DOSSIER

Dark Web Monitoring

QU'EST-CE QUE LE DARK WEB ?
COMMENT LA SURVEILLANCE DU DARK WEB RÉDUIT VOS RISQUES DE COMPROMISSION ?

serenety
By xmco

Sommaire

Avant-propos.

LES MOYENS DE RENDRE VULNÉRABLE UNE ENTREPRISE N'ONT CESSÉ DE SE DÉVELOPPER NOTAMMENT À TRAVERS LE CYBERESPACE. C'EST LA RAISON POUR LAQUELLE, DANS SA MISSION DE PROTECTION, L'ENTREPRISE, ET PLUS PRÉCISÉMENT LA DIRECTION DES SYSTÈMES D'INFORMATION, NE DOIT PAS NÉGLIGER LES MENACES QUI SE CACHENT DANS LES PROFONDEURS DU WEB…

Dans ce dossier nous expliquons ce qu'est le Dark Web, ce qu'on y trouve et comment sa surveillance permet à toute entreprise de limiter ses risques d'attaques et d'anticiper l'éventuelle utilisation de failles de sécurité rendues publiques sur ces réseaux.

1. Qu'est-ce que le Dark Web ?

Qu'est-ce que le Dark Web ?

Il est commun de représenter le web en 3 parties :

SURFACE WEB

Représente tous les sites internet et les pages qui sont indexées par les moteurs de recherches classiques tels que Google ou Bing. **C'est le web auquel tout le monde a accès via des recherches directes.** Toutefois, représenté par « la partie émergée de l'iceberg », on suggère souvent que le « Clear web » ne représenterait que 5% de la totalité du web.

DEEP WEB

Représente les pages web qui ne sont pas directement accessibles ou non indexées par les moteurs de recherches classiques.
Cela s'explique par différents points : **des pages dont aucun lien ne pointe vers celles-ci ; seulement accessibles via une authentification ; expressément non indexées par les moteurs de recherches** (via le fichier robots.txt) ou encore des types de fichiers non lisibles par les moteurs de recherche.

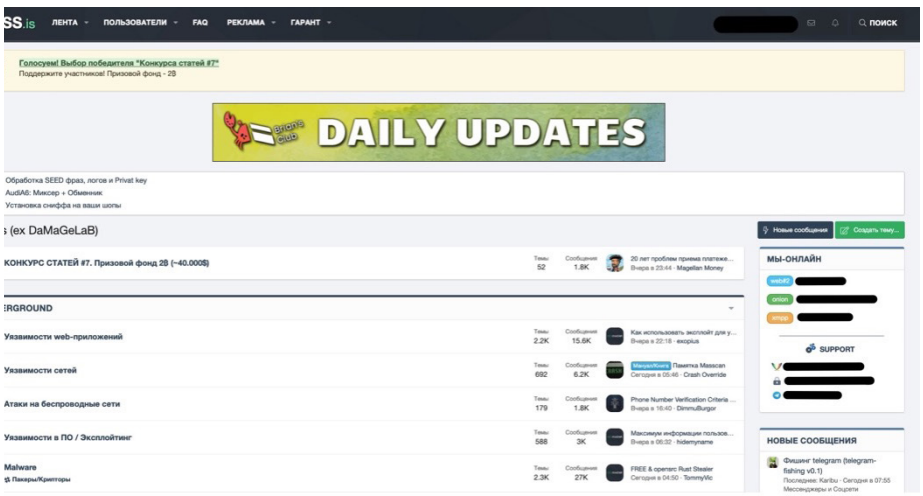
DARK WEB

Le Dark Web est aussi vieux qu'Internet, il existe plusieurs tentatives de définition du "Dark Web", toutefois il est communément admis par les experts en sécurité que le **Dark Web est un ensemble de réseaux anonymes, aussi appelés "Dark Nets" (tel que Tor, I2P, Freenet), permettant d'accéder à du contenu qui leur**

FORUMS VS BLACK MARKETS

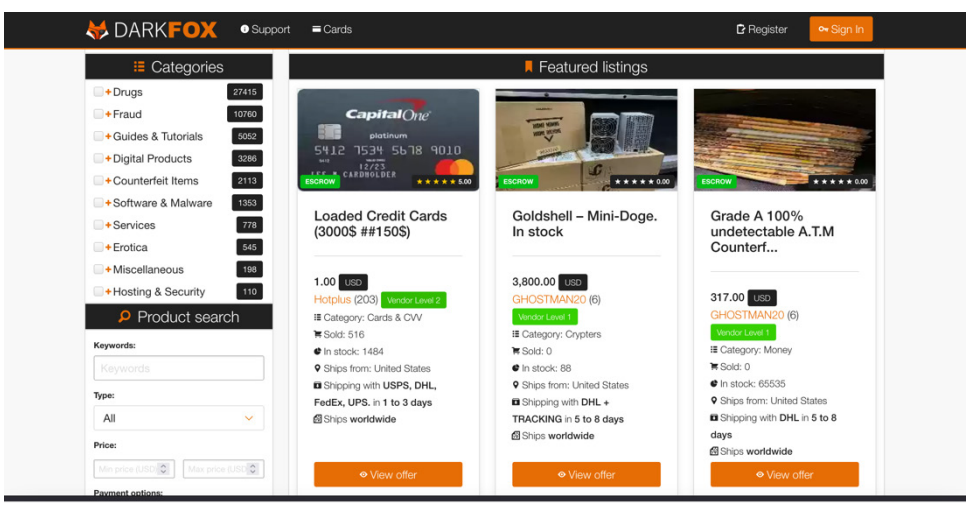
Deux grandes catégories de sites sont particulièrement représentées dans ces réseaux : les Forums et les Marketplace (ou Blackmarkets) :

