - Adresse email

Nous avons ensuite calculé le pourcentage de cartes obtenues par piratage, vol ou violation de données. La condition requise était que des données supplémentaires (adresse du domicile, numéro de sécurité sociale, date de naissance, numéro de téléphone ou adresse électronique) soient incluses. Les autres ont pu être obtenues par force brute, car elles ne contiennent que les données de la carte elle-même. Cependant, le pourcentage de cartes piratées est une estimation prudente. Il est probable que certaines données de cartes classées dans la catégorie “force brute” résultent également d’un vol ou d’une infraction. Par ailleurs, le pourcentage de cartes ayant fait l’objet d’une attaque par force brute représente le nombre maximal possible (il est quasiment impossible d’obtenir d’autres éléments d’information en plus des détails de la carte en utilisant cette méthode).

Nous avons comparé les données statistiques sur les cartes entre les pays avec les statistiques démographiques de l’ONU et le nombre de cartes en circulation par pays ou région de Visa, Mastercard et American Express. À l’aide des informations ci-dessous, nous avons créé un indice de risque pour comparer les probabilités de trouver les données de cartes bancaires de citoyens de différents pays sur le Dark Web :

- **Nombre de cartes dans la base de données** (N)
- **Population** (P)
- **Nombre de cartes en circulation par personne** (C)
- **Le pourcentage de cartes manifestement volées par piratage** (H)

La dernière variable a été ajoutée pour tenir compte du risque supplémentaire lié au fait que certains pays sont des cibles plus importantes pour les pirates informatiques. Les attaques par force brute peuvent potentiellement toucher tous les pays, tandis que les violations et les piratages majeurs ont tendance à se concentrer sur des entreprises, des sites ou d’autres entités spécifiques liées à des pays particuliers. L’indice de risque a été calculé selon la formule suivante :

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

À partir de ces types de données, nous avons pu analyser les tendances et les différences entre les pays.

Résultats

Notre étude montre qu'un grand nombre d'informations sur les cartes sont volées en même temps que d'autres données personnelles sensibles, ce qui représente un risque important d'usurpation d'identité. Les données de millions de cartes sont divulguées gratuitement sur les marchés du Dark Web. Le prix moyen des 2,5 millions de cartes disponibles à la vente était de 7,01 dollars (6,36€), l'ensemble des données volées ayant une valeur de 18,5 millions de dollars (16,77 millions d'euros).

Le tableau à la fin de cette section présente les 20 premiers pays en fonction des paramètres clés suivants : nombre de cartes, prix moyen et pourcentage de cartes comportant des informations supplémentaires (exigence minimale pour les cartes piratées), ainsi que les indices de risque les plus élevés et les plus faibles.

Cartes

Sur notre base de données contenant près de 6 millions de cartes, plus de la moitié provenait des États-Unis (3 461 444 cartes, soit 58,1%). C'est logique, car les États-Unis ont un taux de pénétration des cartes plus élevé, une population importante et une économie forte. Viennent ensuite l'Inde (3,7%), le Royaume-Uni (2,8%) et le Mexique (2,6%), puis le Brésil, la Chine, la France et l'Italie : un mélange de pays très peuplés et dotés d'une économie ou d'une réputation politique forte.

Sur les 2,5 millions de cartes vendues sur les places de marché du Dark Web, les cartes en provenance du Danemark ont atteint le prix moyen le plus élevé, soit 11,54 dollars (10,46€) par carte. Ensuite viennent les cartes du Japon, du Portugal et de l'Ukraine, qui coûtent toutes plus de 11 dollars (9,97€) en moyenne.

Les cartes en provenance des États-Unis sont comparativement moins chères : à 6,86 dollars (6,22€), elles se situent juste en dessous du coût moyen global de 7,01 dollars (6,36€). Les cartes en provenance d'Argentine et de Nouvelle-Zélande étaient les moins chères, avec une moyenne inférieure à 2,50 dollars (2,27€). Vu l'ampleur des dégâts que peuvent causer les données de cartes volées et les informations personnelles qu'elles contiennent, il s'agit d'un montant étonnamment faible, ce qui laisse penser que l'utilisation de cartes volées pourrait être relativement modulable, même par ceux qui ont obtenu les informations d'occasion sur le Dark Web.

Informations complémentaires

Plus de la moitié (51,5%) des cartes étaient accompagnées d'une adresse, tandis qu'un nombre important d'entre elles étaient accompagnées d'un numéro de téléphone (39,8%) et d'une adresse email (28,7%). Très peu de cartes comportaient une date de naissance (2,5%) ou un numéro de sécurité sociale (1,8%), alors que ces informations supplémentaires exposeraient la victime à un risque nettement plus élevé d'usurpation d'identité.

