Tor envahi par des mouchards ?

Tor envahi par des mouchards ?

Selon des chercheurs, 110 relais du réseau d'anonymisation Tor étaient à la recherche d'informations sur les services cachés auxquels ils permettent d'accéder.

Deux chercheurs de la Northeastern University (Boston), Guevara Noubir et Amirali Sanatinia, démontrent à leur tour que le réseau Tor est la cible d'espions. Cette fois, les chercheurs n'ont pas étudié des noeuds de sortie détournés pour mener des attaques de type *« Man In The Middle »*. Ils se sont intéressés à d'autres relais : ceux qui permettent d'accéder à des services cachés et référencent des éléments clés (adresse en .onion, clé publique, points d'introduction) .

Ces relais (HSDirs, *Hidden Service Directories*) font partie intégrante des services cachés et du dark web. Mais des entités (gouvernements, entreprises, hackers, etc.) peuvent en modifier le code pour obtenir des informations, découvrir une adresse ou exploiter une faille.

Pot de miel

Dans le cadre de leurs travaux, les chercheurs ont déployé 4500 services cachés (en .onion), 72 jours durant. *« Nos résultats expérimentaux montrent que, durant cette période, au moins 110 relais (HSDirs) étaient à la recherche d'informations sur les services cachés qu'ils accueillent »*, soulignent les chercheurs dans une note. Ils ont également indiqué à *Motherboard* que la recherche de vulnérabilités n'est pas exclue des motivations de ceux qui pilotent ces relais. La plupart d'entre eux sont hébergés aux États-Unis, en Allemagne et en France. Mais il est toujours possible d'opérer un serveur à distance…

Roger Dingledine, cofondateur du projet Tor, a expliqué au magazine que peu, voire aucun de ces relais ne se trouvent dans le réseau Tor en ce moment. Le projet travaille, par ailleurs, à la mise en place d'une prochaine génération de services *« onion »*. Quant aux chercheurs, ils présenteront leurs travaux lors de la Defcon 24, qui se déroulera du 4 au 7 août prochains à Las Vegas.

Article original de Ariane Beky

Réagissez à cet article

Original de l’article mis en page : Tor envahi par des noeuds espions ?

Selon Denis Jacopini, le Darknet s’apparente à un marché noir

Bernard Debré, médecin et député LR de Paris, dénonce la simplicité avec laquelle on pourrait acheter des produits stupéfiants sur internet. Denis Jacopini, spécialiste en Protection des données personnelles, cybercriminalité, informatique légale et Sécurité de l'information alerte ceux qui veulent faire un tour sur le côté dark d'Internet.
Interview du 29 juin 2016

https://soundcloud.com/sputnik_fr/denis-jacopini-le-darknet-sapparente-a-un-marche-noir

Pourquoi d'après vous le gouvernement se penche si peu sur le darknet et préfère faire passer loi renseignement qui concerne surtout le coté ouvert d'Internet ?
Qu'est ce que le public doit savoir sur le darknet ?

Est qu'il y a un nombre estimé de personnes qui utilisent le darknet?
12 millions de sites internet pour 1,5 millions à travers le monde.

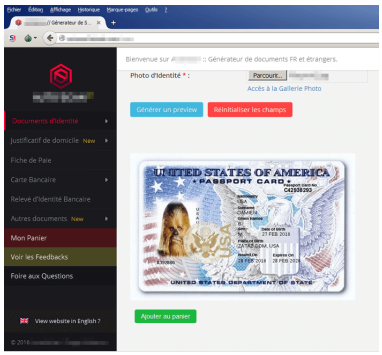
Quels sont les dangers du darknet?

Des experts disent que bientot le darknet sera le refuge de la liberté d'expression, pensez vous que c'est possible que bientot le public « normal » va passer plus de temps sur le darknet que sur le net ouvert ?

