zscaler™

l'Etat des attaques cryptées en 2020

L'équipe de recherche Zscaler™ ThreatLabZ partage les principaux aperçus sur la manière dont les hackers améliorent leur utilisation du cryptage SSL/TLS pour contourner les défenses traditionnelles

JANVIER - SEPTEMBRE 2020

Sommaire

À propos de ThreatLabZ

ThreatLabZ est l'équipe responsable de la sécurité mondiale de Zscaler. En plus d'être chargée de protéger les clients de Zscaler contre les menaces émergentes, cette équipe analyse le trafic d'entreprise qui traverse le cloud Zscaler. Dotée d'expertise en cybersécurité, en data science et en IA/ apprentissage automatique, ainsi que d'un volume de données analysées à partir de plus de 120 milliards de transactions quotidiennes dans la plateforme cloud Zero Trust Exchange™ de Zscaler, ThreatLabZ est très bien placée pour fournir des aperçus sur les tendances en matière de trafic d'entreprise et de sécurité.

Lorsque ThreatLabZ découvre une nouvelle campagne d'attaque ou un nouveau programme malveillant dotés de techniques ou de capacités hors du commun, les chercheurs dépècent ces fichiers. Ils analysent leur code pour voir exactement comment leur programmation leur permet d'échapper à la détection tout en provoquant la perte de payloads, le vol d'informations, le contrôle des appareils, l'espionnage de l'utilisateur, et en se propageant. Les résultats des analyses sont publiés sur le **blog de recherche de Zscaler** au profit de la communauté de sécurité.

Concernant les tendances SSL, les chercheurs de ThreatLabZ ont récemment découvert, analysé et signalé les menaces visant les canaux cryptés. Lirez les articles suivants pour plus d'informations:

- **De faux sites VPN livrent des Infostealers**
- **Détournement de l'outil StackBlitz pour héberger des pages d'hameçonnage**
- **JavaScript Skimmers**
- **Higaisa: une menace persistante avancée**

Pour voir le cloud de Zscaler à l'œuvre, consultez le **Cloud Activity Dashboard**, qui affiche le nombre de transactions en cours de traitement ainsi que les menaces bloquées chaque seconde.

Le trafic SSL dissimule des programmes malveillants. Beaucoup d'entre eux.

Il existe une croyance sur le cryptage SSL qui est aussi persistante qu'erronée: «Je pensais que, tant qu'un site Web utilisait le cryptage SSL, il serait sécurisé». Une idée fausse qui agace les experts en sécurité.

Le cryptage SSL a été conçu pour protéger le trafic des yeux indiscrets, mais les adversaires l'ont également utilisé pour cacher les attaques, transformant l'utilisation du cryptage sans inspection adéquate en une menace potentielle.

Tout comme les experts en sécurité, les cybercriminels savent que le cryptage SSL/TLS est le moyen standard qu'utilise l'industrie pour protéger les données en transit. Ces cybercriminels utilisent aussi des méthodes de cryptage aux normes de l'industrie, concevant des moyens astucieux pour dissimuler des programmes malveillants dans le trafic crypté afin de mener des attaques qui contournent la détection. En fait, entre janvier et septembre, le cloud de Zscaler a intercepté 6,6 milliards de menaces de sécurité dissimulées dans le trafic crypté, soit une moyenne de 733 millions de menaces bloquées par mois. Cette moyenne mensuelle représente une augmentation de près de 260 pour cent par rapport à 2019, année durant laquelle le cloud de Zscaler bloquait mensuellement 283 millions menaces en moyenne dans le trafic crypté.

L'inspection du trafic crypté doit constituer un élément clé des défenses en matière de sécurité de toute l'entreprise. Le problème provient du fait que les outils de sécurité traditionnels sur site, comme les pare-feux de nouvelle génération, ont du mal à fournir les performances et les capacités nécessaires pour efficacement décrypter, inspecter et crypter à nouveau le trafic. Tenter d'inspecter l'ensemble du trafic SSL mettrait un frein aux performances (et à la productivité), à tel point que de nombreuses entreprises laissent passer au moins une partie de leur trafic crypté sans l'inspecter. C'est le cas du trafic provenant des fournisseurs de services cloud et d'autres jugés « fiables ». Il s'agit là d'une grave faille. Ne pas inspecter l'ensemble du trafic crypté, c'est clairement exposer les entreprises aux attaques d'hameçonnage cachées, aux programmes malveillants et bien plus, ce qui pourrait être désastreux.

Entre janvier et septembre, le **cloud de Zscaler a identifié et stoppé 6,6 milliards de menaces** dissimulées dans le trafic crypté.

L'équipe ThreatLabZ a analysé le trafic crypté dans le cloud de Zscaler pendant les neuf premiers mois de l'année 2020, en évaluant son utilisation dans certaines industries. L'objectif de l'analyse est de comprendre non seulement le volume du trafic utilisant le cryptage, mais aussi les menaces dissimulées au sein de ce trafic. Voici quelques-uns des points marquants :

- **La majorité du trafic Internet est crypté:** 80 % du trafic utilise par défaut le cryptage SSL/TLS.
- **Une croissance exponentielle en volume:** Augmentation de 260 % des menaces basées sur le SSL ces neuf derniers mois, accélérée par la montée en flèche des applications collaboratives axées sur le cloud durant la pandémie de COVID-19.
- **Attaque sur l'industrie de la Santé:** L'industrie de la Santé fut la plus ciblée de toutes avec 1,6 milliards de menaces cryptées identifiées et stoppées, suivi par les finances et l'industrie manufacturière.
- **Détournement grandissant des services axés sur le cloud et utilisés pour le partage de fichiers:** Plus de 30 % de toutes les attaques basées sur le SSL se cachent dans des services de collaboration tels que Google Drive, OneDrive, AWS, ou Dropbox.
- **Augmentation de ransomwares dissimulés :** Au moins 5 fois plus de ransomwares sont livrés dans le trafic Web crypté.

Les cybercriminels utilisent également le SSL/TLS : Importance du l'inspection du trafic crypté

Le cryptage du trafic internet via le protocole SSL (Secure Sockets Layer), et son remplaçant plus moderne, le TLS (Transport Layer Security), est la norme mondiale pour la protection des données en transit, et la grande majorité du trafic Internet est aujourd'hui cryptée.[1] Malheureusement, les criminels utilisent aussi le cryptage pour cacher des programmes malveillants et autres exploits. Ainsi, le trafic passant par des canaux cryptés ne peut plus être fiable simplement en vertu d'un certificat numérique.

Les cybercriminels ont créé des chaînes d'attaques sophistiquées qui commencent par un e-mail d'hameçonnage tout innocent d'apparence mais dissimulant un exploit ou un programme malveillant. Si un utilisateur peu méfiant clique dessus, l'attaque passe à la phase d'installation du programme malveillant et, au final, à l'exfiltration de précieuses données d'entreprise.

Ce qui rend les attaques si néfastes, c'est que l'exploit ou le programme malveillant caché est aussi crypté, ce qui change complètement sa structure de fichier. Les systèmes de cybersécurité s'appuient sur la structure d'un fichier (ou «empreinte digitale») pour identifier les menaces entrantes; si elle est structurée d'une certaine manière, elle sera bloquée par le système. Mais dès qu'un fichier est crypté, il reçoit une toute nouvelle empreinte digitale qui empêche de l'identifier comme étant une menace.