Les forums sont des espaces communautaires, abordant des discussions en tout genre (actualités, faits divers, conseils en informatique, art, sexualité, etc.) et où le partage de ressources (tutoriels, comptes piratés, etc.) est très présent. Certains de ces forums permettent également l'achat et la vente de produits de "la main à la main", c'est à dire de manière non automatisée, via échange de messages privés, à la manière de ce que l'on peut voir sur des sites comme LeBonCoin.



Aperçu du forum XSS

Les Blackmarkets assimilés à des "Ebay ou des Amazon du Dark Web", sont des boutiques quasiment complètement automatisées : dépôt de monnaie sur la plateforme (Bitcoin, Monero), blocage de l'argent le temps de la livraison ("escrow"), système de notes et avis, achat/vente et livraison en quelques clics.



Aperçu du blackmarket DarkFox

Démystifions le Dark Web

Le "Dark Web", amalgamé parfois avec le "Deep Web" soulève pléthore de fantasme depuis plusieurs années.

Parmi les mythes les plus connus :

IL EST COMPLIQUÉ D'ACCÉDER AU DARK WEB

ON NE TROUVE QUE DES CHOSES ILLÉGALES SUR LE DARK WEB

LE DARK WEB EST LE MARCHÉ NOIR D'INTERNET

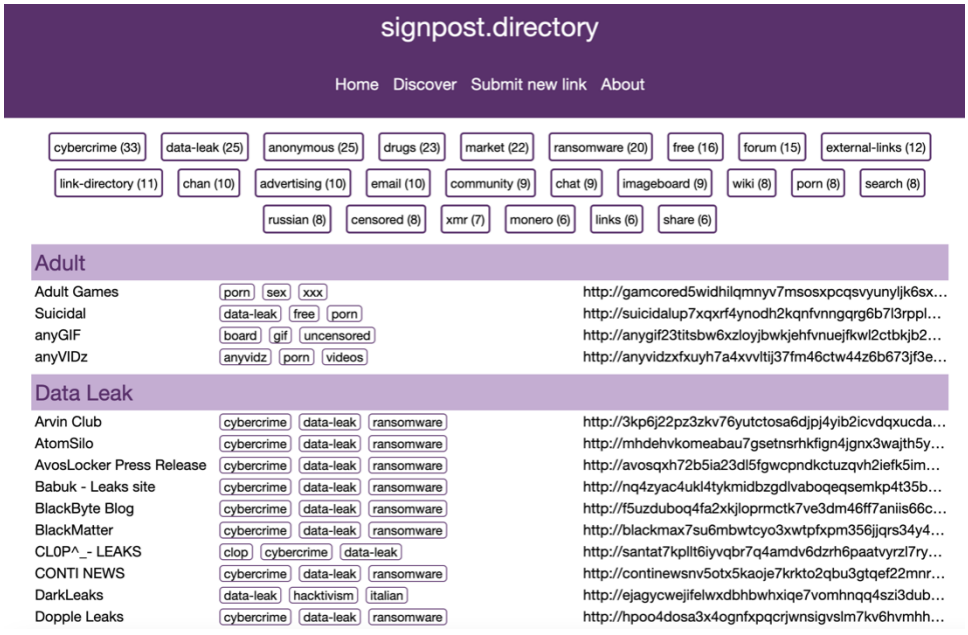
SUR LE DARK WEB LES PIRATES SONT ANONYMES ET AGISSENT EN TOUTE IMPUNITÉ

Il est compliqué d'accéder au Dark Web
Faux

Par définition les sites du Dark Web ne sont pas référencés par les moteurs de recherche tel que Google, ainsi **il faut souvent disposer de l'adresse exacte du site et du navigateur approprié.** Toutefois, **il est très facile de trouver sur le web « traditionnel » des guides, des annuaires et des sites répertoriant des liens du Dark Web (HiddenWiki).** Quelques ébauches de moteurs de recherche spécifiques au Dark Web existent également.

La particularité de ces réseaux est le caractère éphémère des sites, ainsi un site peut être en ligne quelques semaines, ou quelques jours puis disparaître du jour au lendemain. Cela peut s'expliquer par l'illégalité de certains sites, des places de marchés qui ont pour but de "partir avec la caisse" une fois devenues assez populaires.

La principale difficulté au sein de ces réseaux est la nécessité de réaliser une veille quotidienne afin de maintenir son annuaire à jour.



Aperçu du blackmarket DarkFox

On ne trouve que des choses illégales sur le Dark Web

Faux

Initialement, le Dark Web est même bien loin de ne proposer que des contenus illégaux ou tendancieux. La navigation sur les contenus du Dark Web et l'utilisation de ces réseaux anonymes **permettent ainsi à de nombreux opposants de régimes totalitaires ou restreignant la liberté d'expression (Corée du Nord, Chine,...) d'éviter la censure** et d'accéder à des ressources et des contenus sans être traqués par les autorités.