Denis JACOPINI répond à ces questions dans cet interview.
Cliquez sur le cercle orange pour faire play

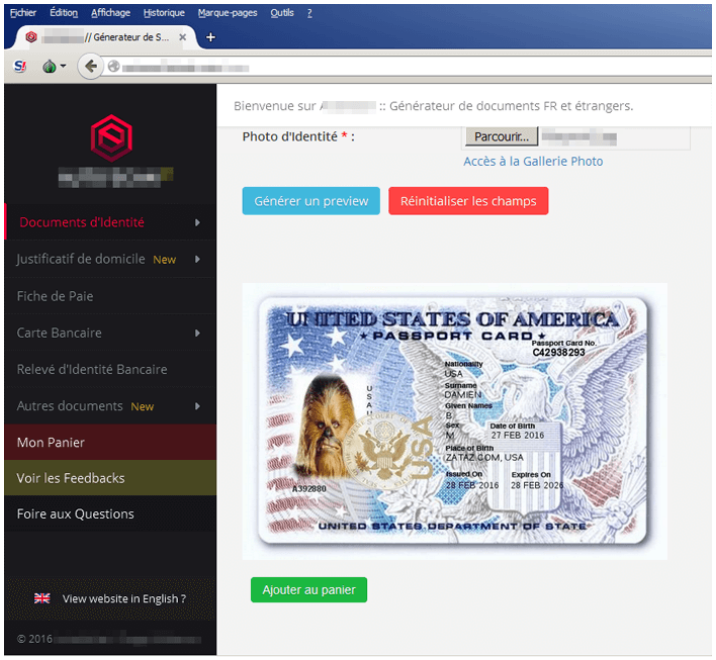
Réagissez à cet article

Le Darknet cache un générateur de faux documents



Le Darknet cache un générateur de faux documents

Vous cherchez de faux documents comme un diplôme du baccalauréat, de BTS ? Une fausse facture FREE, EDF, Direct Énergie ? Un faux permis de conduire ? Une fausse fiche de paie ou une fausse carte bancaire ? Un site Internet vous propose d'automatiser l'usurpation.



Ils sont de petites stars dans le black market, deux francophones devenus des références dans la contrefaçon de documents. Les autorités leurs poseraient bien deux/trois questions, mais les deux administrateurs du portail A.S. [Le nom a été modifié, NDR] sont malins, cachées dans les méandres du darknet. Leur site, pas la peine de me réclamer l'adresse, est caché sous une adresse .onion. A.S. profite de l'anonymat proposé par le service TOR pour éviter d'afficher ouvertement son serveur, son ip d'origine. Et même si vous mettiez la main sur ce dernier, l'hébergement est hors de l'hexagone.

« ***Bienvenue sur A'S. :: Générateur de documents FR et étrangers*** » souligne l'introduction affichée par le site. Mission de ce dernier, pour quelques euros, facturés en Bitcoins, générer de fausses factures, fausses fiches de paie, faux relevé d'identité bancaire (RIB). Il est possible de générer un faux diplôme du Baccalauréat, de BTS, d'IUT. Une fausse carte vitale ? Pas de problème. Une facture d'un achat effectuée chez Darty, ok. Passeport Français, Américain et autres copies d'une carte nationale d'identité boucles ce service… qui n'a rien d'illégal, du moins si vous rentrez vos propres coordonnées. Il en va tout autrement si les informations que vous fournissez permettent d'usurper une identité, une fonction, un titre via ses faux documents. La loi punit de trois ans d'emprisonnement et de 45000 euros d'amende le faux et l'usage de faux documents.

Les prix varient de 4,99€ pour une copie de passeport, une facture. 9,99€ pour le scan d'un bulletin de fiche de paie. 6,99€ pour la copie d'un diplôme du baccalauréat général. Les auteurs de ce business proposent même un abonnement à vie. Pour ~~79 800~~ euros, les commerciaux indiquent permettre « ***un accès illimité et à vie à tous les articles de cet Autoshop pour 200€ ~~BTC~~***« . La boutique annonce un anonymat garanti. [Correction : selon les auteurs, il s'agit de 200€ et non 200 BT comme il était écrit sur leur site, NDR]… [Lire la suite]

Réagissez à cet article

Source : *ZATAZ Générateurs de faux documents – ZATAZ*

Plus de 100 millions de mots de passe LinkedIn dans la nature… depuis 2012 !

	**Plus de 100 millions de mots de passe LinkedIn dans la nature… depuis 2012 !**

Une base de données, contenant 117 millions de combinaisons d'identifiants et de mots de passe, est vendue 2000 euros par des pirates. Le réseau social professionnel enquête.