Dans l'ensemble, 62,8% (près des deux tiers) des cartes étaient accompagnées d'une forme ou d'une autre d'informations supplémentaires, ce qui indique un piratage, tandis que jusqu'à 37,2% des cartes ont été devinées par des attaques par force brute (rappelons qu'il s'agit d'une estimation haute pour les attaques par force brute et d'une estimation basse pour les piratages). Cela signifie que la majorité des données de cartes volées ont été obtenues par l'une des méthodes de piratage mentionnées plus haut.

Les chiffres varient selon les pays. Soulignons que les enregistrements sans informations valables sur le pays ont suivi une tendance inverse, la quasi-totalité des entrées ne contenant que les détails de la carte (92,4%). En général, les pays ayant le plus grand nombre de cartes dans l'ensemble de données avaient des taux plus élevés de cartes avec des informations supplémentaires, à l'exception de la Chine (qui a peut-être suivi la tendance en raison d'un manque d'intégration avec les systèmes d'information mondiaux et de la nature fermée du réseau Internet chinois, des plateformes d'achat en ligne et bancaires).

Près de 90% des cartes en provenance de l'Inde contenaient des données supplémentaires, exposant ainsi les victimes indiennes à des problèmes plus vastes de fraude d'identité. D'une manière générale, les pays européens et les pays économiquement plus développés affichent des taux plus élevés d'informations supplémentaires, ce qui montre qu'il existe une faible corrélation entre la valeur perçue de la victime et les tentatives de piratage.

Indice de risque

En utilisant le calcul décrit ci-dessus, nous avons créé un indice de risque pour 98 pays. Notre indice considère la probabilité qu'une de vos cartes se retrouve sur le Dark Web et les risques supplémentaires posés par sa vente avec des informations additionnelles.

Les pays présentant l'indice de risque le plus élevé (et donc le risque le plus important) sont Malte, l'Australie et la Nouvelle-Zélande. Cette situation peut s'expliquer par leur association avec l'UE ou la communauté anglo-saxonne et par leur population moins nombreuse par rapport à leur poids financier et politique. Les États-Unis se classent au 5e rang, tandis que Singapour et Hong Kong sont respectivement au 9e et au 10e rang.

En revanche, la Russie a obtenu le score de risque le plus bas et la Chine s'est classée à l'avant-dernière place. Ces informations rejoignent les hypothèses les plus courantes concernant la localisation des opérations de piratage à grande échelle et le ciblage délibéré des pays anglo-européens. Les autres pays moins bien classés dans l'indice de risque avaient généralement des économies plus petites (à l'exception de l'Allemagne, qui occupait la quinzième place en partant de la dernière position).

L'indice de risque n'est pas nécessairement corrélé au nombre de cartes dans l'ensemble de données, ce qui montre l'importance de prendre en compte la taille de la population, la pénétration des cartes et d'autres facteurs pour évaluer le risque. Il y a aussi le cas de l'Allemagne qui, malgré une économie forte et une population importante pour un pays européen, avait une note de risque très basse. Cela peut être dû à des facteurs politiques et comportementaux, tels qu'une plus grande attention portée aux réglementations ainsi qu'à l'augmentation des mesures de sécurité et de protection de la confidentialité mises en œuvre pour les individus et les organisations.

Les 20 premiers pays selon différentes catégories de données

Pays	Cartes	%
États-Unis	3461444	58,1
Inde	218053	3,7
Royaume-Uni	164143	2,8
Mexique	156613	2,6
Brésil	144297	2,4
Chine	114765	1,9
Canada	97552	1,6
France	97032	1,6
Italie	78676	1,3
Australie	65350	1,1
Espagne	60173	1
Afrique du Sud	46737	0,8
Turquie	41803	0,7
Chili	30079	0,5
Allemagne	26558	0,4
Malaisie	22504	0,4
Argentine	16792	0,3
Pérou	13968	0,2
Danemark	12468	0,2
Norvège	12055	0,2

Pays	Prix moyen
Danemark	$11.54 (10,45€)
Japon	$11.07 (10,03€)
Portugal	$11.07 (10,03€)
Ukraine	$11.02 (9,99€)
Slovénie	$10.83 (9,81€)
Vietnam	$10.74 (9,73€)
Slovaquie	$10.64 (9,64€)
Chili	$10.55 (9,56€)
Arabie Saoudite	$10.55 (9,56€)
Thaïlande	$10.27 (9,31€)
Singapour	$10.20 (9,24€)
Philippines	$10.00 (9,06€)
Mauritanie	$9.98 (9,05€)
Hongrie	$9.71 (8,80€)
France	$9.42 (8,54€)
Ouganda	$9.04 (8,20€)
Cameroun	$8.98 (8,14€)
Italie	$8.90 (8,07€)
Russie	$8.62 (7,82€)
Brésil	$8.47 (7,68€)