La navigation « anonymisée » est ainsi souvent citée comme l'un des facteurs ayant favorisé l'émergence du printemps arabe.
Certaines ONG proposent même des formations et des tutoriels sur l'utilisation de ses outils afin d'éviter la censure.

De nombreux sites sur le Dark Web n'ont rien à voir avec du contenu illégal. Ces réseaux permettent d'héberger de nombreux sites d'activistes (neutralité du net, théories conspirationnistes, etc.).


REPORTERS SANS FRONTIERES
POUR LA LIBERTÉ DE L'INFORMATION

NOS ACTIONS ENGAGEZ-VOUS Assistance et services Qui sommes-nous ?

ACTUALITÉS

25 avril 2014 - Mis à jour le 25 janvier 2016

Reporters sans frontières et Torservers.net, partenaires contre la surveillance et la censure en ligne

Reporters sans frontières et Torservers.net s'associent pour créer et maintenir 250 serveurs supplémentaires au sein du réseau Tor.

Aperçu d'une publication de Reporter Sans Frontière soutenant le réseau Tor

Par ailleurs, **un grand nombre de sites populaires (Facebook, le moteur de recherche DuckDuckGo, Wikileaks...) disposent de « versions Dark Web ».**

Enfin, c'est aussi un mode de fonctionnement pour certains activistes ou influenceurs inquiétés par les risques de l'Internet traditionnel quant à la protection de la vie privée et des informations personnelles.


"O" Rue 89 Newsletters Services La Conjugaison Espace abonnés Applications

L'OBS avec Rue89

NOS VIES INTIMES LA VIE MATÉRIELLE NOTRE ÉPOQUE MOOC RUE89

L'Obs > Rue89 > Médias

ProPublica, « premier site d'info majeur du Dark Web »

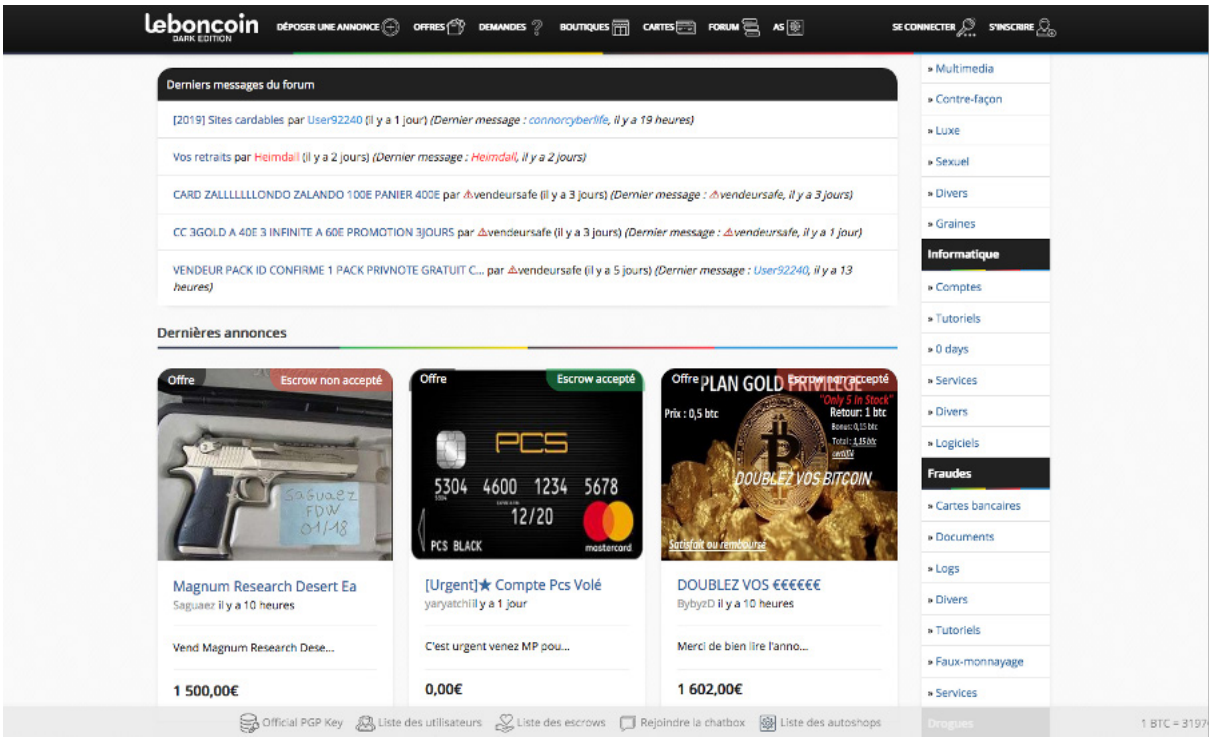
La petite phrase est tracée au feutre bleu sur un tableau de la rédaction de ProPublica, organisme indépendant non lucratif qui verse dans le journalisme d'investigation. Elle est tirée de Wired, qui expliquait jeudi 7 janvier pourquoi le...

Aperçu d'un article de l'Obs présentant ProPublica un site d'information également présent sur le Dark Web

Le Dark Web est le marché noir d'internet
Vrai

Le Dark Web, reste le lieu de prédilection pour tous ceux qui ont des choses à cacher ou se livrent à des commerces illégaux : drogues, piratage informatique, armes, pédophilie...