Le piratage massif dont a été victime LinkedIn en 2012 revient hanter le réseau social professionnel. Une base de données contenant plus de 100 millions d'identifiants et de mots de passe est actuellement proposée à la vente sur une place de marché du dark web, «The Real Deal», rapporte le siteMotherBoard. Le fichier est proposé à la vente pour 5 bitcoins, soit un peu plus de 2000 euros. Il concerne 167 millions de comptes, dont 117 millions sont associés à un mot de passe.

Le site LeakedSource, qui a eu accès au fichier, assure avoir réussi à déchiffrer en trois jours «90% des mots de passe». Ils étaient en théorie protégés par un procédé de hachage cryptographique, SHA-1, mais sans salage, une technique compliquant leur lecture en clair. Deux personnes, présentes dans le fichier, ont confirmé à un chercheur en cybersécurité que le mot de passe associé à leur identifiant était authentique.

LinkedIn avait reconnu en 2012 le vol des données de connexion, mais sans jamais préciser le nombre d'utilisateurs concernés. Un fichier, concernant 6,5 millions de comptes, avait à l'époque été mis en ligne. «À l'époque, notre réponse a été d'imposer un changement de mot de passe à tous les utilisateurs que nous pensions touchés. De plus, nous avons conseillé à tous les membres de LinkedIn de changer leurs mots de passe», commente aujourd'hui le réseau social professionnel sur son blog.

123456, linkedin, password, 123456789 et 12345678

En réalité, un porte-parole de LinkedIn avoue «ne pas savoir combien de mots de passe ont alors été récupérés». «Nous avons appris hier qu'un jeu de données supplémentaire qui porterait supposément sur plus de 100 millions de comptes et proviendrait du même vol de 2012, aurait été mis en ligne. Nous prenons des mesures immédiates pour annuler ces mots de passe et allons contacter nos membres. Nous n'avons pas d'éléments qui nous permettent d'affirmer que ce serait le résultat d'une nouvelle faille de sécurité», ajoute LinkedIn sur son blog.

Selon LeakedSource, la base de données aurait été détenue jusqu'alors par un groupe de pirates russes. Ces informations de connexion, même si elles remontent à 2012, ont encore une grande valeur. Elles peuvent être utilisées tout à la fois pour pénétrer dans d'autres comptes plus critiques (sites d'e-commerce, banque en ligne…) ou organiser des campagnes de phishing, une technique utilisée pour obtenir les renseignements personnels d'internautes. Nombre d'utilisateurs utilisent la même combinaison d'adresse email et de mot de passe sur tous les sites, et en changent peu souvent, ce qui démultiplie les effets de tels piratages.Preuve de cette imprudence générale, les cinq mots de passe les plus utilisés dans le fichier mis en vente étaient 123456, linkedin, password, 123456789 et 12345678… [Lire la suite]

Réagissez à cet article

Source : *Plus de 100 millions de mots de passe LinkedIn dans la nature*

Retrouvrer les traces d’une attaque informatique peut s’avérer complexe et coûteuse

Retrouvrer les traces d’une attaque informatique peut s’avérer complexe et coûteuse

---

Selon l'un des principes fondamentaux de la police scientifique, sur une scène de crime, tout contact laisse une trace. Dans l'univers de la cybercriminalité, chercher les traces pour remonter le fil des événements jusqu'à l'auteur de l'attaque, se révèle souvent compliqué.

Lorsqu'un incident survient, il est généralement difficile pour l'entreprise de définir qui a accédé à son système d'information et ce que cette personne – ou groupe de personnes – a fait. La tâche se complique encore un peu plus lorsque cet incident provient d'utilisateurs internes bénéficiant d'un haut niveau de privilèges sur le système – voire même de la personne en charge de prévenir les attaques sur le réseau.
Que l'incident soit le résultat d'une action malveillante d'un utilisateur interne, d'une erreur humaine ou d'une faille, dès lors que l'entreprise n'est pas capable de remonter les informations, elle passe à côté de preuves cruciales, et rend l'enquête beaucoup plus longue et onéreuse.