L'inspection SSL est le seul moyen efficace de bloquer les fichiers malveillants transmis [à l'aide de ces services], car les moteurs de sécurité ne peuvent pas bloquer ce qu'ils ne peuvent pas voir.

[1] https://transparencyreport.google.com/https/overview?hl=en

Tendances du trafic SSL

Les entreprises ont largement accepté le fait que le cryptage est une exigence pour protéger les données en transit afin qu'elles ne soient ni interceptées ni exploitées. L'analyse a révélé que le secteur de l'éducation cryptait la majorité de son trafic, suivi de l'industrie manufacturière, des finances et de la Santé. Mais toutes les industries, y compris la vente au détail/le commerce de gros, les services, les technologiques en matière de communication et les administrations publiques, sont regroupés de manière assez étroite. Au cours de la période d'analyse, allant de janvier à septembre 2020, il a été constaté que l'utilisation du cryptage dans toutes les industries représentait une moyenne d'environ 75 % avec un pic de 80 %.

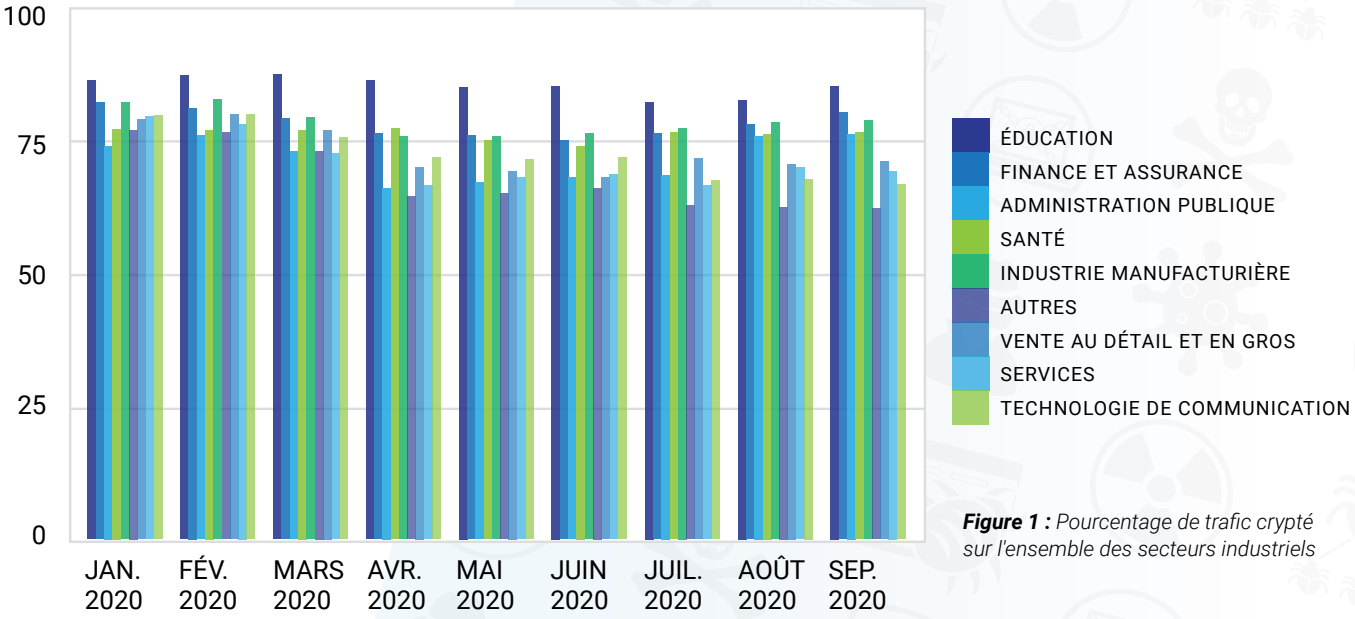


Figure 1 : *Pourcentage de trafic crypté sur l'ensemble des secteurs industriels*

Des taux élevés de trafic crypté ont été observés dans tous les secteurs industriels, ce qui signifie que toutes les entreprises doivent réfléchir à la façon d'inspecter le SSL/TLS afin de détecter les menaces.

La recherche a révélé que les cybercriminels ciblent le domaine de la Santé avec des attaques de programmes malveillants cryptés plus que tout autre secteur. Entre janvier et septembre 2020, le secteur de la Santé représentait 25,5 % de toutes les menaces avancées bloquées sur les canaux cryptés dans le cloud de Zscaler, suivi par celui des finances/assurances avec 18,3 %, l'industrie manufacturière avec 17,4 % et les administrations publiques avec 14,3 %.

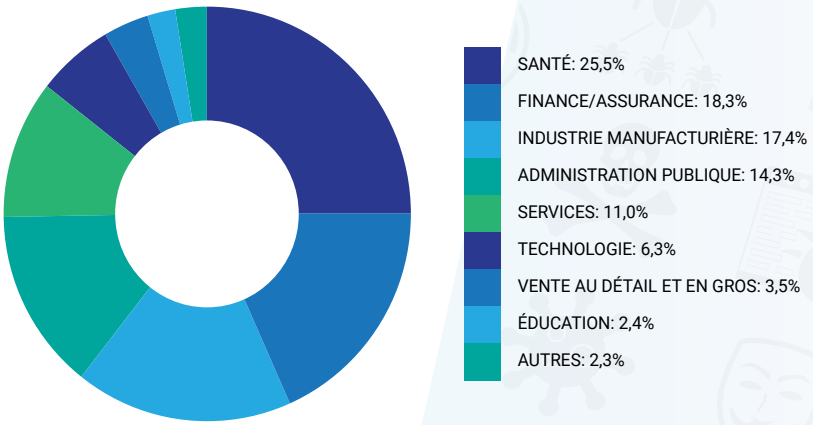


Figure 2: *Menaces avancées bloquées sur des canaux cryptés par industrie*

Les entreprises du domaine de la Santé ont été ciblées avec le plus grand nombre de menaces transmises par le biais de canaux cryptés, malgré que la pandémie mondiale rend leurs services plus critiques que jamais. Les hackers se sont également servis de la pandémie pour lancer de nouvelles campagnes, avec de faux sites proposant des nouveautés, des produits et des remèdes. Au cours des trois premiers mois de 2020, ThreatLabZ a fait état d'une montée en flèche de **30.000 pour cent** du nombre de menaces liées au COVID.

Gros plan sur l'industrie de la Santé

Bien plus que tout autre secteur, l'industrie de la Santé a été la cible de plus de 1,69 milliards de tentatives d'attaques sur des canaux cryptés lors de notre analyse. La grande majorité des attaques sur ce secteur sont venues via des URL malveillantes (84,2 %). Ces URL malveillantes peuvent être transmises aux utilisateurs par: e-mail, SMS, fenêtres publicitaires contextuelles ou en page, conduisant au téléchargement de programmes malveillants, de logiciels espions, de ransomwares, de comptes piratés, etc.

L'industrie de la Santé est souvent la cible de cyberattaques en raison de la présence de systèmes obsolètes (due à l'approbation prolongée de la FDA) dans l'environnement. Ils sont dépourvus de contrôles de sécurité et sont souvent vulnérables à des problèmes connus. En absence de contrôles unifiés, de visibilité centralisée et d'une application des politiques, ces entreprises se retrouvent avec des failles dans leurs contrôles de sécurité, ce dont les cybercriminels tentent de tirer profit.