Pays	% piraté
Inde	89,8
Slovaquie	86,3
Arabie Saoudite	82,8
Portugal	82
Ukraine	82
Chili	81,4
Hongrie	79,2
Japon	78,9
Slovénie	77,2
États-Unis	76,8
Islande	76,3
France	74,9
Bahrain	74,6
Danemark	74,1
Italie	73,3
Russie	73,2
Irak	72,9
Grèce	72,2
Suisse	72,1
Royaume-Uni	71,9

Pays	Indice de risque
Malte	1
Australie	0,91
Nouvelle-Zélande	0,84
Slovénie	0,82
États-Unis	0,79
Bahrain	0,79
Bahamas	0,78
Émirats Arabes Unis	0,78
Singapour	0,77
Hong Kong	0,77
Namibie	0,77
Quatar	0,74
Botswana	0,73
Chili	0,72
Puerto Rico	0,72
Eswatini	0,72
Islande	0,71
Turquie	0,71
Oman	0,71
Hongrie	0,68

Pays	RI (plus bas)
Russie	0
Pakistan	0,01
Chine	0,04
Bangladesh	0,06
Vénézuéla	0,09
Ukraine	0,16
Indonésie	0,16
Égypte	0,18
Bénin	0,18
Zimbabwe	0,2
Paraguay	0,21
Irak	0,26
Vietnam	0,26
Nigeria	0,27
Allemagne	0,28
Maroc	0,3
Colombie	0,31
Pologne	0,31
Mozambique	0,31
Tunisie	0,32

Quelques recommandations

Les banques sont capables de réduire les risques en utilisant des moyens technologiques, mais elles doivent alors faire face à une surveillance invasive et coûteuse des clients et à des transactions potentiellement frauduleuses. De même, les banques et les boutiques en ligne ne peuvent tout simplement pas contrôler les problèmes plus vastes liés à l'usurpation d'identité et aux violations de données. C'est souvent à l'utilisateur de se protéger contre ces risques en intégrant dans sa vie quotidienne des outils de protection de la confidentialité et de la sécurité en ligne.

Nous vous recommandons de lire notre guide expliquant comment se protéger contre l'usurpation d'identité ou de suivre ces étapes spécifiques et d'utiliser les outils NordVPN pour lutter contre des menaces spécifiques :

VPN pour la banque en ligne

- Protégez les données de votre réseau, en particulier sur les réseaux Wi-Fi publics, afin d'assurer la sécurité de vos informations personnelles et financières.

Protection anti-menaces

- Recherchez les malwares pendant les téléchargements pour éliminer les menaces potentielles des terminaux de paiement personnels et professionnels.
- Bloque les sites web malveillants qui pourraient faire fuiter vos données ou les publicités malveillantes qui permettraient des détournement de formulaires.
- Associée à des VPN et à d'autres outils de cybersécurité, Protection Anti-menaces peut aider à se prémunir contre les tentatives d'hameçonnage (phishing) par lesquelles les pirates tentent d'amener les victimes à révéler des informations confidentielles.

Surveillance Dark Web

- Recevez des alertes si vos identifiants apparaissent sur le Dark Web à la suite d'une attaque par force brute ou d'une violation de données, ce qui vous permet de prendre les devants et d'éviter que les criminels ne prennent une longueur d'avance.

NordPass

- Utilisez des mots de passe uniques et complexes pour protéger vos comptes bancaires en ligne et autres comptes contre les attaques par force brute et autres méthodes de piratage.

NordLayer

- Réduisez le risque de fuites de données pour votre entreprise et protégez-les (et celles de vos clients) grâce à une protection réseau multicouche et évolutive, surtout si vous avez des travailleurs à distance.

Il existe différents moyens de voler, de pirater ou de divulguer des données de cartes ou des données personnelles. Il est donc préférable d'adopter une approche multidimensionnelle de la sécurité. Combinez ces outils pour réduire le risque global que vos données soient vendues sur le Dark Web et les conséquences à long terme de l'usurpation de crédit et d'identité qui pourraient en découler.

Références

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

Caballero, J., Grier, C., Kreibich, C. and 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. et 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. and 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. and 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. and 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. and 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. and 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.

Références

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. et Chen, L. 2022. Practical EMV Relay Protection. IEEE Symposium on Security and Privacy: 1737-1756.

Scaife, N., Peeters, C. and 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. et 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. et 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. et 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. et Anderla, A. 2019. Credit Card Fraud Detection - Machine Learning methods. 18th 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. et 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