Le facteur temps : la clé de la réussite
Dans toutes investigations post-incident de sécurité, le temps est un facteur crucial. Pour mener à bien une enquête, il est plus facile, plus précis et généralement moins couteux de conduire une analyse criminalistique, dite forensics, poussée immédiatement, plutôt que plusieurs semaines voire plusieurs mois après l'incident.
L'examen approfondi des logs : remonter les étapes d'une attaque
Lorsqu'une faille est avérée, l'entreprise dépend des logs générés par les terminaux et les applications sur le réseau, pour déterminer la cause initiale et remonter les étapes de l'attaque. En pratique, trier les informations peut prendre des jours – en d'autres termes, cela revient à chercher une aiguille dans une botte de foin.
L'intégrité des logs : le respect du standard des preuves
Si les logs ont été modifiés et qu'ils ne peuvent pas être présentés dans leur format original, l'intégrité des données de logs peut être remise en question lors d'une procédure légale. Les logs doivent respecter le standard légal des preuves, en étant collectés de manière inviolable. A contrario, les logs qui ont été modifiés ou qui n'ont pas été stockés de manière sécurisée, ne seront pas acceptés comme preuve légale dans une cour de justice.
Cependant, même pour les organisations qui ont implémenté des solutions fiables de collecte et de gestion des logs, l'information cruciale peut manquer et ce chainon manquant peut empêcher l'entreprise de reconstituer tout le cheminement de l'incident et ainsi de retrouver la source initiale du problème.

Les comptes à privilèges : une cible fructueuse pour les cybercriminels
En ciblant les administrateurs du réseau et autres comptes à privilèges qui disposent de droits d'accès étendus, voire sans aucune restriction au système d'information, aux bases de données, et aux couches applicatives, les cybercriminels s'octroient le pouvoir de détruire, de manipuler ou de voler les données les plus sensibles de l'entreprise (financières, clients, personnelles, etc.).

L'analyse comportementale : un rempart nouveau pour les entreprises
Les nouvelles approches de sécurité basées sur la surveillance des utilisateurs et l'analyse comportementale permettent aux entreprises d'analyser l'activité de chacun des utilisateurs, et notamment les événements malveillants, dans l'intégralité du réseau étendu.
Ces nouvelles technologies permettent aux entreprises de tracer et de visualiser l'activité des utilisateurs en temps réel pour comprendre ce qu'il se passe sur leur réseau. Si l'entreprise est victime d'une coupure informatique imprévue, d'une fuite de données ou encore d'une manipulation malveillante de base de données, les circonstances de l'événement sont immédiatement disponibles dans le journal d'audit, et la cause de l'incident peut être identifiée rapidement.
Ces journaux d'audit, lorsqu'ils sont horodatés, chiffrés et signés, fournissent non seulement des preuves recevables légalement dans le cadre d'une procédure judiciaire, mais ils assurent à l'entreprise la possibilité d'identifier la cause d'un incident grâce à l'analyse des données de logs.
Lorsque ces journaux sont complétés par de l'analyse comportementale, cela offre à l'entreprise une capacité à mener des investigations forensics beaucoup plus rapidement et à moindre coût, tout en répondant pro activement aux dernières menaces en temps réel… [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Liberté) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Recouvrer les traces d'une attaque informatique : l'investigation peut s'avérer complexe et coûteuse – JDN*

Comment s'introduire dans le web invisible ?

Comment s'introduire dans le web invisible ?

La façon la plus répandue et la plus simple de s'introduire dans cette partie immergée du web est le serveur Tor, acronyme pour The Onion Router. Pourquoi oignon ? Parce que le logiciel assure plusieurs couches de protection, qui permettent entre autres de conserver l'anonymat de l'internaute.

Tous les sites qui ont cours sur ce moteur de recherche se terminent par .onion. L'étudiant en informatique qui a accepté de faire une démonstration à L'Express affirme qu'à toutes les fois qu'une personne brassant des affaires sur le «*deep web*» fait une requête, elle ne passe jamais par le même chemin afin de brouiller les pistes.
«Tout le monde se connecte sur un même serveur et une fois que tu es connecté sur ce serveur, tu passes par un réseau de connections international, explique-t-il. Tu as un serveur d'entrée et un serveur de sortie. Ce qui se passe entre, on ne le sait pas. Ton adresse IP se perd. »

Un enseignant en informatique au Cégep de Drummondville, Louis Marchand, abonde également en ce sens : «Si la personne est excessivement prudente dans ses démarches, la seule chose qui pourrait être retracée serait sa connexion au réseau Tor. Toutes les actions, légales ou pas, que cette personne a pu effectuer à l'intérieur du serveur sont pratiquement introuvables.» Pratique lorsqu'on veut publier des anecdotes sur un blogue en évitant la censure… ou pour publier une offre d'achat de cocaïne.
Ce moteur de recherche, développé par la marine américaine, se télécharge aussi facilement que Google Chrome et est associé avec le moteur Firefox. Comme quoi Tor n'est pas illégal du tout : «c'est l'utilisation qu'on en fait qui peut être négative», complète l'étudiant.

