RAPPORT 2021

IoT dans l'entreprise : édition bureau vide

Que se passe-t-il lorsque les employés abandonnent leurs appareils intelligents au travail ?

zscaler™

Tout au long de l'année 2020 et en 2021, la pandémie de COVID-19 a laissé de nombreux bureaux d'entreprise étrangement silencieux et dépourvus d'employés. Mais en dépit de l'absence évidente d'employés, ces bâtiments bourdonnaient toujours d'activité. Les bâtiments eux-mêmes n'étaient pas les seuls éléments abandonnés : les montres intelligentes, la signalisation digitale, les imprimantes en réseau et de nombreux autres appareils IoT étaient toujours connectés au réseau — actualiser les données, exécutant des fonctions, en attente de commandes.

Les acteurs malveillants l'ont remarqué et beaucoup ont essayé d'en tirer profit. Au milieu de la gigantesque transition mondiale vers le télétravail. Cela se traduit par un ahurissant record de 833 programmes malveillants IoT bloqués toutes les heures.

L'éventail toujours plus large de dispositifs IoT qui se fraie un chemin vers les réseaux d'entreprise englobe un large écosystème, des montres intelligentes aux caméras IP en passant par les automobiles et les appareils musicaux. Soixante-seize pour cent des transactions s'effectuent sur des canaux en texte brut non chiffrés, bien que tous les appareils utilisent le protocole SSL pour au moins un sous-ensemble de leurs communications. Les entreprises doivent appliquer des politiques et des architectures Zero Trust pour protéger leurs réseaux de toute fraude via ces appareils. S'appuyant sur des données provenant du cloud Zscaler recueillies sur deux semaines, ce rapport approfondi de ThreatLabz, l'équipe de recherche de Zscaler sur les menaces, révèle quels sont les dispositifs IoT approuvés ou non approuvés, ainsi que les tendances des programmes malveillants IoT.

Nous allons examiner les données de deux études : une étude sur l'empreinte digitale des appareils IoT qui identifie les appareils IoT et le trafic, et une étude sur les programmes malveillants IoT basée sur les données du cloud Zscaler. Étant donné que les dispositifs IoT — en particulier les dispositifs autorisés — ne disposent pas d'agents, toutes les données de ce rapport représentent des dispositifs et des attaques sur les réseaux d'entreprise dans des bureaux physiques. Les données de ce rapport ont été recueillies entre le 15 et le 31 décembre 2020, lorsque la plupart des bureaux d'affaires non essentiels étaient fermés.

Résultats clés

- Les programmes malveillants IoT sur les réseaux d'entreprise ont augmenté de 700 % depuis notre étude de 2019, bien qu'une grande partie des effectifs du monde entier soit en télétravail.
- Les appareils de divertissement et de domotique présentaient le plus grand risque en raison de leur variété, de leur faible pourcentage de communication chiffrée et de leurs connexions aux destinations suspectes.
- Gafgyt et Mirai — des familles de logiciels malveillants couramment utilisées dans les botnets — représentaient 97 % des charges utiles de programmes malveillants IoT bloquées par le cloud Zscaler.
- Les secteurs de la technologie, de la production, de la vente en gros et au détail, ainsi que des soins de santé représentent 98 % des victimes d'attaques IoT.
- La plupart des attaques provenaient de Chine, des États-Unis, et d'Inde.
- La plupart des cibles d'attaques IoT étaient en Irlande, aux États-Unis et en Chine.

Empreinte digitale des dispositifs IoT

Appareils les plus courants

En examinant plus d'un demi-milliard de transactions de dispositifs IoT, ThreatLabz a identifié 553 types d'appareils différents provenant de 212 fabricants et les a classés en 21 catégories. Les trois catégories les plus courantes — soit près de 65 % du total des appareils — étaient des décodeurs (29 %), des téléviseurs connectés (20 %) et des montre connectées (15 %).

