Veille technologique (Carding)

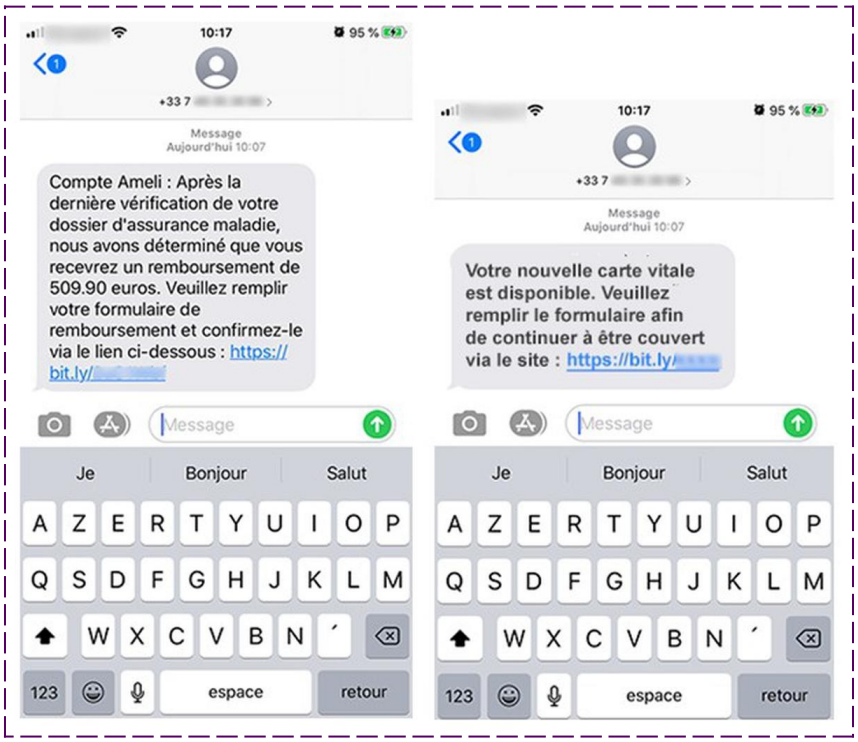
11/04/2024

Introduction :

Qu’est ce que le carding ?

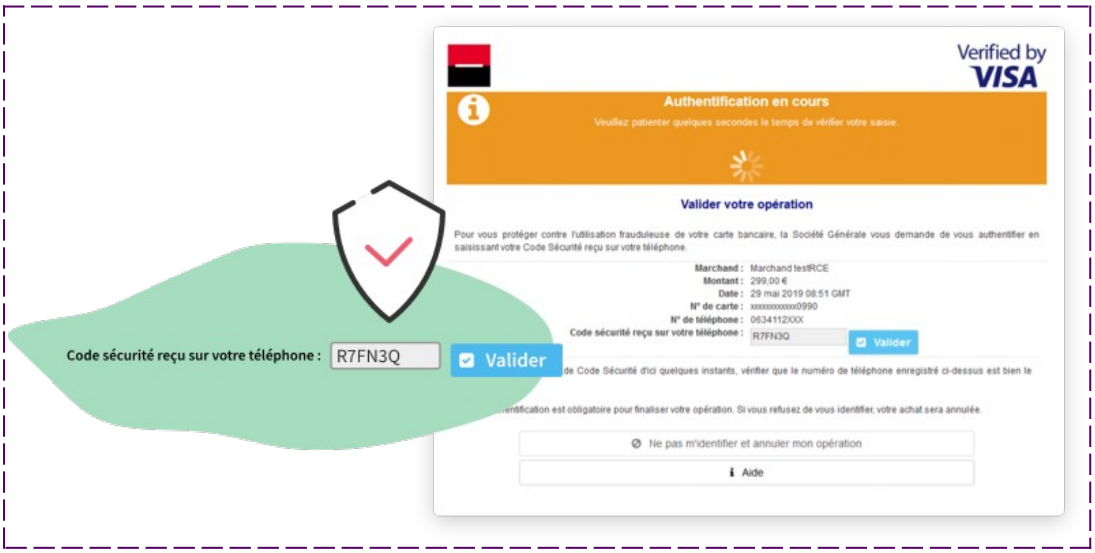
Pour débuter, il est crucial de définir le terme "carding". Il s'agit d'une forme d'escroquerie en ligne qui tire son nom de "card", le terme anglais pour "carte". Dans cette fraude, les informations de cartes bancaires volées sont exploitées pour réaliser des achats frauduleux sur Internet.

La première étape pour les criminels informatiques est d'obtenir vos données de carte bancaire. Pour ce faire, ils utilisent diverses techniques, allant du phishing sophistiqué à l'exploitation de failles de sécurité sur des sites de commerce en ligne.