Les bitcoins, la monnaie virtuelle anonyme
La monnaie ayant cours sur le web invisible est le *bitcoin*, une forme d'argent virtuelle cryptée. Elle n'est soumise à aucun taux de change ni à aucune banque, donc aucun intermédiaire n'existe entre l'acheteur et la marchandise. Cependant, son atout majeur pour les consommateurs de produits illicites est qu'elle peut être utilisée de façon anonyme.
Louis Marchand décrit le bitcoin comme n'étant rien d'autre qu'un fichier. «Il faut faire attention à ça : toutes les transactions sont enregistrées, même si le bitcoin en tant que tel n'est pas identifié. C'est beaucoup plus difficile de retracer de l'argent liquide, puisque absolument rien ne lie un 20 $ à son propriétaire», spécifie-t-il.

Selon l'enseignant, le bitcoin fonctionne exactement comme l'or ou le diamant. «Ce qui diffère, c'est que quelque chose de virtuel change beaucoup plus rapidement que n'importe quelle ressource physique. Demain, un bitcoin peut valoir 2 $ et le lendemain, plus de 2000 $. C'est un coup de dé.»
Cette monnaie est cependant extrêmement difficile à générer et est très coûteuse en électricité, d'après Louis Marchand : elle nécessite beaucoup de ressources et de temps, puisqu'elle doit correspondre à des critères mathématiques très précis. C'est notamment ce qui expliquerait la valeur toujours montante des bitcoins. Au moment de la vérification de L'Express, un de ces fichiers valait 550 $.
Selon les dires de l'étudiant en informatique qui a préféré conserver l'anonymat, lorsqu'il s'est lui-même procuré huit bitcoins il y a quelques années, ça ne lui avait pas coûté plus d'une centaine de dollars. «Si je me souviens bien, ça a déjà monté à 1400 $. C'est hallucinant», s'étonne-t-il.
Il faut dire que le marché du web invisible, dans lequel évoluent les bitcoins, est aussi extrêmement lucratif. La Sureté du Québec, les deux compères ayant testé les drogues du «*deep web*» et l'informaticien s'accordent tous sur un point : la rémunération est la motivation principale de n'importe quel trafiquant de marchandises illégales sur Internet, selon eux.
«Moins c'est légal, plus c'est payant. Personne n'ira vendre un foie sur Internet, à part pour l'argent que ça rapporte. Il faut oublier le côté humain et ne penser qu'au montant final», croit Louis Marchand… [Lire la suite]

Source : *Le logiciel Tor, la porte d'entrée du web invisible – Actualités – L'Express – Drummondville*

Darknet: qu’est ce qu’on y trouve et comment y accéder ?

Darknet:, qu’est ce qu’on y trouve et comment y accéder ?

Au fil de nos CyberBalades, notre souris s’est arrêtée sur un article très intéressant sur le DarkNet. Pour votre plus grand plaisir, veuillez trouver ci-dessous un extrait et le lien permettant de le consulter en entier.

Qu’est-ce qu’on trouve dans le Darknet ?

Ce qui frappe en premier c’est la **quantité de contenus illégaux**. On compte environ un tiers de porno (dont une bonne partie de pédopornographie et d’autres trucs louches), un autre tiers de contenu illégal (culture de drogue, négationnisme, numéro de carte bancaire, comment faire un petit engin explosif, etc.) et un dernier tiers de sites inclassables… [Lire la suite]

Liste des URL intéressantes pour explorer le darknet

• **Moteur de recherche** : http://hss3uro2hsxfogfq.onion
• **Hidden wiki**: http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page
• **Annuaire des liens** : http://torlinkbgs6aabns.onion
• **Facebook pour Tor**: https://facebookcorewwwi.onion
• **Moteur de recherche Darknet**: http://grams7enufi7jmdl.onion
• **Vente des mobiles débloqués:** http://mobil7rab6nuf7vx.onion
• **Location des services d’un hacker**: http://2ogmrlfzdthnwkez.onion
• **Moteur de recherche DuckDuckGo**: http://3g2upl4pq6kufc4m.onion
[Lire la suite]

Réagissez à cet article

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques**.