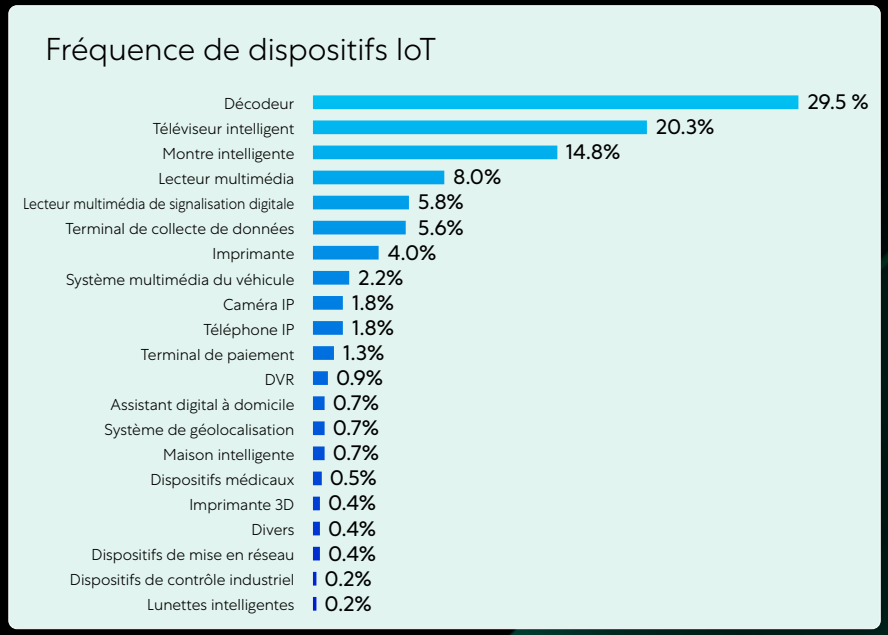
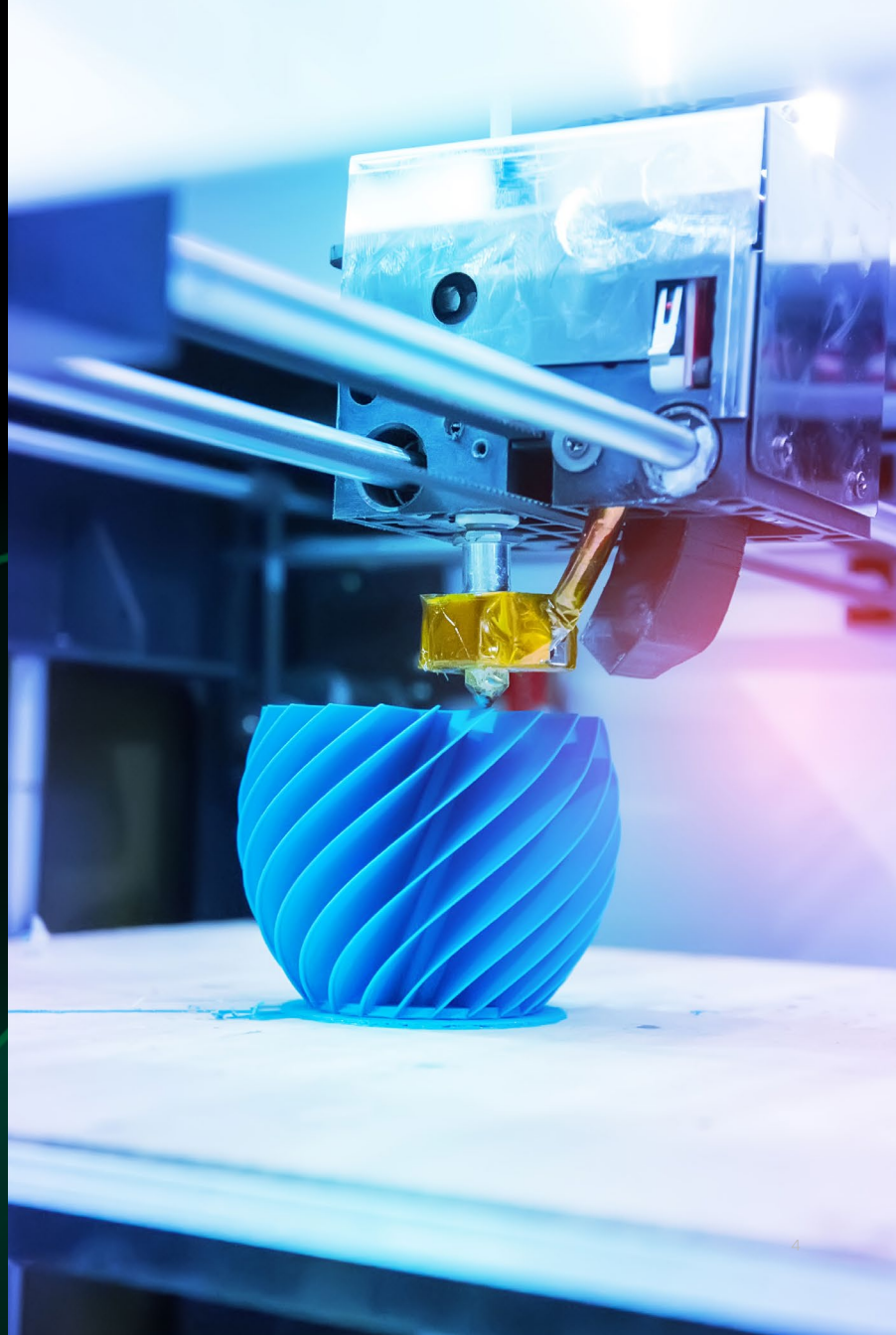