Il a récemment été évoqué dans les médias les fermetures de certaines places de marché de masse spécialisée dans le commerce de la drogue, véritables Ebay ou Amazon du Dark Web. Cependant, celles-ci sont souvent vite remplacées et des forums plus discrets proposant de la drogue, des armes, des données personnelles volées ou des services de piratage sont légion.



Aperçu du blackmarket LeBonCoin Dark Edition

Sur le Dark Web les pirates sont anonymes et agissent en toute impunité
Vrai et Faux

On pourrait croire en effet qu'il est très difficile de s'immiscer dans ces réseaux (ex: TOR) et il est vrai qu'ils garantissent un anonymat très satisfaisant. Néanmoins, cet anonymat peut vite être levé lorsqu'on manque de vigilance. Comme le démontrent les fermetures et démantèlements de certains sites, les autorités (police, services de renseignement) sont-elles aussi très actives sur le Dark Web et cherchent à s'infiltrer comme elles pourraient le faire dans le monde physique. On peut notamment penser aux démantèlements de :

• 2022/01 :
Raidforums, démantèlement réalisé dans le cadre de l'opération « Tourniquet » en coopération avec le Department of Justice des Etats-Unis, Europol, le Royaume-Uni, la Suède, le Portugal et la Roumanie

• 2018/06 :
La Main Noire (The Black Hand) démantèlement réalisé grâce à des techniques d'ingénierie sociale par la police française ayant infiltré le blackmarket

• 2017/07 :
Alpha Bay à cause notamment à une mauvaise configuration des envois de mail qui exposait l'adresse email personnelle de l'administrateur. Une enquête de police à suffit à retracer l'individu.

• 2017/07 :
Hansa Market démantelé grâce à la prise de contrôle des serveurs via une enquête judiciaire chez l'hébergeur

Les pirates et malfaiteurs commettent également des erreurs et certains journalistes d'investigation comme Brian Krebs se sont fait une spécialité de traquer ces individus en liant leur activité dans le web visible et le web invisible.

Par ailleurs, et bien que probablement peu utilisées due à leur complexité de mise en oeuvre, il existe des attaques permettant de réduire l'anonymat au sein de TOR, on peut citer :

- **Defcon 2016 : Deanonymizing Tor**
- **2016 : DefecTor - The Effect of DNS on Tor's Anonymity**
- **2014 : Traffic correlation using netflows**

2. Comment accéder au Dark Web ?

CES DIFFÉRENTS « DARK WEB » PROPOSENT CHACUN UN LOGICIEL PERMETTANT D'ACCÉDER À LEUR CONTENU. AINSI IL SUFFIT D'EXÉCUTER LE LOGICIEL POUR ACCÉDER AU RÉSEAU.

3 vecteurs d'attaque privilégiés par les attaquants.

TOR

Le réseau privé Tor est le Dark Net le plus connu et médiatisé, il compte environ **90% des utilisateurs**. Celui-ci permet d'accéder aux sites en .onion (TLD) auxquels un navigateur classique ne saurait se connecter. Pour cela Tor propose le logiciel « Tor Browser » dispoible sur Windows, Mac, Linux et Android. C'est en réalité un navigateur web (dérivé de Mozilla Firefox) couplé à un proxy donnant l'accès au réseau.

https://www.torproject.org/

I2P

Semblable à TOR, I2P est un réseau anonyme comptant environ **6% des utilisateurs**, se présentant sous la forme d'une couche logicielle permettant à un ensemble d'applications (p2p, IRC, navigateur internet, client mail...etc.) de se connecter au réseau privé de manière chiffrée. À l'instar de Tor, il possède également son type de sites web : les eepsites. I2P est également disponible sur Windows, Mac, Linux et Android.

https://geti2p.net/

FREENET

Freenet compte **4% des utilisateurs**, c'est un espace de stockage partagé et distribué (pair à pair chiffré), il est ainsi très différent de Tor et I2P. Freenet est run Dark Net reconnu comme très lent et représente le réseau de prédilection pour la publication de documents (pages web, PDF, images, vidéos...) de manière anonyme et résistante à la censure.

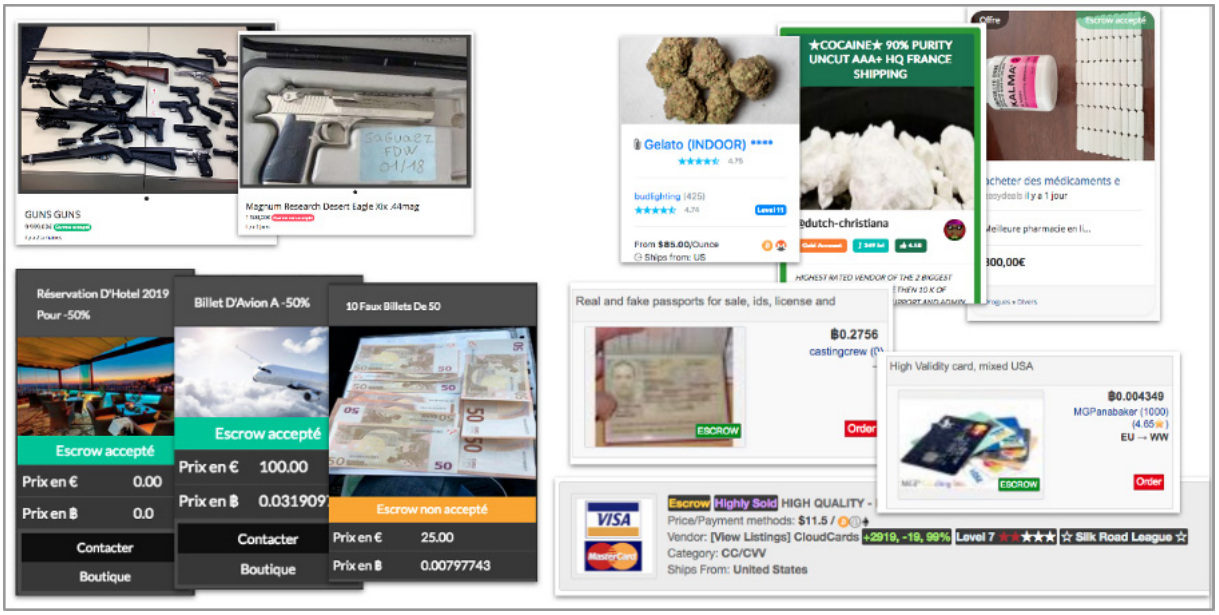
Comme I2P et Tor Freenet est disponible sur Windows, Mac, Linux et Android.