Quel sont nos principales activités ?

- **RGPD**
  - FORMATION AU RGPD
  - FORMATION DE DPO
  - AUDITS RGPD
  - MISE EN CONFORMITÉ RGPD
  - ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**
  - FORMATIONS / SENSIBILISATION D'UTILISATEURS

- RECHERCHE DE PREUVES

- **EXPERTISES**
  - EXPERTISES PRIVÉES
  - EXPERTISES DE VOTES ÉLECTRONIQUES
  - EXPERTISES JUDICIAIRES
  - RECHERCHE DE PREUVES
  - RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)

Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

« *Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et*

les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.
Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Source : *Darknet: qu'est ce qu'on y trouve et comment y accéder ?*

Auteur : Ahmed EL JAOUARI

Comment fonctionnent les Kits d’exploitation ?

Comment fonctionnent les Kits d’exploitation ?

Ces dernières années, nous avons observé une augmentation massive de l'utilisation des kits d'exploitation de vulnérabilités. Aucun site web n'est de taille face à la puissance d'un grand nombre de ces kits, à l'image de celui d'un célèbre quotidien britannique, notoirement victime d'une campagne de publicité malveillante exposant des millions de lecteurs au ransomware CryptoWall.

Les Exploit kits, des boites à outils faciles à utiliser

Cependant, l'aspect peut-être le plus préoccupant des kits d'exploitation tient à leur facilité d'utilisation. Ces « boîtes à outils à louer » ont principalement pour but de réduire les compétences techniques nécessaires au lancement de campagnes de malware, afin qu'un assaillant n'ait pas besoin de créer ou implanter le code malveillant lui-même. De fait, de nombreux kits s'accompagnent même désormais d'une interface ergonomique, permettant aux malfaiteurs de gérer et de surveiller leur malware tout au long d'une campagne.

La charge malveillante des kits d'exploitation se présentait jusque-là sous la forme de différentes sortes de malwares, qu'il s'agisse de fraude au clic publicitaire, de malware bancaire ou de ransomware, la nature de ces attaques variant selon le profil de l'utilisateur. Compte tenu de la facilité de personnalisation d'une attaque et de l'ergonomie des kits, il n'est guère surprenant que ceux-ci soient devenus l'arme de prédilection d'un grand nombre de cybercriminels, moins compétents sur le plan technique.

De quoi sont-ils faits ?

En règle générale, l'infrastructure d'un kit d'exploitation comprend trois composants :

- le « back-end », qui contient le tableau de commande et les charges malveillantes ;
- la couche intermédiaire, qui héberge le code malveillant et crée un tunnel dans le serveur back-end ;
- la couche proxy, qui transmet le malware directement à la victime.

La chaîne d'infection/exploitation demeure en outre largement similaire pour les différents kits :

- La victime se rend sur le site web, entièrement ou partiellement contrôlé par l'assaillant ;
- Elle est ensuite redirigée à travers de nombreux serveurs intermédiaires ;
- À son insu, elle aboutit sur le serveur hébergeant le kit d'exploitation ;
- Le kit tente alors de s'installer en exploitant une vulnérabilité logicielle sur le serveur cible ;

En cas d'installation réussie, la charge malveillante est alors activée.

La différence marquante entre les kits réside dans les types de vulnérabilités exploitées pour infecter les visiteurs et les diverses astuces employées pour échapper aux antivirus.

Vers la multiplication des cibles mobiles

Alors que les kits d'exploitation avaient traditionnellement tendance à cibler principalement les ordinateurs, les appareils mobiles sont de plus en plus visés en raison du grand nombre d'utilisateurs qui s'en servent pour surfer sur le Web, échanger des e-mails, consulter les réseaux sociaux et même pour effectuer des opérations bancaires. La plupart de ces utilisateurs n'étant pas au fait des meilleures pratiques pour sécuriser correctement leur mobile, ils offrent par essence une cible bien plus facile.