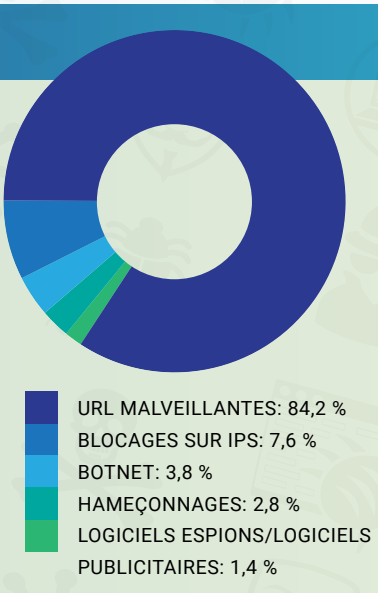


Figure 3: *Menaces sur les canaux cryptés ciblant le secteur de la Santé*

Les attaques deviennent de plus en plus sophistiquées

Les professionnels de l'informatique avertissent souvent les utilisateurs, leur demandant de vérifier soigneusement l'URL d'un site soupçonné d'être un faux afin d'y déceler des erreurs, des fautes d'orthographe ou d'autres indices indiquant qu'il est illicite. Mais de nos jours, les cybercriminels utilisent des techniques telles que le cybersquattage de domaine et les attaques homographiques IDN pour rendre leurs sites quasiment indiscernables des vrais.

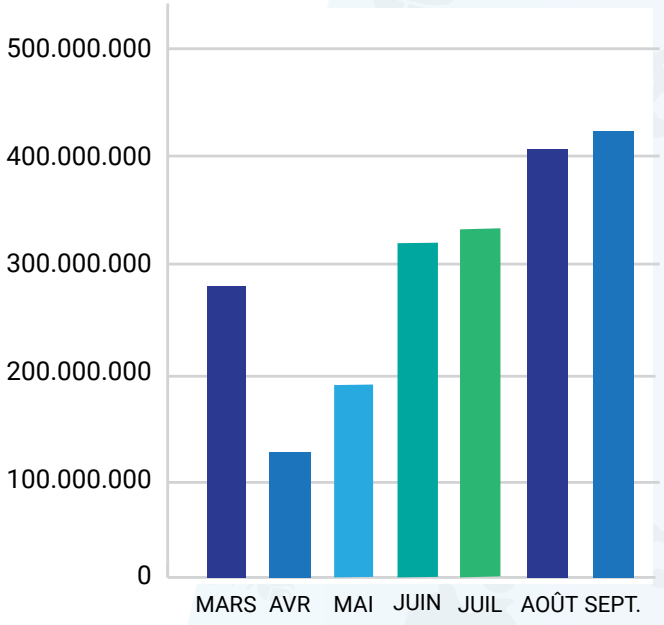
Le cybersquattage de domaines consiste à enregistrer un domaine de premier niveau similaire à une marque connue (telle que gmali.com) à des fins d'hameçonnage, de vol d'identifiants ou pour servir de programmes malveillants.

Une attaque homographique, comme le cybersquattage de domaines, est utilisée pour inciter les gens à cliquer sur les liens en utilisant des caractères, tel que le chiffre «1» au lieu d'un «l» dans l'URL de Apple (https://www.app1e.com).

Détournement des services de stockage cloud

Les services de stockage cloud sont devenus des outils populaires pour lancer des attaques. Ces services sont très pratiques pour partager des fichiers en toute sécurité via une transmission basée sur le protocole SSL sur le Web. Mais comme les cybercriminels savent que la plupart des entreprises sont incapables d'inspecter le trafic SSL à grande échelle, et que les services cloud sont généralement jugés « fiables », ils lancent des attaques qui semblent provenir de ces services.

De mars à septembre 2020, le cloud de Zscaler a bloqué **deux milliards de menaces** dans le trafic crypté, dont la majorité concerne des contenus malveillants hébergés sur Google, AWS, Dropbox et OneDrive. Ces menaces ont presque doublé entre mars et septembre et représentaient près de 30 % de toutes les menaces cryptées par SSL/ TLS au cours de ces mois.



De mars à septembre, le cloud de Zscaler a bloqué **deux milliards de menaces** dans le trafic SSL provenant de fournisseurs de services de stockage cloud.

Figure 4: *Menaces avancées bloquées sur TLS/SSL provenant des meilleurs services de stockage cloud*

La figure 5 montre comment les services cloud sont exploités pour héberger et propager des programmes malveillants. Les cybercriminels chargent le payload des programmes malveillants (souvent un fichier téléchargeur de niveau 1) sur un ou plusieurs services et distribuent les URL dans le cadre d'une campagne de spam par e-mail. L'utilisation de services de premier plan tels que Google, Microsoft, Amazon et Dropbox augmente les chances de voir des utilisateurs finaux cliquer sur le lien.

Les cybercriminels profitent également des certificats SSL du joker appartenant à ces fournisseurs de services. Quand le trafic des fournisseurs de cloud est jugé sûr et passe sans être inspecté, les hackers s'en servent pour propager des payloads de programmes malveillants à travers des canaux cryptés et à contourner les solutions de sécurité basées sur le filtrage d'URL, telles que l'antispam, la protection d'e-mail, les pare-feux, etc. **Un e-mail d'hameçonnage contenant un lien vers un fichier malveillant hébergé dans un service de confiance axé sur le cloud peut échapper aux solutions traditionnelles de sécurité d'e-mail.**

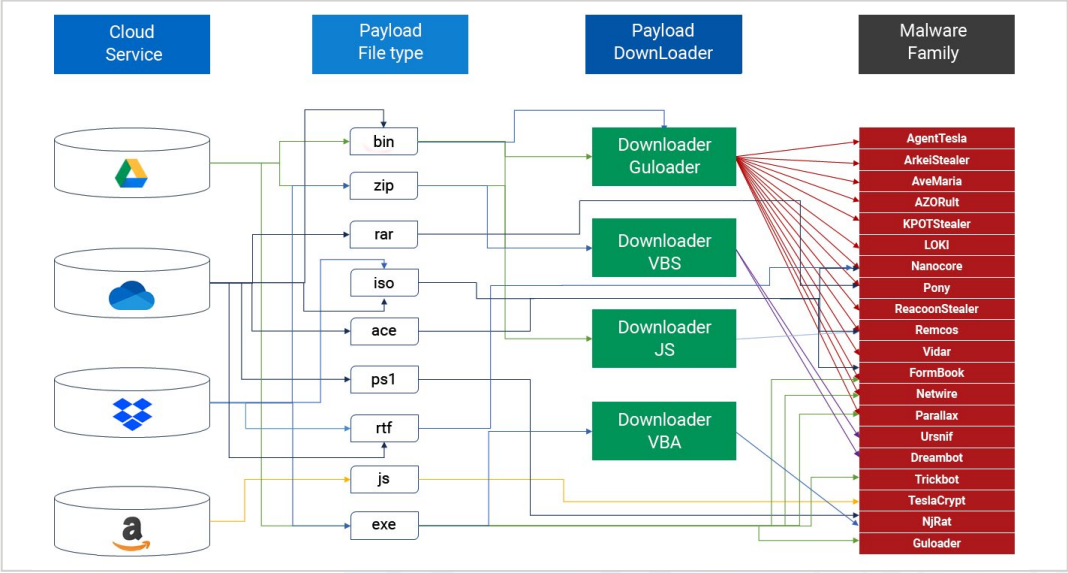


Figure 5 : *Payloads de programmes malveillants fournies via des services cloud*

L'exemple ci-dessous présente les URL du service de stockage cloud OneDrive. Les deux premières URL sont malveillantes et entraînent le téléchargement de programmes malveillants appartenant aux familles «Trojan EdLoader» et «Backdoor LokiBot». La troisième URL par contre est légitime et télécharge le véritable fichier de l'utilisateur. Le sous-domaine et l'URI (Uniform Resource Identifier) apparaissent comme des modèles de chaînes aléatoires qui rendent impossible la distinction entre les URL légitimes et les URL malveillantes. L'inspection SSL est le seul moyen efficace de bloquer les fichiers malveillants transmis à l'aide de ces services, car les moteurs de sécurité ne peuvent pas bloquer ce qu'ils ne peuvent pas voir.