https://freenetproject.org

3. Les enjeux du Dark Web pour XMCO

Ces réseaux contiennent à la fois du contenu légal et illégal. Comme mentionné plus tôt c'est le lieu de prédilection à tout ce qui suppose une forme d'anonymat : journalistes, dissidents, lanceurs d'alertes, pirates, trafiquants.

- Armes de poing, armes de guerre
- Vente de faux documents
- Produits de contrefaçon
- Vente de drogue (cannabis, cocaïne, MDMA, etc.)
- Vente de cartes bleu (CC, CVV), comptes Paypal, etc.
- Vente de comptes compromis (e-commerce)
- Tutoriels divers et variés (ouvrir un compte bancaire anonymement, techniques de monétisation, carding etc.)



Aperçu des types de produits disponibles à la vente sur le Dark Web

Dans le cadre de Serenety, notre service de Cyber Threat Intelligence, ces recherches sur le Dark Web ont plusieurs enjeux :

- L'identification de la vente de comptes collaborateurs clients piratés afin de détecter des intrusions et contrer des attaques en cours (Phishing, intrusion, etc.).
- Les discussions à propos de nos clients afin de détecter des attaques en cours de préparation.
- Le vente de données clients confidentielles.

4. Les analystes VS le Dark Web : Comment procé-dons-nous ?

Les analystes du CERT-XMCO effectuent **une veille quotidienne sur un grand nombre de plateformes du Deep Web et du Dark Web à la recherche de données clients et de bases de données compromises.** À ce titre, pour l'année écoulée, **nous avons établi une présence sur plus de 150 plateformes.** Mais, étant donné le caractère très volatile de celles-ci, à la fois quant à leur apparition, que leur disparition, il est nécessaire de **tenir un annuaire à jour et de rechercher de manière permanente des nouvelles sources (blackmarkets et forums).**

Également, au-delà de cette surveillance, **nos analystes échangent de manière quotidienne avec les attaquants** dans le but d'**obtenir des informations pertinentes sur des ventes de données volées** ou tout simplement pour nous permettre de maintenir cette présence sur ces forums et marketplaces.

Les efforts des analystes sont aussi concentrés vers l'**infiltration de zones plus restreintes au sein de ces plateformes**, dans l'objectif d'accéder à des données ou conversations plus pertinentes concernant nos clients.

Sur 7 500 alertes envoyées cette année à nos clients, 677 concernaient des fuites d'informations sensibles et 103 d'entre elles ont été le fruit de ces recherches sur le Dark Web.

Par ailleurs, **cette veille permanente a permis de collecter et d'indexer 7,5 milliards de comptes compromis au sein de notre plateforme d'indexation.**

L'équipe Serenety, accompagne les entreprises de toutes tailles dans l'anticipation des menaces émanent du Dark Web.

Elle effectue une surveillance continue sur le Dark Web pour identifier les informations échangées ou vendues qui vous concernent.

Accéder au webinar «les analystes du CERT-XMCO contre-attaquent» Épisode 1 : le retour du Dark Web

Accéder au webinar «les analystes du CERT-XMCO contre-attaquent» Épisode 2 : l'ascension des nouvelles menaces

Surveillance du Dark Web avec Serenety

L'équipe Serenety, accompagne les entreprises de toutes tailles dans l'anticipation des menaces émanent du Dark Web. Elle effectue une surveillance continue sur le Dark Web pour identifier les informations échangées ou vendues qui vous concernent.

LA SURVEILLANCE DE VOTRE SURFACE D'ATTAQUE (IP, DNS) NOUS PERMET :

- L'identification des systèmes exposés ou vulnérables
- La découverte de nouveaux assets
- Le suivi de l'obsolescence et de l'expiration de vos systèmes
- L'identification du niveau de risque de vos assets (présence sur des sites de phishing, sur des blacklists...)
- L'identification des nouvelles menaces sur votre périmètre (failles 1day)

LA SURVEILLANCE DE VOTRE SURFACE D'EXPOSITION (MOTS-CLÉS SUR LE WEB, DEEP WEB ET DARK WEB) NOUS PERMET :

- Identification du shadow IT (maîtrise et contrôle de votre périmètre)
- Cartographie en continu de l'évolution de votre périmètre
- Surveillance des réseaux sociaux et des forums ou market places
- Identification des fuites de données sensibles ou critiques pour votre organisation

LA RECHERCHE AUTOMATISÉE ET L'ANALYSE HUMAINE

Nos recherches automatisées font l'objet d'une corrélation, d'une analyse et d'un tri pour éliminer les faux positifs.