Ensuite, les criminels informatiques effectuent des achats en utilisant vos informations. Les articles choisis et le montant des dépenses peuvent varier, allant de petites transactions discrètes à des achats importants susceptibles d'attirer rapidement l'attention.

Ils privilégient les sites moins sécurisés ne nécessitant pas de validation par mobile ou par SMS. Les plateformes comme Amazon et d'autres sites de commerce en ligne sont rarement utilisées, sauf pour de petites sommes.



Les arnaqueurs vous contacte ensuite, souvent appelées "arnaque à l'usurpation d'identité", ce sont des stratagèmes où les escrocs utilisent des informations récupérées via des sites Web pour contacter leurs victimes par téléphone.

Une fois en communication avec la victime, les fraudeurs utilisent ces informations personnelles pour gagner leur confiance. Ils peuvent prétendre être des représentants de services légitimes tels que des banques, des entreprises de télécommunications ou des agences gouvernementales.

En se faisant passer pour des membres du personnel de confiance, ils induisent la victime en erreur et lui font croire qu'ils disposent déjà de données confidentielles, ce qui renforce leur crédibilité.

Ils peuvent ensuite inciter la victime à effectuer une action, comme valider une transaction bancaire ou partager des informations supplémentaires, en utilisant des tactiques de manipulation et de pression psychologique.

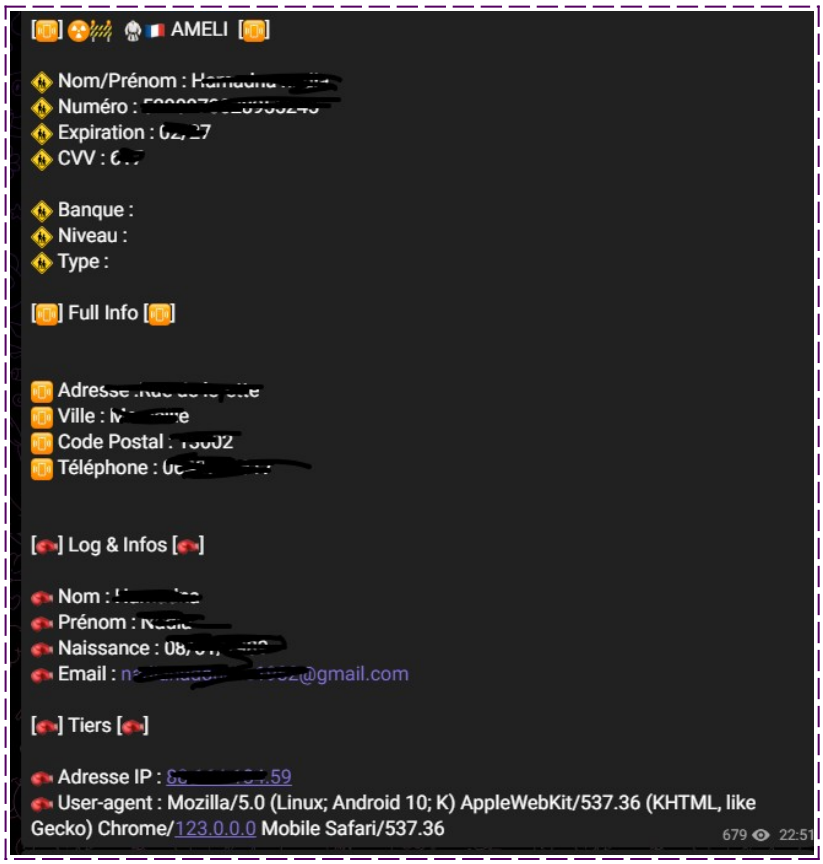
Ces escroqueries téléphoniques sont souvent sophistiquées et peuvent causer des pertes financières importantes aux victimes. Il est crucial pour les individus d'être vigilants et de ne jamais divulguer d'informations personnelles ou financières sensibles lorsqu'ils sont contactés par téléphone, surtout s'ils ont des doutes sur l'identité de l'appelant.

Parfois, ils recourent même à des appareils physiques tels que des lecteurs RFID ou NFC pour obtenir ces informations. Toutes les méthodes sont utilisées pour acquérir un maximum de données personnelles.

Ensuite, les criminels informatiques effectuent des achats en utilisant vos informations. Les articles choisis et le montant des dépenses peuvent varier, allant de petites transactions discrètes à des achats importants susceptibles d'attirer rapidement l'attention.

Ils privilégient les sites moins sécurisés ne nécessitant pas de validation par mobile ou par SMS. Les plateformes comme Amazon et d'autres sites de commerce en ligne sont rarement utilisées, sauf pour de petites sommes.

Une fois que la victime a saisi ses données sur le site de phishing de l'escroc, ces informations sont souvent transmises aux arnaqueurs via des canaux tels que Telegram ou Discord.