Il faut donc s'attendre à ce que les auteurs des attaques s'orientent progressivement vers la diffusion de malware mobile via des pages web sur un navigateur mobile, c'est-à-dire essentiellement le même mode d'infection que dans la plupart des cas sur les ordinateurs.

Dès lors que le virus réussit à s'implanter sur un ordinateur ou un mobile, il peut opérer derrière les firewalls d'une entreprise ou d'un particulier. Le malware se propage ainsi à d'autres équipements et se connecte au serveur de commande et de contrôle (C&C) via Internet, ce qui lui permet ensuite d'exfiltrer des données ou de télécharger d'autres logiciels malveillants. Cette communication entre le serveur C&C et la machine infectée passe souvent par le serveur de noms de domaines (DNS) de la cible.

Connaître son ennemi

Même si tous les kits d'exploitation ne sont pas identiques, il est important d'en identifier deux principaux.

Le baromètre Infoblox des menaces DNS observées au 4ème trimestre 2015 révèle que le kit Angler a représenté 56 % des nouvelles activités de ce type, et le kit RIG 20 %. En quoi consistent ces kits et leurs activités ?

Le kit d'exploitation Angler est l'un des plus élaborés actuellement utilisé par les cybercriminels. Notoirement connu pour avoir inauguré la technique du « masquage de domaine », Angler peut ainsi contrer les stratégies de blocage sur la base de la réputation et infiltrer des URL malveillantes dans des réseaux publicitaires légitimes. Il redirige ensuite les visiteurs du site web qui cliquent sur les liens publicitaires infectés vers d'autres sites qui implantent à leur tour un malware. Ces kits tendent à être actualisés avec les dernières failles « zero day » découvertes dans des logiciels répandus, tels que Apache Flash ou WordPress. Si l'on y ajoute l'utilisation de techniques complexes de dissimulation, cela rend Angler particulièrement difficile à détecter pour les solutions antivirus classiques.

Face à cette évolution constante, les entreprises doivent investir dans des technologies de protection qui non seulement bloquent un composant du kit Angler mais sont aussi capables d'identifier et d'interrompre l'activité malveillante sur l'ensemble de la chaîne d'infection.

Bien que de conception plus ancienne, le kit d'exploitation RIG a récemment fait son retour. Cela montre que les menaces passées peuvent réapparaître sous une nouvelle forme à mesure que les kits sont mis à jour. L'analyse par Infoblox de l'activité de RIG en 2015 révèle que celui-ci a commencé à utiliser des techniques de masquage de domaine similaires à celles employées par Angler.

Même si RIG est souvent déployé dans le cadre de campagnes de publicité malveillante, Heimdal Security a récemment découvert qu'il sert également pour la pollution de référencement Google, consistant à détourner les tactiques d'optimisation du moteur de recherche pour faire la promotion de sites web malveillants.

Avec leurs différentes déclinaisons et techniques, les kits d'exploitation offrent aux malfaiteurs dépourvus de compétences techniques l'opportunité de tirer profit du monde de la cybercriminalité. Pour se protéger contre cette menace sans cesse croissante, les entreprises doivent faire appel à une source fiable de veille des menaces et s'appuyer sur ces informations pour interrompre les communications des malwares passant par des protocoles au sein de leur propre infrastructure, notamment le DNS… [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, arnaques Internet...) et judiciaires (contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