Figure 1 : fréquence des dispositifs IoT



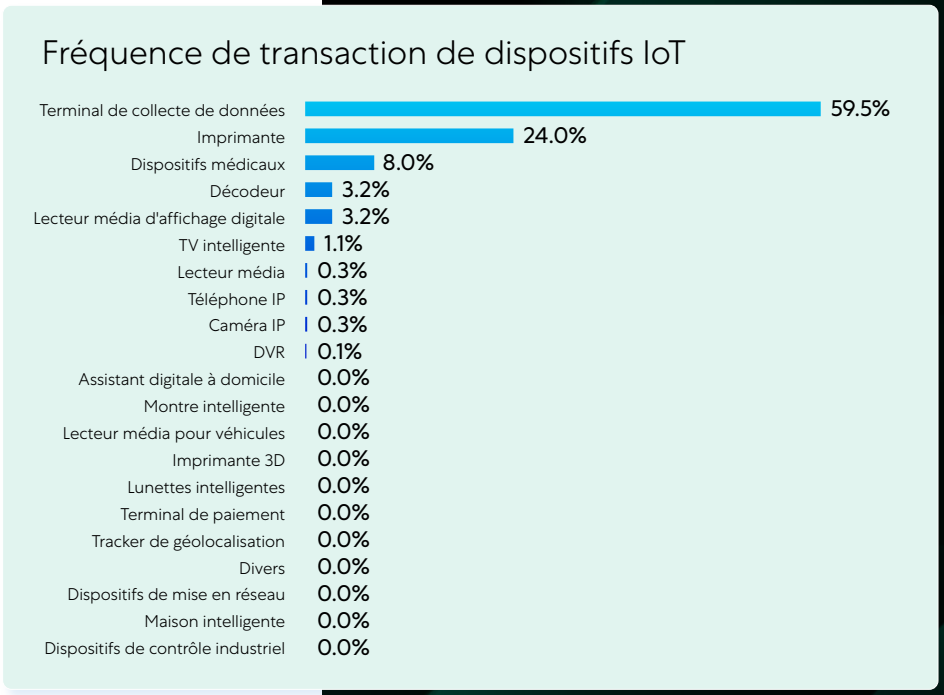
L'Internet des meubles musicaux ?

L'"Internet des objets" continue d'évoluer vers de nouvelles catégories, dont certaines pourraient être complètement en dehors du radar des équipes informatiques. ThreatLabz a découvert un certain nombre d'appareils insoupçonnés se connectant au cloud, notamment :

- **Réfrigérateurs intelligents :** un réfrigérateur intelligent Samsung a la possibilité de diffuser de la musique, des vidéos et du contenu depuis le téléphone du propriétaire vers un écran sur le battant du réfrigérateur.
- **Lampe musicale :** Ikea et Sonos ont créé une lampe de table combinée à un lecteur multimédia intelligent Symfonisk.
- **Automobiles :** lTesla et Honda proposent des lecteurs automobiles multimédias qui se connectent aux réseaux d'entreprise.
- **Cartes mémoire Wi-Fi :** les cartes mémoire Wi-Fi de Eye Fi, généralement utilisées dans les caméras pour stocker et partager des photos, envoyaient du trafic via le cloud Zscaler.

Appareils les plus bavards

Les transactions d'appareils IoT représentaient 0,038 % du total des transactions sur le cloud Zscaler pendant la période de deux semaines. Certains appareils représentaient beaucoup plus de transactions que d'autres, les terminaux de collecte de données et les imprimantes représentant plus de 80 % du trafic IoT total en eux-mêmes, comme le montre la Figure 2.



Base : 575 091 158 transactions de dispositifs IoT
Figure 2 : transactions de dispositifs IoT

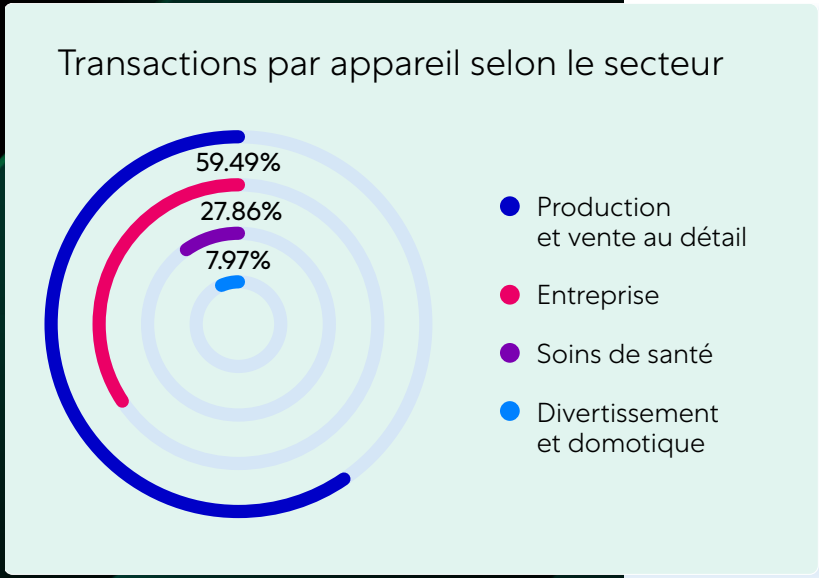


Figure 3 : dispositifs IoT par type

Trafic par appareil – classification verticale

Les dispositifs IoT ont également été regroupés en quatre catégories en fonction des secteurs les produisant :