Figure 6 : *Des chaînes aléatoires dans les sous-domaines empêchent de distinguer les URL malveillantes des URL légitimes*

Attaques sur les appareils mobiles

Les smartphones sont également devenus des cibles privilégiées.Tout comme les cybercriminels usurpent les pages Web, ils créent de fausses applications qui semblent légitimes.Par exemple, un Trojan bancaire Android appelé Cerberus utilise un nom d'application et une icône afin d'imiter l'application légitime Google Play.Dès qu'un utilisateur peu méfiant clique sur la fausse application, celle-ci envoie une notification pour obtenir l'autorisation à un «service d'accessibilité». (Le service d'accessibilité permet aux utilisateurs handicapés d'utiliser les appareils et les applications Android.)

Cet exploit suppose que de nombreux utilisateurs «accepteront» une notification sans la lire attentivement. Dans ce cas, cliquer sur «Autoriser» permet à l'application de visualiser le contenu d'autres applications affichées à l'écran et d'effectuer diverses actions à l'insu de l'utilisateur.

Le programme malveillant accède aux informations d'identification des applications bancaires, de Gmail ou de l'application d'authentification à deux facteurs Google Authenticator, puis les exfiltre. Il peut également exécuter d'autres actions malveillantes, telles qu'enregistrer discrètement de l'audio et voler de messages texte. Il y a plus grave. Une fois l'autorisation au service d'accessibilité accordée au programme malveillant, il peut empêcher l'utilisateur de désactiver l'application d'autorisation ou de la désinstaller.

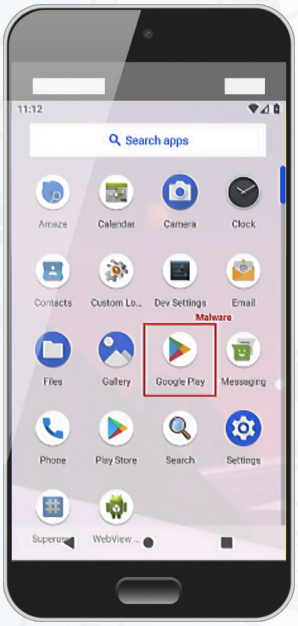


Figure 7: *Une fausse application Google Play*

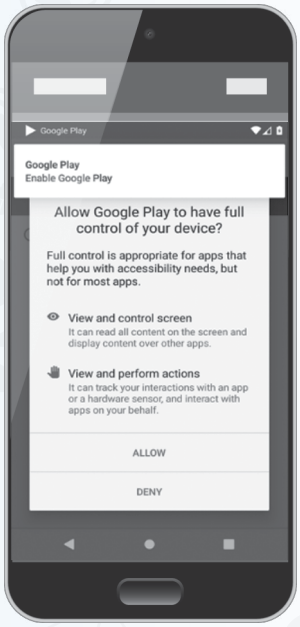
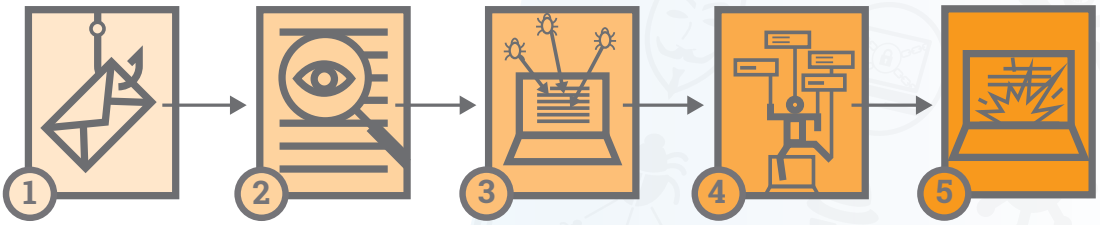


Figure 8: *Notification sur une fausse application Google Play*

Anatomie d'une attaque



La livraison peut consister en un e-mail d'hameçonnage dissimulant en son sein un exploit ou un programme malveillant. Ce dernier est livré lorsqu'un utilisateur le télécharge ou clique sur un lien contenu dans l'e-mail.

L'exploitation désigne ce qui se passe lorsque le programme recherche des vulnérabilités qu'il peut exploiter dans le système et qu'il exécute le code.

L'installation se produit lorsque le programme malveillant est chargé sur la machine de la victime.

Le rappel de commande et de contrôle (C & C) se produit lorsqu'un programme malveillant tente de communiquer avec les serveurs C & C, souvent pour obtenir des instructions ou envoyer des données volées.

L'explosion est l'étape au cours de laquelle le programme malveillant peut installer d'autres programmes malveillants, exfiltrer des données, ou exécuter d'autres actions programmés par le serveur C & C.

Analyse de la chaîne d'attaque

Hameçonnage

Puisque que l'hameçonnage est généralement la première étape d'une cyberattaque séquentielle impliquant un vol d'informations d'identification, nous avons analysé les plus de **193 millions de tentatives d'hameçonnage** transmises sur des canaux cryptés, mais qui furent identifiées et bloquées par le cloud de Zscaler entre janvier et septembre 2020. Les tentatives par secteurs industriels ont été classées. Dotée d'installations individuelles qui utilisent souvent des infrastructures et des systèmes informatiques différents (les rendant potentiellement plus vulnérables), l'industrie manufacturière était la cible la plus importante, recevant 38,6 % des tentatives d'hameçonnage, suivies du secteur des services avec 13,8 %.