Vocabulaires des arnaqueurs :

no vbv : Le terme "no vbv" fait référence à un site Web ou à une plateforme de paiement qui n'exige pas la vérification de la carte bancaire (VbV) lors d'une transaction.

La vérification de la carte bancaire (VbV) est une mesure de sécurité supplémentaire mise en place par certaines banques pour authentifier les transactions en ligne. Elle nécessite souvent la saisie d'un code ou d'un mot de passe supplémentaire pour valider la transaction, ce qui rend plus difficile pour les fraudeurs d'utiliser des cartes de crédit volées ou frauduleuses.

Ainsi, un "site no vbv" est souvent recherché par les fraudeurs car il leur permet d'effectuer des transactions frauduleuses en contournant cette

vérification de sécurité supplémentaire. Cela facilite l'utilisation de cartes de crédit volées ou obtenues de manière frauduleuse pour effectuer des achats en ligne sans être bloqué par la vérification de la carte bancaire.

Spoofer : Un "spoofer" est un logiciel qui utilise des techniques de "spoofing" pour falsifier ou masquer son identité, son adresse IP ou d'autres informations lors de la communication sur Internet. Le "spoofing" est une pratique consistant à manipuler les données d'identification afin de faire croire à une identité ou à une source différente de celle réelle.

Voici quelques exemples de "spoofing" courants :

Spoofing d'adresse IP : Falsification de l'adresse IP d'un ordinateur ou d'un appareil pour masquer sa véritable identité ou sa localisation.

Spoofing d'e-mail : Envoi d'e-mails frauduleux en utilisant une adresse e-mail falsifiée pour faire croire qu'ils proviennent d'une source légitime.

Spoofing d'identifiant de téléphone : Modification de l'identifiant de l'appelant lors d'appels téléphoniques pour masquer le numéro réel de l'appelant.

Les spoofers peuvent être utilisés à des fins malveillantes, telles que la fraude en ligne, le phishing, l'usurpation d'identité ou les attaques de déni de service distribué (DDoS).

Alloteur : Terme utilisé dans le langage des escrocs pour désigner une personne qui pratique des arnaques téléphoniques ou des fraudes par téléphone.

C'est une personne qui appelle les victimes potentielles dans le but de les tromper ou de leur soutirer de l'argent en utilisant divers stratagèmes frauduleux.

Les alloteurs peuvent se faire passer pour des représentants de services légitimes tels que des banques, des entreprises de télécommunications ou des agences gouvernementales, dans le but de gagner la confiance de leurs

victimes et de les inciter à divulguer des informations personnelles ou à effectuer des paiements.

Allo : Dans le langage des arnaqueurs, le terme "allo" est souvent utilisé pour désigner une personne qui est victime d'une arnaque ou d'une escroquerie.

C'est une abréviation dérivée de l'expression "allô la police", souvent utilisée pour se moquer ou ridiculiser quelqu'un qui est tombé dans une arnaque et qui pourrait être tenté de signaler l'incident aux autorités.

C'est donc un terme péjoratif utilisé pour désigner une personne dupée ou manipulée dans le cadre d'une fraude.

Spammeur : Dans le contexte du carding, un "spammeur" est une personne qui envoie massivement des e-mails ou des messages texte frauduleux dans le but de promouvoir des techniques de carding, des sites de phishing ou des offres de cartes de crédit volées.

Ces spams peuvent contenir des liens vers des sites Web frauduleux où les utilisateurs sont incités à divulguer leurs informations personnelles ou financières, ou à acheter des cartes de crédit volées.

Les spammeurs dans le domaine du carding utilisent souvent des techniques sophistiquées pour contourner les filtres anti-spam et atteindre un grand nombre de destinataires.

Leurs messages peuvent promettre des offres alléchantes ou des opportunités financières, mais en réalité, ils visent à escroquer les destinataires en leur soutirant de l'argent ou en utilisant leurs informations personnelles à des fins frauduleuses.

Sources :

J'ai infiltré un réseau d'arnaqueurs au SMS

https://en.wikipedia.org/wiki/Carding_(fraud)

https://www.oracle.com/fr/security/qu-est-ce-que-carding/

https://www.leblogduhacker.fr/le-carding-un-business-lucratif-pour-les-cybercriminels/

https://www.zdnet.fr/actualites/carding-les-donnees-de-carte-bancaire-de-40-000-francais-exposees-39927259.htm

https://fastercapital.com/fr/contenu/Carding--exposer-le-commerce-de-cartes-de-credit-illicite-sur-les-marches-DarkNet.html

https://www.leparisien.fr/archives/ils-fabriquaient-des-fausses-cartes-de-paiement-28-05-2014-3877447.php