- **Les appareils destinés à la production ou à la vente au détail** représentaient 59 % des transactions et comprenaient 57 types d'appareils différents provenant de 20 fabricants, notamment des imprimantes 3D, des systèmes de géolocalisation, des dispositifs de contrôle industriel, des systèmes multimédia automobiles, des terminaux de collecte de données et des terminaux de paiement.
- **Les appareils d'entreprise** représentaient 28 % des transactions et comprenaient des lecteurs médias de signalisation digitale, des enregistreurs vidéo digitales, des caméras et des téléphones IP, des imprimantes et des appareils de mise en réseau.
- **Les dispositifs de soins de santé** représentaient huit pour cent des transactions et comprenaient un certain nombre d'appareils médicaux provenant principalement de trois fabricants : GE Healthcare, Abbott Laboratories et HOLOGIC.
- **Les appareils de divertissements et de domotique** représentaient cinq pour cent des transactions générées à partir d'une grande variété d'appareils tels que les assistants digitaux domestiques, les lecteurs multimédias, les décodeurs, les lunettes intelligentes, les appareils domestiques intelligents, les téléviseurs intelligents et les montres intelligentes. Bien que ces appareils aient représenté le plus faible pourcentage de transactions, ils étaient les plus variés et comprenaient un certain nombre d'appareils grand public — un total de 420 appareils provenant de 150 fabricants différents.

Les dispositifs IoT communiquent la plupart du temps en texte brut

ThreatLabz a observé que 76 % des transactions totales effectuées à partir de dispositifs IoT l'ont été sur des canaux en texte brut, et que 24 % des transactions seulement l'ont été sur des canaux chiffrés sécurisés. Même si ce ratio semble incroyablement faible, il est presque trois fois supérieur à notre étude de 2019, dans laquelle seuls 8,5 % des communications IoT étaient chiffrées. Néanmoins, le risque de sécurité persiste : il est beaucoup plus aisé pour les pirate informatique d'espionner ou, pire encore, d'intercepter et de modifier des communications en texte clair, ce qui leur permet d'exploiter les dispositifs IoT à des fins malveillantes.

L'ensemble des 553 appareils observés au cours de l'étude utilisaient dans une certaine mesure le protocole SSL, mais le pourcentage de communications réellement chiffré variait largement selon le type d'appareil. Les dispositifs de divertissement à domicile et d'entreprise communiquaient presque entièrement en texte brut, tandis que les dispositifs de soins de santé communiquaient via SSL environ la moitié du temps.