Les analystes envoient des alertes lorsqu'il y a un risque avéré ainsi que des recommandations pour prendre des mesures immédiates pour se prémunir des risques. Ces alertes sont intégrées sur votre dashboard de suivi ou injectées sur votre outil via notre API.

SUIVI DES RISQUES ET PILOTAGE SÉCURITÉ

- Suivi des contrôles après correction
- Suivi des corrections liées aux menaces 0-day
- Visualisation des indicateurs et tableaux de bords
- Notes d'analyses contextualisées sur les groupes d'attaquants ou les modes opératoires

Cette méthodologie permet d'éviter un grand nombre de risques tels que : le vol et fuite de données, l'atteinte à l'image et l'usurpation d'identité, la fraude, les planifications d'attaque…

Demandez votre démonstration

Retour d'expérience Serenety

« Il est difficile de protéger ce qu'on ne connaît pas. Notre activité nous impose une exposition sur internet. Nous ne pouvons pas nous mettre dans un bunker. Ce serait contraire à nos services de smart city et services aux usagers. »

L'une des pistes envisagées était donc d'améliorer leur connaissance des interfaces exposées et de leur configuration.

Il nous fallait une solution qui nous permette de « surveiller notre exposition, mettre en exergue tout ce qu'on ne connaissait pas, connaître nos principales menaces et avoir une connaissance de ce qui est exposé et comment ».

Yohann Guiot, RSSI et DPO Groupe

FLOWBIRD
Urban
Intelligence

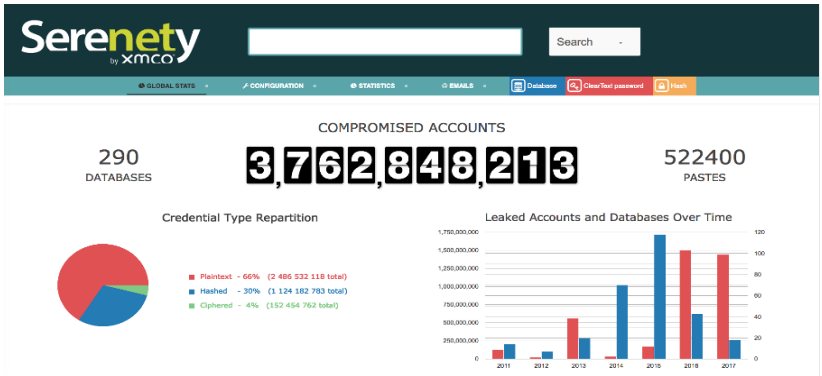
Lire le retour d'expérience complet

5. Quelles sont les données vraiment pertinentes ?

PARMI LA TOTALITÉ DES ALERTES ENVOYÉES PAR LE CERT-XMCO, ON PEUT CLASSER 6 TYPES D'ALERTES.

1 COMPTES COLLABORATEURS COMPROMIS

Depuis la création de cet outil d'indexation, XMCO a été en mesure de récupérer et d'indexer 7,5 milliards de comptes compromis



Aperçu de notre outil d'indexation de comptes compromis

2 VENTE D'ACCÈS À DES SITES WEB COMPROMIS

Au cours de nos investigations, nous avons constaté 5 accès à des sites web client compromis, à la vente. Il s'agissait d'accès SQL ou Administrateur, et également la vente de vulnérabilités.

Aperçu des annonces de vente d'accès à des sites web compromis

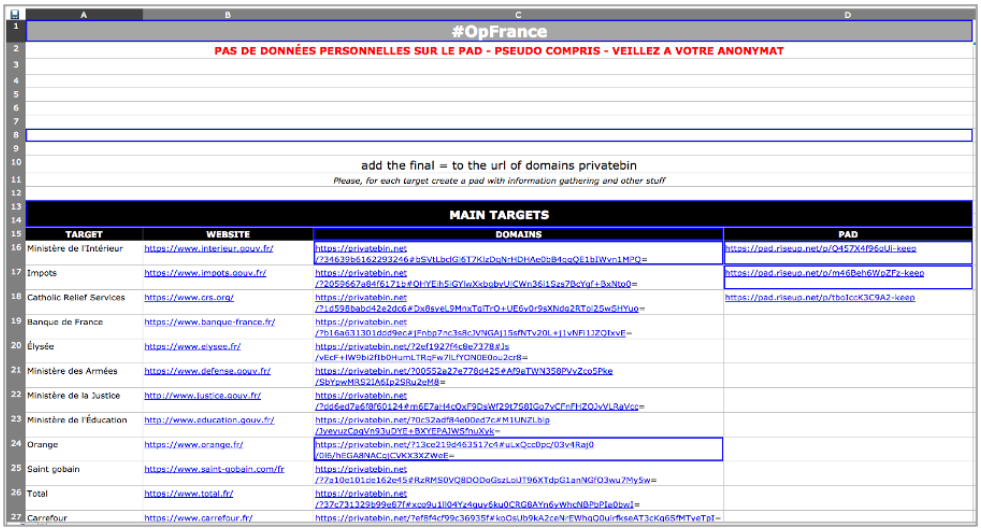
3 FICHIERS CONFIDENTIELS À LA VENTE

Nous avons comptabilisé plus de 2000 fichiers confidentiels affectant nos clients à la vente sur le Dark Web, tel que des contrats, documents stratégiques ou documents techniques.