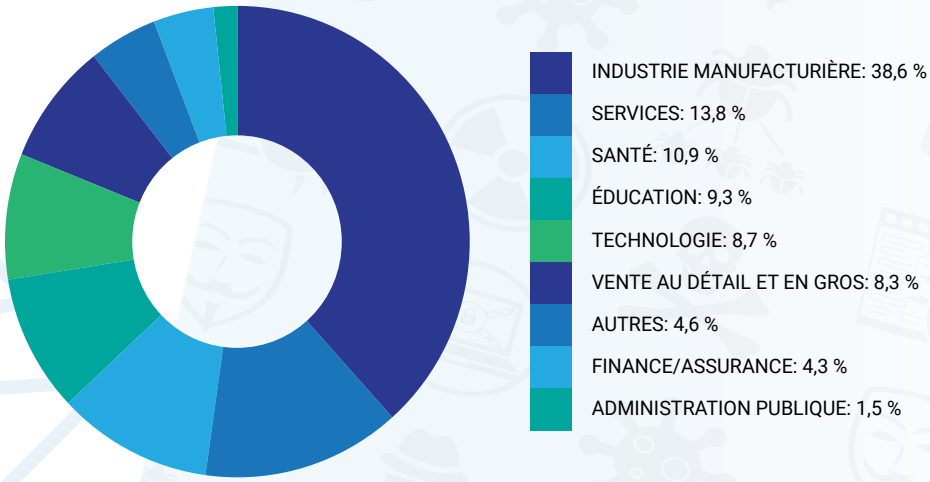


***Figure 9:** Menaces d'hameçonnage bloquées sur des canaux cryptés par type d'industrie*

Des services d'entreprise et des marques en train d'être hameçonnés

Une tentative d'hameçonnage comprend souvent un site Web usurpé qui imite une marque ciblée. En termes simples, un e-mail arrive et demande à l'utilisateur de cliquer sur un lien qui le dirige vers un faux site Web. Sur ce site, l'utilisateur est invité à saisir un nom d'utilisateur/mot de passe ou d'autres informations essentielles qui peuvent être utilisées par les cybercriminels pour mener des attaques.

Les recherches ont révélé que la marque la plus hameçonnée était Microsoft. Les attaques portent sur diverses propriétés Web sur le thème Microsoft (Office 365, SharePoint, OneDrive, etc.), grâce auxquelles les cybercriminels tentent de voler les informations d'identification des services d'entreprise. Le deuxième type d'attaques d'hameçonnage les plus populaires sont les escroqueries du «support technique». En général, ces attaques utilisent une redirection vers des sites Web compromis qui prétendent que l'ordinateur de l'utilisateur a été piraté et que le «support Microsoft» est disposé à le résoudre (une fois que l'utilisateur aura envoyé les informations de carte de crédit).

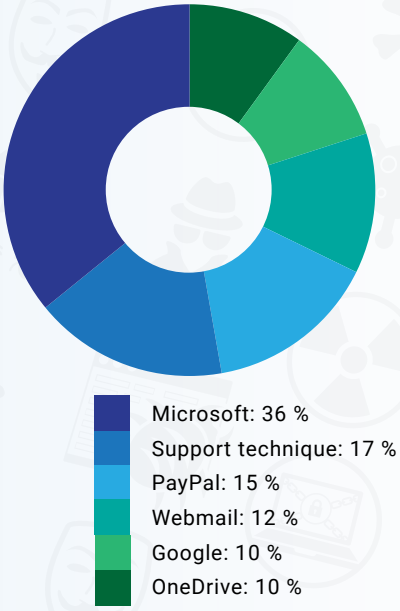


Figure 10: *Marques d'entreprise et services les plus fréquemment hameçonnés*

PayPal et Google figuraient également parmi les plus grandes marques victimes de ces attaques d'hameçonnage.Les sites usurpés ressemblent étrangement aux sites réels, ce qui les rend difficile à détecter.

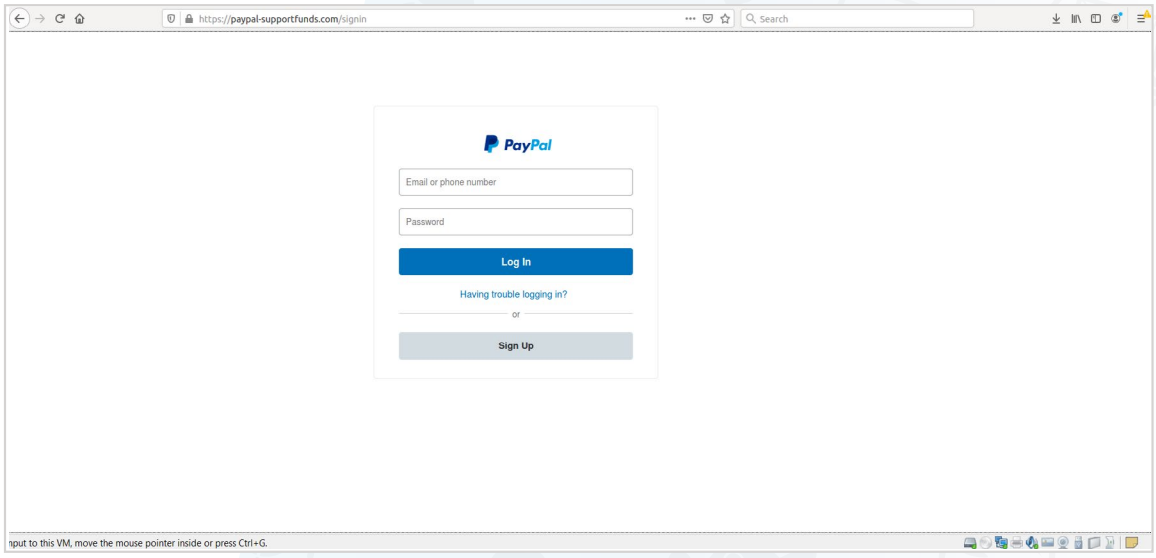


Figure 11: *Un site d'hameçonnage PayPal via HTTPS*

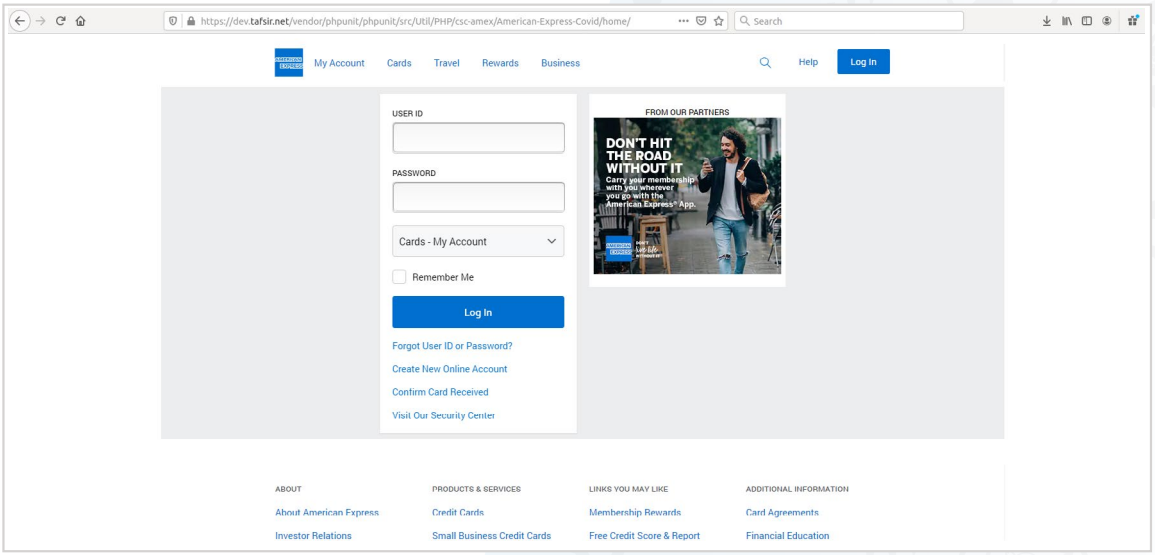


Figure 12: *Un site d'hameçonnage American Express via HTTPS*

Hameçonnage Netflix via HTTPS

L'utilisation des services de divertissement en streaming tels que Netflix a augmenté durant la pandémie, ce que les cybercriminels ont remarqué. Les hackers ciblent les services de streaming pour hameçonner les identifiants des utilisateurs. Malheureusement, comme l'illustre la figure 13, il est difficile de distinguer ces fausses pages des vraies.