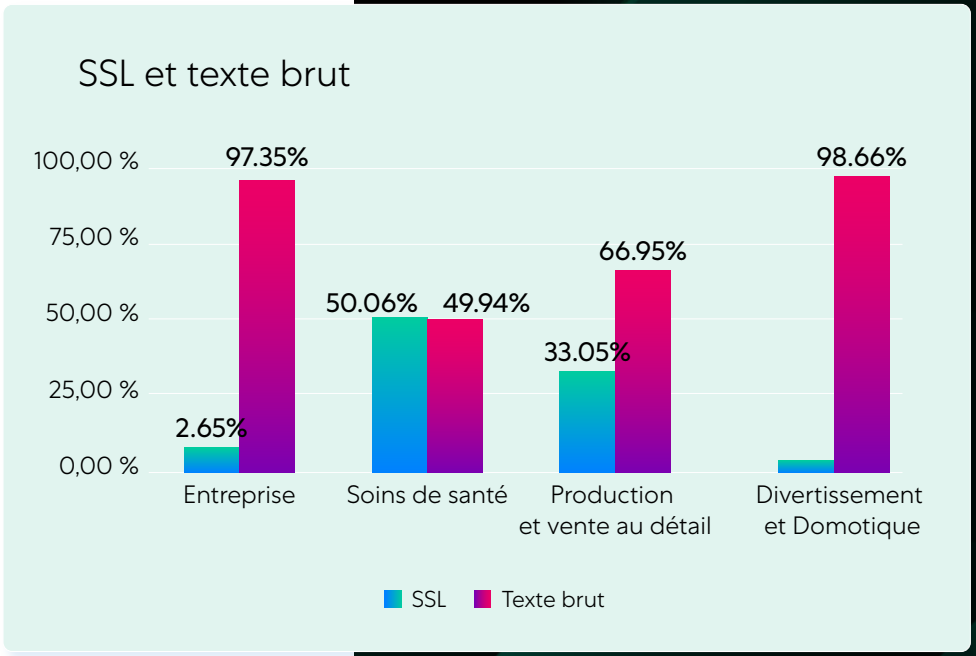


Figure 4 : pourcentage de communications chiffrées par type d'appareil

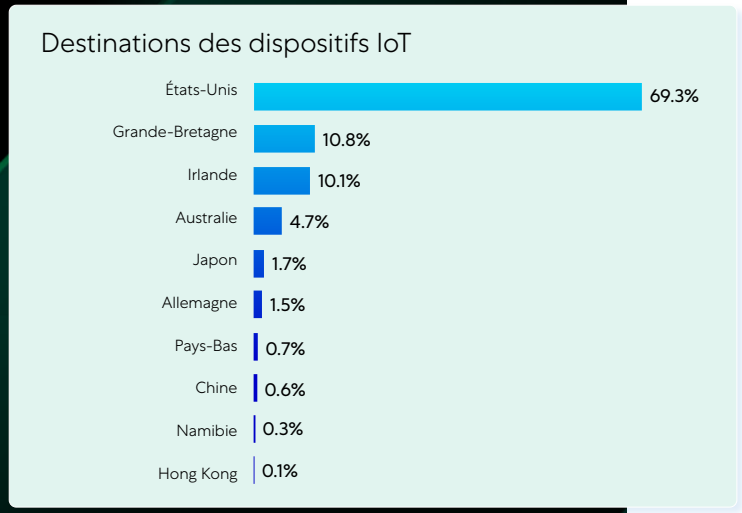


Figure 5 : principales destinations des communications IoT

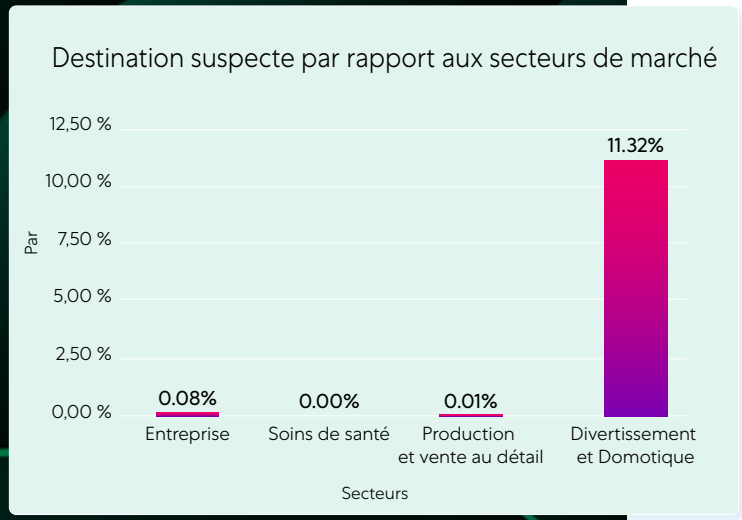


Figure 6 : pourcentage de trafic suspect par type d'appareil

Quels sont les pays avec lesquels les dispositifs IoT échangent ?

ThreatLabz a examiné les pays vers lesquels les dispositifs IoT acheminaient les données — appelés "destinations". La plupart de ces communications sont légitimes, les dispositifs IoT faisant ce pour quoi ils sont conçus, c'est-à-dire envoyer et recevoir des données. Les États-Unis étaient de loin la destination principale, recevant 69 % du trafic, suivie par la Grande-Bretagne (11 %) et l'Irlande (10 %). Les dix principaux pays de destination sont affichés ci-dessous.

Les dispositifs de divertissement et de domotique sont beaucoup plus susceptibles d'être acheminés vers la Chine et la Russie

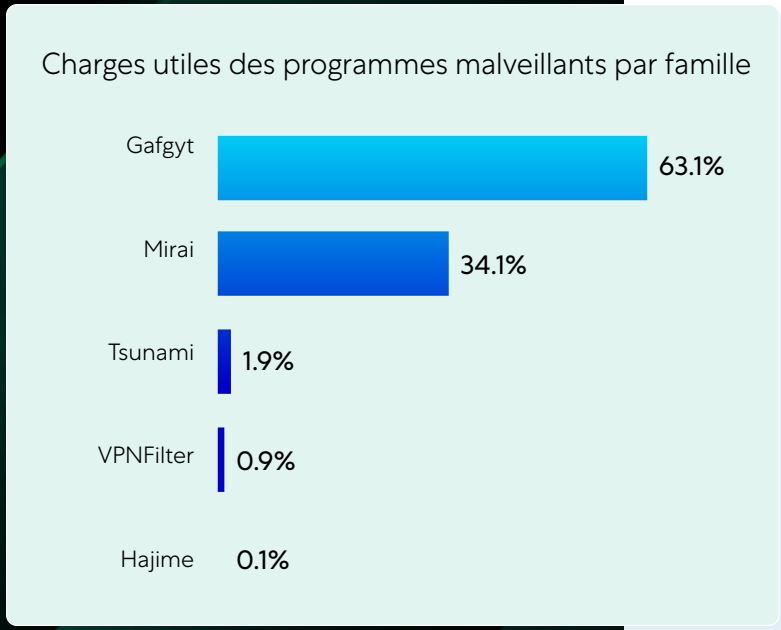
Onze pour cent du trafic provenant des appareils de divertissement et de domotique était destiné à la Chine et à la Russie. Bien qu'une grande partie de ce trafic soit légitime et non malveillant, il s'agit de destinations que ThreatLabz considère suspectes en raison de leur potentiel d'espionnage par le gouvernement et d'autres vulnérabilités de données. La quasi-totalité (99,9 %) de ce trafic suspect provenait de téléviseurs intelligents et de décodeurs.