Aperçu d'une vente de documents confidentiels

4 ATTAQUES EN COURS ET SUIVIS EN TEMPS RÉEL

Cette présence sur le Dark Web a également permis de détecter des attaques en cours à l'encontre de nos clients, et de suivre en temps réel la progression des attaques. Ces éléments ont permis à nos clients d'organiser les efforts de défense afin de contrer les attaques en cours.



#OpFrance

PAS DE DONNÉES PERSONNELLES SUR LE PAD - PSEUDO COMPRIS - VEILLEZ A VOTRE ANONYMAT

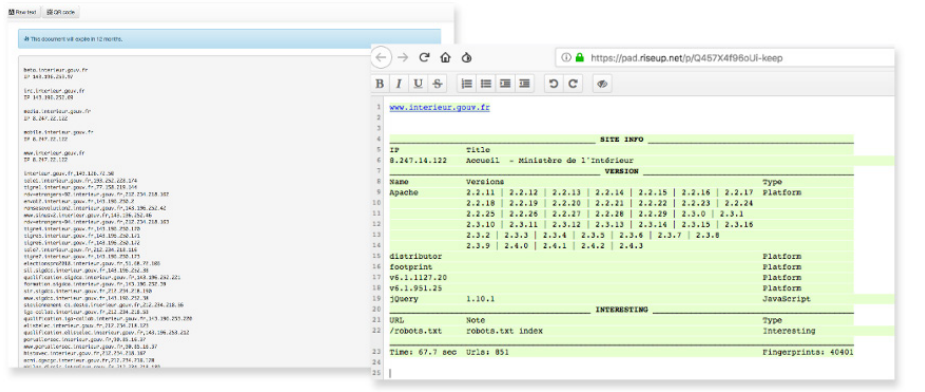
add the final = to the url of domains privatebin

Please, for each target create a pad with information gathering and other stuff

MAIN TARGETS

TARGET	WEBSITE	DOMAINS	PAD
Ministère de l'Intérieur	https://www.interieur.gouv.fr/	https://privatebin.net/?2f4639b61622932462#bSVtLbdGi6T7KizDqNrHDHAe0bB4qqQE1biWvn1MPQ=	https://pad.riseup.net/p/Q457X4f96oUi-keep
Impots	https://www.impots.gouv.fr/	https://privatebin.net/?2059566?a84f6171#QHYEIh5iGYIwXsbqbyUiCWn36i1Gzs7BcYqf+BxNtq0=	https://pad.riseup.net/p/m46Beh6WpZFz-keep
Catholic Relief Services	https://www.crs.org/	https://privatebin.net/?1d598babd42e2dc6#Dx8sveL9MnxTqITrO+UE6v0r9sXNdg2RTpi25wSHYuo=	https://pad.riseup.net/p/tbo1ccK3C9A2-keep
Banque de France	https://www.banque-france.fr/	https://privatebin.net/?b16a631301ddd9ec#jFnhp7nc3sRcJVNGAJ15efNTv20L+j1vNFi1JZQfxvE=	
Élysée	https://www.elysee.fr/	https://privatebin.net/?2ef1927f6c8e7378#Js/vEcF+IW9bi2fIbDHumLTRqFw7lJYQN0E0ou2cr8=	
Ministère des Armées	https://www.defense.gouv.fr/	https://privatebin.net/?00552a27e778d425#Af9qTWN358PvyZcoSPke/SbYewH8S2IA6Ip2SRu2eM8=	
Ministère de la Justice	http://www.justice.gouv.fr/	https://privatebin.net/?qd6ed7a6f0f60124#m6E7aiH4cQxf9DaWf29t7S01Go7vCFnFhIZOJvVLRaVcc=	
Ministère de l'Éducation	http://www.education.gouv.fr/	https://privatebin.net/?0c52adf84e00ed7c#M1UNZLhjp/IyeyuzCqgVn93uDYE+BXYEPAIWSfnuXyk=	
Orange	https://www.orange.fr/	https://privatebin.net/?13ce219d463517c6#uLxQcc0pc/03v4Raj0/0l6/hfGA8NACqCVKK3X2WoE=	
Saint gobain	https://www.saint-gobain.com/fr	https://privatebin.net/?7a10c101e162ef5#RzRMS0VQ8OODoGszLoUT96XTdpG1anNGfO3wu7MySw=	
Total	https://www.total.fr/	https://privatebin.net/?37c731329b99e87f#xcp9u1ll04Yz4guy5ku0CRG8AYn6yWhcNBPbPIa0bwI=	
Carrefour	https://www.carrefour.fr/	https://privatebin.net/?ef8f4cf99c36935f#koOsUb9kA2ceNrEWhqQOuirfkseAT3cKq65fMTveTpI=	