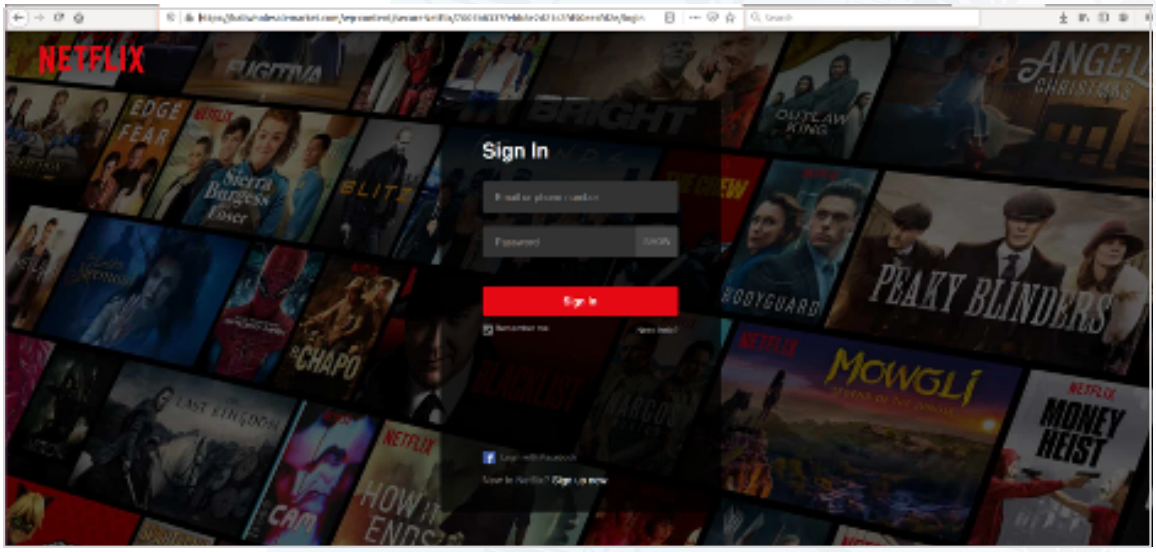


Figure 13: *Image d'hameçonnage Netflix*

Escroquerie de type support technique via HTTPS visant les utilisateurs de Microsoft

La figure 14 montre une page d'escroquerie de type support technique Microsoft. En cliquant sur l'URL, vous verrez le certificat HTTPS tel qu'authentifié par Microsoft. Le certificat utilisé montre que les hackers exploitent Azure (une autre marque bien connue) pour tenter d'ajouter de la crédibilité et indiquer qu'il s'agit d'une page légitime envoyée par Microsoft.

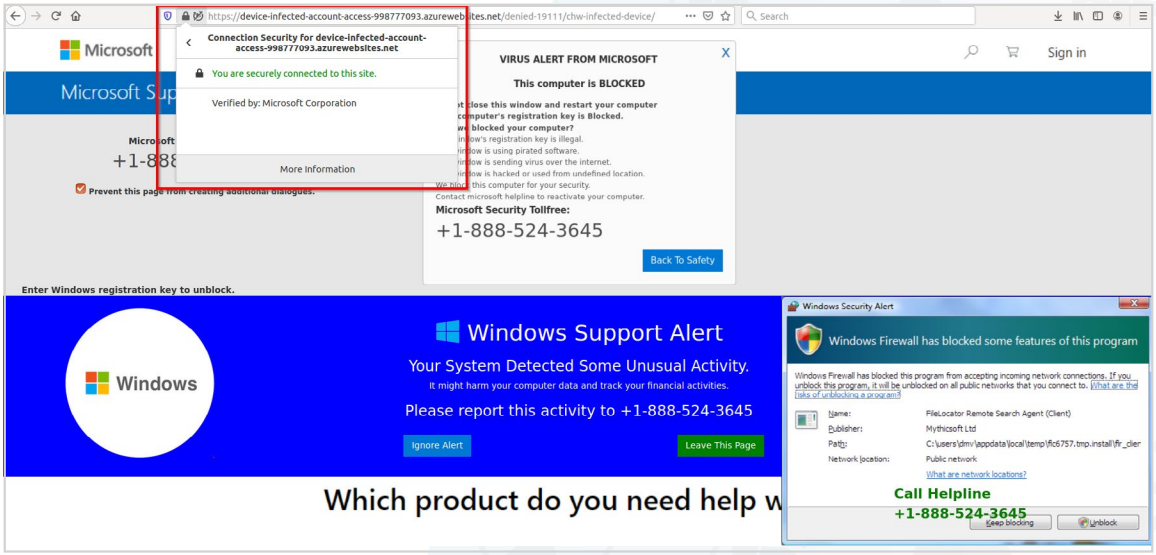


Figure 14: *Escroquerie de type support technique via HTTPS visant les utilisateurs de Microsoft*

Attaques de navigateur

Durant les attaques de navigateur, les hackers tirent parti d'une vulnérabilité dans un système d'exploitation ou modifient les paramètres du navigateur des utilisateurs à leur insu. Le cloud de Zscaler a bloqué plus de 658.000 menaces d'attaques de navigateur ciblant l'industrie manufacturière (26,5 %) et le secteur des finances/assurances (19,9 %), qui sont leurs cibles privilégiées.

L'industrie manufacturière est souvent la cible de cyberattaques parce qu'elle est (traditionnellement, du moins) très fragmentée, avec des installations individuelles utilisant chacune des infrastructures informatiques différentes et de multiples systèmes hétéroclites. Comme dans toute autre industrie, sans contrôles unifiés, sans visibilité centralisée et sans application des politiques, la sécurité est incomplète et les cybercriminels ne cessent de profiter de ces failles.

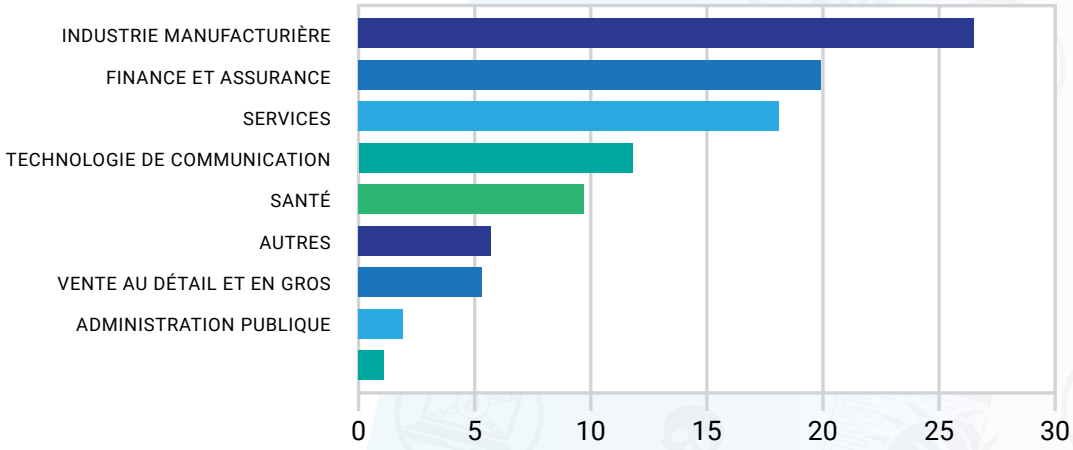


Figure 15 : *Attaques de navigateur bloquées sur des canaux cryptés par type d'industrie*

Ransomware

Zscaler ThreatLabZ a constaté une augmentation de 500 % du nombres d'attaques de ransomware via des canaux SSL/TLS depuis mars 2020. Avec une majorité des employés travaillant à distance et accédant aux applications internes, il y a eu une augmentation de l'activité des ransomwares ciblant les secteurs industriels les plus susceptibles de payer des rançons.