À l'inverse, les dispositifs conçus pour les entreprises, les soins de santé, la production et la vente au détail avaient collectivement moins de 0,1 pour cent de leur trafic aller-retour vers des destinations suspectes.

Étude sur les programmes malveillants IoT

Au cours des deux semaines où nous avons mené notre étude sur l'empreinte digitale IoT, ThreatLabz a également examiné les activités spécifiques aux programmes malveillants IoT dans le cloud de Zscaler.

ThreatLabz a observé environ 300 000 transactions bloquées ayant un lien avec des logiciels malveillants IoT, des exploitations et des communications de commande et de contrôle, ce qui représente une augmentation de près de 700 % par rapport à l'année précédente. En ce qui concerne le volume de transaction des programmes malveillants, nous avons observé un total de 18 000 hôtes uniques et environ 900 livraisons uniques de charges utiles sur une période de 15 jours.



Base : 900 charges utiles
Figure 7 : charges utiles de programmes malveillants uniques par famille

Principales menaces liées à l'IoT

Gafgyt et Mirai étaient de loin les deux familles de programmes malveillants IoT les plus prolifiques dans notre étude. En fait, 97 % des 900 livraisons de charges utiles uniques que nous avons observées appartenaient à ces deux familles. Les autres familles actives comprenaient Tsunami, VPNFilter et Hajime.

Alors que Gafgyt disposait des charges utiles les plus uniques, les charges utiles des malwares Mirai étaient plus fréquemment utilisées dans les attaques IoT pendant notre étude. En ce qui concerne les volumes de transactions, 76 % des attaques bloquées provenaient de la famille de malwares Mirai, 5 % de Gafgyt et 19 % d'autres familles.

Botnets IoT
Les exploits de dispositifs IoT peuvent fournir aux pirate informatique un accès à la fois à l'appareil et aux réseaux connectés, rendant possible toutes sortes d'activités malveillantes. Mirai et Gafgyt sont particulièrement connus pour utiliser des appareils pour créer des botnets — des réseaux d'appareils sous le contrôle d'un hacker qui permettent des attaques coordonnées à grande échelle. Les botnets ont été utilisés pour des attaques par déni de service distribué (DDoS), des violations financières, l'exploration de crypto-monnaies et des intrusions ciblées, pour n'en citer que quelques-unes. Le botnet Mirai est connu pour avoir mené ce qui a été la plus grande attaque DDoS de l'histoire en 2016, provoquant des pannes Internet généralisées. ThreatLabz a évalué une tentative de rappel par botnet dans le cadre de cette étude sur les programmes malveillants, et a constaté que les hackers ciblaient non seulement les dispositifs IoT, mais aussi un certain nombre de routeurs populaires et d'autres appareils de mise en réseau pour mener à bien ces attaques :

Principaux dispositifs de rappel botnet	
Vidéosurveillances et enregistreurs digitales de plus de 70 fournisseurs	MVPower DVR
Plusieurs appareils utilisant le SDK Realtek avec le miniigd daemon	Appareils Linksys
Huawei HG532	Appareils Netgear R7000/R6400
Routeur zyXEL	Routeurs Netgear DGN1000
Routeurs Dasan GPON	Appareils D-Link
Routeurs Eir D1000	Appareils Vacron NVR
Appareils D-Link	

Secteurs les plus ciblés

Les entreprises technologiques ont connu le taux d'attaque le plus élevé des programmes malveillants IoT, ce qui représente 40 % des infections. Les secteurs les plus ciblés étaient la production (28 %) et la vente en gros et au détail (24 %).

Pays menant le plus d'attaques de programmes malveillants

D'après notre étude, 88,5 % des dispositifs IoT compromis acheminaient les données vers des serveurs situés dans l'un de ces trois pays : la Chine (56 %), les États-Unis (19 %) ou l'Inde (14 %). Ceux-ci sont connus sous le nom de pays "destinataires de programmes malveillants" et, dans chaque cas, ils ont soit directement fourni le logiciel malveillant, soit se sont connectés à lui après l'infection. Certains hackers mettront en place des serveurs de commande et de contrôle dans le pays qu'ils ciblent, de sorte que l'emplacement du serveur ne pourrait pas nécessairement indiquer l'emplacement réel du hacker.