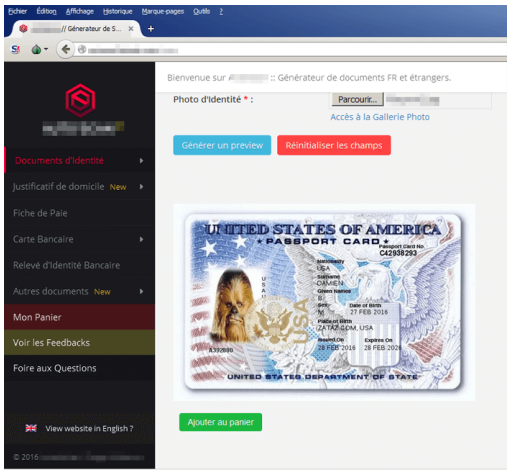
Contactez-nous

Suivez-nous sur

Réagissez à cet article

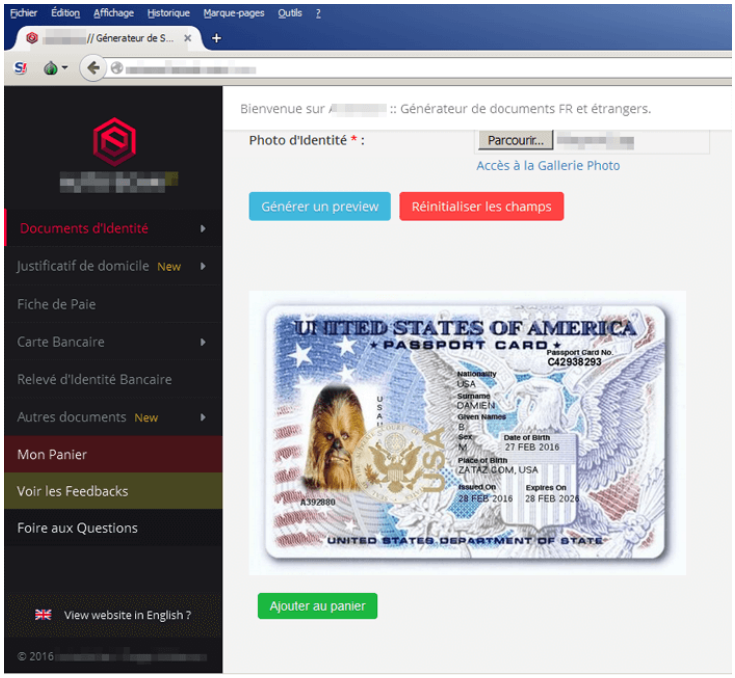
Source : *Comment fonctionnent les Kits d'exploitation ? – Global Security Mag Online*

Le Darknet cache un générateur de faux documents



Le Darknet cache un générateur de faux documents

Vous cherchez de faux documents comme un diplôme du baccalauréat, de BTS ? Une fausse facture FREE, EDF, Direct Énergie ? Un faux permis de conduire ? Une fausse fiche de paie ou une fausse carte bancaire ? Un site Internet vous propose d'automatiser l'usurpation.



Ils sont de petites stars dans le black market, deux francophones devenus des références dans la contrefaçon de documents. Les autorités leurs poseraient bien deux/trois questions, mais les deux administrateurs du portail A.S. [Le nom a été modifié, NDR] sont malins, cachées dans les méandres du darknet. Leur site, pas la peine de me réclamer l'adresse, est caché sous une adresse .onion. A.S. profite de l'anonymat proposé par le service TOR pour éviter d'afficher ouvertement son serveur, son ip d'origine. Et même si vous mettiez la main sur ce dernier, l'hébergement est hors de l'hexagone.

« ***Bienvenue sur A'S. :: Générateur de documents FR et étrangers*** » souligne l'introduction affichée par le site. Mission de ce dernier, pour quelques euros, facturés en Bitcoins, générer de fausses factures, fausses fiches de paie, faux relevé d'identité bancaire (RIB). Il est possible de générer un faux diplôme du Baccalauréat, de BTS, d'IUT. Une fausse carte vitale ? Pas de problème. Une facture d'un achat effectuée chez Darty, ok. Passeport Français, Américain et autres copies d'une carte nationale d'identité boucles ce service… qui n'a rien d'illégal, du moins si vous rentrez vos propres coordonnées. Il en va tout autrement si les informations que vous fournissez permettent d'usurper une identité, une fonction, un titre via ses faux documents. La loi punit de trois ans d'emprisonnement et de 45000 euros d'amende le faux et l'usage de faux documents.
Les prix varient de 4,99€ pour une copie de passeport, une facture. 9,99€ pour le scan d'un bulletin de fiche de paie. 6,99€ pour la copie d'un diplôme du baccalauréat général. Les auteurs de ce business proposent même un abonnement à vie. Pour ~~79 800~~ euros, les commerciaux indiquent permettre « ***un accès illimité et à vie à tous les articles de cet Autoshop pour 200€ ~~BTC~~***« . La boutique annonce un anonymat garanti. [Correction : selon les auteurs, il s'agit de 200€ et non 200 BT comme il était écrit sur leur site, NDR]… [Lire la suite]

Réagissez à cet article

Source : *ZATAZ Générateurs de faux documents – ZATAZ*