Les industries de la technologie/communication (40,5) et de la Santé (26,5) ont été parmi les plus ciblées par les attaques de ransomware sur les canaux cryptés.

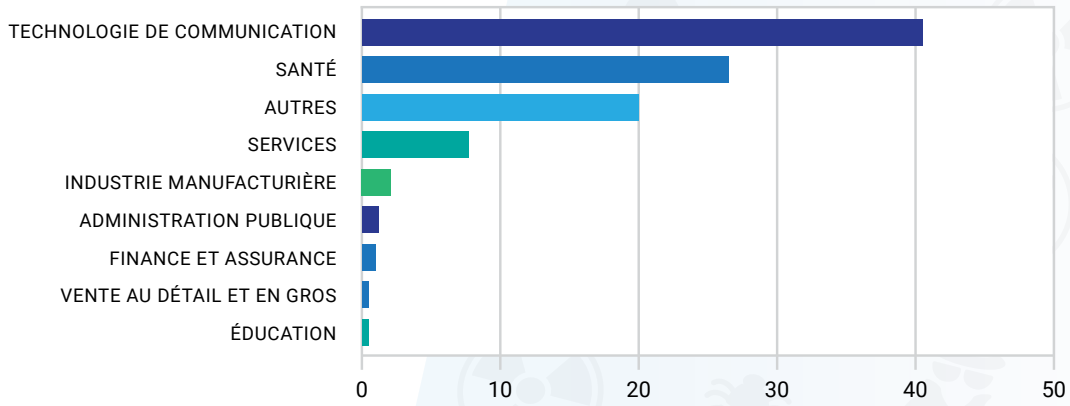


Figure 16: *Ransomwares bloqués sur les canaux cryptés par type d'industrie*

Parmi les principales gammes de ransomwares utilisées dans ces attaques, on trouve les variantes de FileCrypt/FileCoder, suivies de Sodinokibi, Maze et des variantes de gamme de la famille Ryuk. Durant l'année écoulée, un changement important dans bon nombre de ces variantes de la gamme de ransomwares a été l'ajout d'une fonction d'exfiltration de données. Cette nouvelle fonctionnalité permet aux ransomwares d'exfiltrer les données sensibles des victimes avant de les crypter. Ces données exfiltrées constituent une sorte de police d'assurance pour les hackers. Ainsi, même si la victime ou l'entreprise dispose de bonnes sauvegardes, elle devra payer la rançon pour éviter que ses données soient exposées.

Programmes malveillants

Les programmes malveillants offrent un moyen de persistance, donnant à un cybercriminel un accès continu à la machine d'une victime. Ces programmes sont souvent installés lorsqu'ils tirent profit des vulnérabilités ou via des attaques d'ingénierie sociale. C'est de loin le type d'attaques le plus souvent identifié par les chercheurs de Zscaler, comptant plus de **2,6 milliards de menaces de programmes malveillants** bloquées lors de notre analyse.

Les industries qui gèrent des renseignements personnels sont des cibles privilégiées des programmes malveillants. Durant notre analyse, les plus grands nombres d'attaques de ce type qui ont été bloquées sur des canaux cryptés furent dans les industries de la Santé et des finances/assurances, avec respectivement 27,4 et 19,6 %.

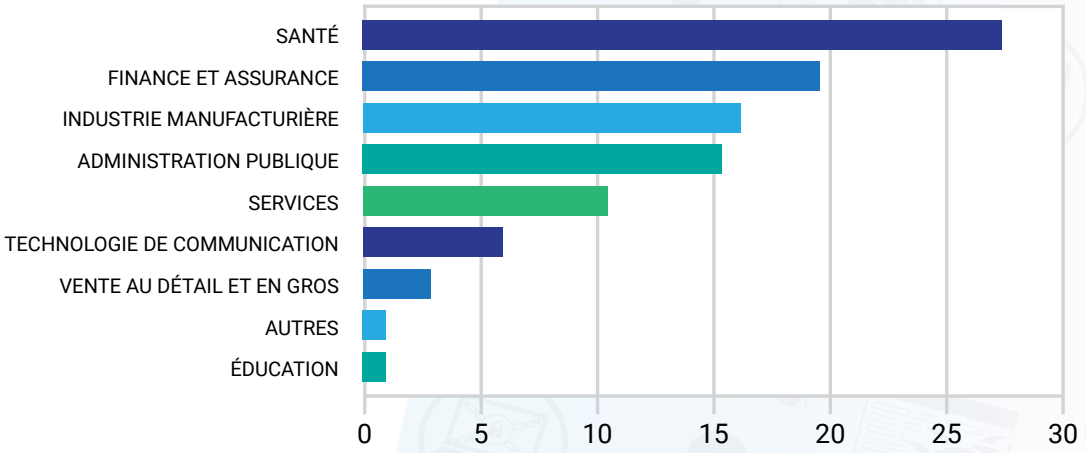


Figure 17: *Programmes malveillants bloqués sur des canaux cryptés par type d'industrie*

Activité de commande et de contrôle (C & C) des programmes malveillants sur les canaux cryptés

La communication C & C est un autre facteur clé de la chaîne d'attaque. Si le programme malveillant n'a pas été détecté et parvient à être installé sur l'appareil d'un utilisateur final, il interpelle le serveur C & C afin de commencer à exfiltrer les données et lancer d'autres attaques. Les payloads des programmes malveillants sont souvent programmées de manière à rester inactifs et attendre les commandes du serveur avant d'initier des activités malveillantes. Emotet et TrickBot étaient les deux gammes de programmes malveillants les plus répandues que nous avons observées durant notre analyse.

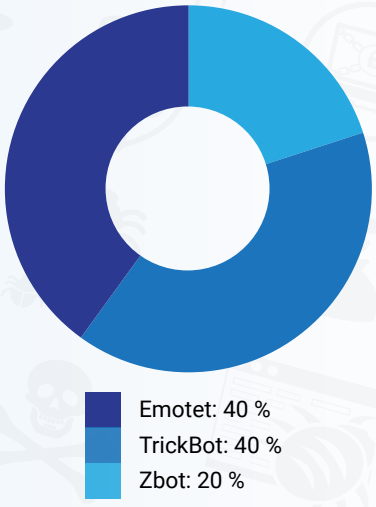


Figure 18: *Activité C & C la plus souvent bloquée sur les canaux cryptées*

Outre Emotet et TrickBot, nous avons noté une activité en provenance de Ursnif et Unruy. Emotet était l'outil de prédilection dans toutes les industries, tandis que TrickBot est le deuxième type de programme malveillant le plus utilisé dans les secteurs des finances/assurances et de l'administration publique. Ursnif était courant dans les attaques contre l'industrie manufacturière et la Santé, et Unruy était deuxième dans les attaques contre les institutions éducatives.