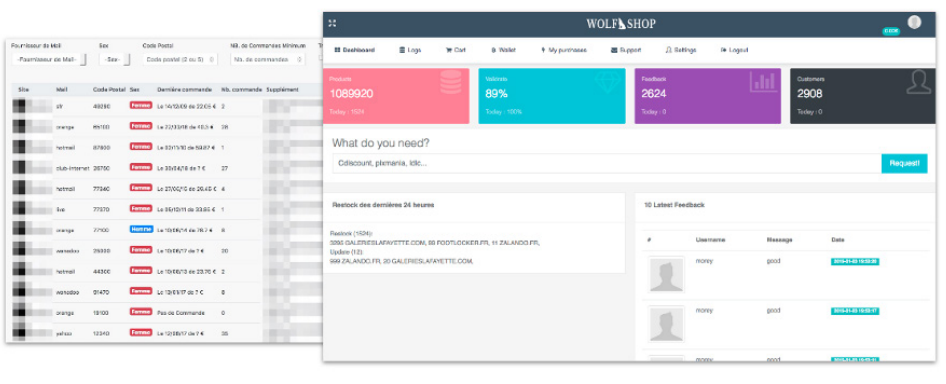
Aperçu d'un document d'organisation de l'OpFrance de décembre 2018



Documents de travail de l'OpFrance de décembre 2018

5 1 100 000 COMPTES CLIENTS À LA VENTE (B2C)

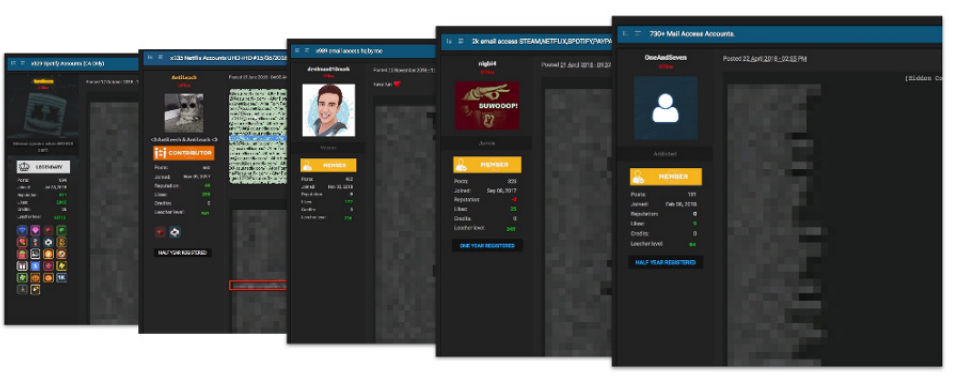
Nos clients dans le secteur du e-commerce B2C sont particulièrement affectés par la vente de comptes clients. Ces comptes ayant du vécu sur leurs plateformes et parfois des moyens de paiement pré-enregistrés sont alors réutilisés par les attaquants afin de légitimer certains achats frauduleux (carding). Dans cette optique, nous avons détecté plus d'1 million de comptes à la vente affectant les clients d'XMCO.



Aperçu de la vente de comptes e-commerce sur les blackmarkets Wolf Shop et House of Cards

6 CENTAINE DE COMPTES COLLABORATEURS PARTAGÉS QUOTIDIENNEMENT

Outre la vente de compte, le partage de comptes piratés est également bien ancré. Il s'agit de partage de comptes pour des produits du quotidien (Netflix, Spotify, Steam, etc.), il n'est pas rare d'y retrouver des adresses email professionnelles. Il n'est également pas rare qu'un collaborateur utilise un même mot de passe pour plusieurs services, y compris ceux du quotidien et ceux de l'entreprise, ouvrant ainsi une porte d'entrée sur le SI.



Aperçu de partages de comptes collaborateurs

Pour conclure, le Dark Web contient énormément de données, pour la plupart concernant des problématiques étatiques (drogues, armes à feu, usurpation d'identité, etc.). Ainsi, l'enjeu sur le Dark Web n'est pas d'accéder à l'intégralité des informations, mais de naviguer parmi les 99% de bruit, afin de trouver le 1% de pépites. Cela implique un traitement massif de données tout en tenant compte du contexte, c'est dans cet objectif que réside l'expertise d'XMCO sur le Dark Web.

Remerciements :

Charles DAGOUAT
Adrien GUINAULT
Charlène GREL
Julien TERRIAC
et Paloma SIGGINI

À propos de

serenety
By xmco

Créée en 2010, Serenety est un service de Cyber Threat Intelligence, développé par le CERT-XMCO et à destination des organisations publiques et privées. Son objectif est d'identifier la surface d'attaque et la surface d'exposition des organisations surveillées au travers d'un outil simple d'utilisation et ergonomique. Il se distingue de ses concurrents par la corrélation de ses résultats issus des analyses automatiques des sources ouvertes surveillées et des investigations manuelles de son équipe d'experts qualifiés. Cette surveillance permet d'identifier les menaces et d'anticiper les risques notamment liés aux fuites de données, aux systèmes exposés et vulnérables ou encore à la compromission de comptes.

À propos d'

xmco

Cabinet de conseil indépendant en cybersécurité, depuis 2002, XMCO a à cœur d'accompagner ses clients, de toute taille et de tous secteurs, dans l'anticipation des vulnérabilités, la détection des failles et la réponse à incidents. XMCO est qualifié PASSI sur l'ensemble des portées, ce qui confirme le cœur de métier historique : l'audit et les tests d'intrusion.

Retrouvez-nous

Sur notre site :

www.xmco.fr

Sur les réseaux sociaux :

Envie d'échanger ?

sales@xmco.fr

01 79 35 29 30