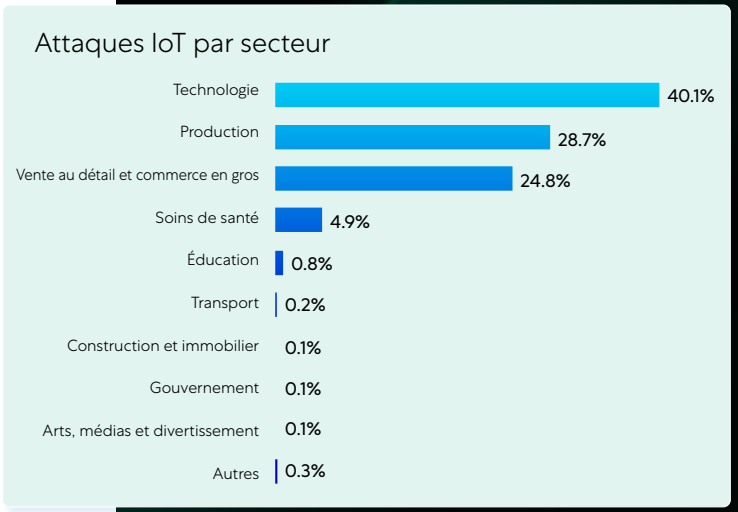


Figure 8 : attaques IoT par secteur

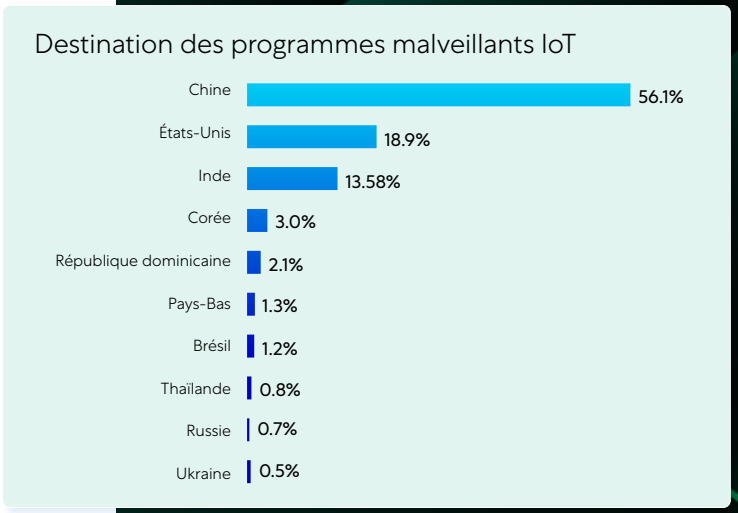


Figure 9 : principales destinations pour les logiciels malveillants IoT

Principaux Systèmes Autonomes des acteurs malveillants

ThreatLabz a effectué une analyse plus approfondie des destinations des logiciels malveillants, et a identifié les principaux numéros de système autonome (ASN) et les adresses IP se connectant aux logiciels malveillants IoT :

ASN	IP	Nom du système autonome
16276	158.69.0.77	OVH, FR
398468	193.42.137.107	VMSNETWORKS, US
213035	193.239.147.144	SERVERION-AS Serverion B.V., NL
36352	107.173.125.167	AS-COLOCROSSING, US
202448	86.105.252.203	MVPS https://www.mvps.net, CY
46606	162.241.126.53	UNIFIEDLAYER-AS-1, US
53667	198.251.81.249	PONYNET, US
212953	46.102.106.25	MRS-BILISIM, TR
35913	45.15.143.175	DEDIPATH-LLC, US
213371	37.49.230.52	SQUITTER-NETWORKS, NL
35913	45.15.143.140	DEDIPATH-LLC, US
42864	45.95.169.218	GIGANET-HU GigaNet Internet Service Provider Co, HU
63916	103.42.214.181	IPTELECOM-AS-AP IPTELECOM Global, HK
134520	103.42.214.181	GIGSGIGSCLOUD-AS-AP GigsGigs Network Services, HK
3462	111.248.163.38	HINET Data Communication Business Group, TW
36352	107.173.181.189	AS-COLOCROSSING, US
36352	192.227.147.157	AS-COLOCROSSING, US
212369	45.155.125.116	TRDESERVER, TR
206898	185.172.110.205	BLADESERVERS, AU
213035	193.239.147.245	SERVERION-AS Serverion B.V., NL

Figure 10 : principaux ASN d'acteurs malveillants

Principales cibles des programmes malveillants IoT

ThreatLabz a également évalué les "pays sources" — les cibles de programmes malveillants — sur la base de l'adresse IP du client. Les trois principales nations victimes d'attaques IoT étaient l'Irlande (48 %), les États-Unis (32 %) et la Chine (14 %).