Les programmes malveillants qui vous ciblent

Emotet: Emotet a commencé comme Trojan bancaire en 2014. Cependant, il est devenu une menace très célèbre surtout utilisée dans le spamming et le téléchargement de programmes malveillants sur des systèmes cibles. L'agence américaine CISA (Cyber Infrastructure Security Agency - Agence pour la sécurité des cyberinfrastructres) a classé Emotet parmi les programmes malveillants **les plus coûteux et les plus destructeurs** affectant à la fois les secteurs public et privé. Emotet s'est avéré tenace et modulaire, doté d'améliorations régulières qui le rendent difficile à détecter par les entreprises.

TrickBot: TrickBot est le successeur du Trojan bancaire Dyre et est devenu l'une des souches de programmes malveillants les plus répandues et les plus dangereuses dans le paysage actuel des cyberattaques. Souvent associé à d'autres types de programmes malveillants, TrickBot est quelques fois utilisé comme premier vecteur d'infection pour se frayer un chemin dans l'hôte cible ou pour télécharger d'autres gammes de programmes malveillants afin de tirer le meilleur parti d'une infection.

Ursnif: Le Trojan Ursnif est l'une des variantes les plus actives et les plus répandues de la famille de programmes malveillants Gozi, également connue sous le nom de Dreambot. Il est souvent diffusé par le biais de kits d'exploitation, de pièces jointes d'e-mail et de liens malveillants.

Unruy: Unruy est un Trojan qui affiche des publicités hors contexte et effectue des clics publicitaires afin de récolter des revenus pour ses contrôleurs. Il communique à distance avec les hôtes et peut également télécharger et exécuter des fichiers arbitraires pour mener à bien ses activités.

Mesures nécessaires pour prévenir les menaces cryptées

Il est de plus en plus crucial d'admettre que le trafic SSL n'est pas nécessairement un trafic sécurisé. L'utilisation du cryptage a augmenté aussi bien en entreprise que chez les hackers qui peuvent ainsi dissimuler leurs attaques. Le besoin d'inspecter le trafic crypté est plus grand que jamais. Plusieurs entreprises suivent les meilleures pratiques en matière de sécurité et cryptent leur trafic Internet. Cependant, les outils obsolètes, tels que les pare-feux de nouvelle génération, manquent souvent de performances et de capacités nécessaires pour inspecter le trafic SSL à grande échelle. Impossible d'interrompre les opérations et les flux de travail, ainsi les équipes informatiques autorisent la plupart du trafic chiffré à passer sans aucune inspection.

De plus, il existe des réglementations strictes concernant la façon dont les entreprises doivent traiter les données qui contiennent des informations personnelles sur les clients, les patients, etc. La mise sur pied de politiques distinctes pour la façon dont certains types de données doivent être inspectés avant de les répliquer à différents emplacements est une tâche ardue, si bien que les entreprises ne s'y penchent souvent même pas.

Ainsi, comment pouvez-vous protéger votre entreprise des dangers cachés dans le trafic crypté sans affecter la performance? La majorité du trafic des entreprises étant désormais crypté, comment s'assurer de le décrypter et de l'inspecter en totalité, tout en maintenant la conformité, pour tous les utilisateurs, qu'ils soient sur le réseau ou pas?

- **Décryptez, détectez et empêchez les menaces dans tout le trafic SSL** grâce à une architecture cloud native basée sur le proxy capable d'inspecter tout le trafic de chaque utilisateur.
- **Mettez en quarantaine les attaques inconnues et bloquez les programmes malveillants de type patient zéro** grâce à la mise en quarantaine pilotée par l'IA, laquelle conserve pour analyse les contenus suspects, contrairement aux approches dites passthrough basées sur le pare-feu.
- **Assurez une sécurité cohérente pour tous les utilisateurs et tous les emplacements** afin de garantir à chacun la même sécurité de haute facture, en tout temps, qu'ils soient à la maison, au siège social ou en déplacement.
- **Réduisez instantanément votre surface d'attaque** en optant pour une position zero trust, où il n'existe pas de mouvement lateral. Les applications sont invisibles aux hackers, et les utilisateurs autorisés accèdent directement aux ressources nécessaires, et non à l'ensemble du réseau.

La solution nécessite l'évolutivité et les performances qui ne peuvent être fournies que par une architecture cloud native basée sur le proxy, telle que Zscaler Zero Trust Exchange. Une plate-forme de sécurité axée sur le cloud répond aux exigences de décryptage et d'inspection en faisant évoluer de manière élastique les ressources informatiques et elle fournit une application cohérente des politiques sur plusieurs emplacements. Zscaler effectue l'inspection SSL à grande échelle dans le cadre de sa plate-forme de services, et à mesure que votre trafic augmente. La capacité est ajoutée instantanément et à la demande. Pas besoin d'appliances à dimensionner, à commander ou à expédier.

Aucune industrie n'est à l'abri des menaces de sécurité. Et comme de plus en plus de trafic est crypté, l'inspection de ce trafic est devenue cruciale. Une stratégie multicouche de défense en profondeur qui prend pleinement en charge l'inspection SSL est essentielle pour garantir que les entreprises sont à l'abri des menaces croissantes dissimulées dans leur trafic crypté.

Découvrez comment **Zscaler** peut inspecter l'ensemble de votre trafic SSL sans affecter les performances ni créer des soucis de conformité. Ou vérifiez votre capacité à inspecter le trafic SSL/TLS à l'aide de notre outil **Internet Threat Exposure Analysis**.

À propos de ThreatLabZ

ThreatLabZ est la branche de recherche en sécurité de Zscaler. Cette équipe de classe mondiale est responsable de la chasse aux nouvelles menaces et de s'assurer que les milliers d'organisations qui utilisent la plateforme mondiale Zscaler sont toujours protégées. En plus de la recherche sur les programmes malveillants et de l'analyse comportementale, les membres de l'équipe sont impliqués dans la recherche et le développement de nouveaux modules prototypes pour la protection avancée contre les menaces sur la plateforme Zscaler, et effectuent régulièrement des audits de sécurité internes pour s'assurer que les produits et l'infrastructure de Zscaler répondent aux normes de conformité de sécurité. ThreatLabZ publie régulièrement des analyses approfondies des menaces nouvelles et émergentes sur son portail, **research.zscaler.com**.

À propos de Zscaler

Zscaler (NASDAQ: ZS) accélère la transformation numérique afin que les clients puissent être plus agiles, plus efficaces, plus tenaces et plus sécurisés. La plateforme Zscaler Zero Trust Exchange™ protège des milliers de clients contre les cyberattaques et la perte des données en connectant de manière sécurisée les utilisateurs, les appareils et les applications indépendamment de l'emplacement. Distribué à travers plus de 150 data centers dans le monde, Zero Trust Exchange basé sur SASE est la plus grande plateforme de sécurité cloud inline. Pour en savoir plus, rendez-vous sur zscaler.com ou suivez-nous sur Twitter **@zscaler**.

zscaler™