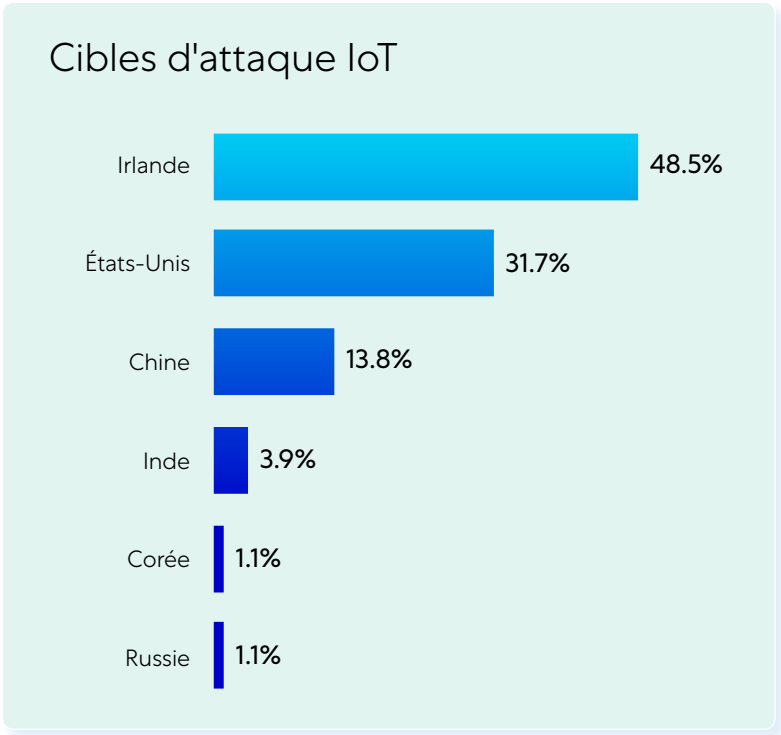


Figure 12 : principaux pays sources de logiciels malveillants IoT

Principes fondamentaux de la défense contre les logiciels malveillants IoT

Alors que la liste des appareils "intelligents" dans le monde s'étend au quotidien, il est presque impossible de les empêcher de pénétrer au sein de votre entreprise. Il est donc essentiel de mettre en place des politiques d'accès qui empêchent ces appareils de servir de porte d'accès à vos données et applications sensibles.

Les meilleures pratiques suivantes vous permettront de vous assurer que vous pouvez juguler la menace des logiciels malveillants IoT, tant avec des appareils autorisés que sanctionnés :

- **Suivre et gérer vos périphériques réseau.** De nombreux appareils IoT ne sont pas gérés ; vous ne pouvez donc pas compter uniquement sur les données des agents de terminaux pour savoir quels appareils sont utilisés sur vos sites. Déployez une solution qui examine les journaux réseau pour comprendre quels appareils communiquent actuellement sur votre réseau ainsi que la nature de leur activité. Mettez en œuvre des architectures qui vous permettent d'inspecter à la fois le trafic réseau chiffré et non chiffré pour les communications d'appareils dont vous n'auriez absolument aucune connaissance autrement. Ensuite, déployer des mesures de protection.

- **Modifier les mots de passe par défaut.** C'est une histoire aussi vieille que l'informatique, mais l'un des moyens les plus simples et les plus courants pour les hackers d'exploiter les appareils est d'utiliser leurs mots de passe par défaut. Le contrôle des mots de passe peut ne pas être possible pour les appareils IoT non autorisés, mais il s'agit d'un indispensable prérequis pour le déploiement d'appareils IoT appartenant à l'entreprise, et devrait faire partie de votre formation à la sécurité pour tous les appareils que les employés utilisent au travail.

- **Rester au fait des correctifs et des mises à jour.** De nombreux secteurs — en particulier ceux de la production et des soins de santé — s'appuient sur les dispositifs IoT pour leurs flux de travail quotidiens. Pour ces appareils autorisés, assurez-vous de rester informé quant à toute nouvelle vulnérabilité détectée et de maintenir à jour la sécurité de votre appareil avec des correctifs.

- **Mettre en œuvre une architecture de sécurité Zero Trust.** Appliquez des politiques strictes pour vos actifs d'entreprise afin que les utilisateurs et les appareils puissent accéder uniquement à ce dont ils ont besoin, et uniquement après authentification. Limitez la communication aux adresses IP, aux ASN et aux ports pertinents nécessaires à l'accès externe. Les dispositifs IoT non autorisés nécessitant un accès Internet doivent faire l'objet d'une inspection du trafic et ne pas pouvoir accéder aux données d'entreprise, de préférence par le biais d'un proxy. La seule façon d'empêcher les dispositifs IoT fantômes d'exposer les réseaux d'entreprise à une menace est d'éliminer les politiques de confiance implicite et de contrôler étroitement l'accès aux données sensibles à l'aide d'une authentification dynamique basée sur l'identité — également appelée Zero Trust.

À propos de ThreatLabZ

ThreatLabz est la branche de recherche en sécurité de Zscaler. Cette équipe d'élite a la responsabilité de traquer les nouvelles menaces et de veiller à ce que les milliers d'entreprises qui utilisent la plateforme mondiale Zscaler Zero Trust Exchange™ soient en permanence protégées. En plus de la recherche et de l'analyse comportementale des programmes malveillants, les membres de l'équipe sont impliqués dans la recherche et le développement de nouveaux modules de prototype 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 Zscaler répondent aux normes de conformité en matière 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 digitale de sorte que les clients deviennent plus agiles, plus efficaces, plus résilients et plus en sécurité. 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**.