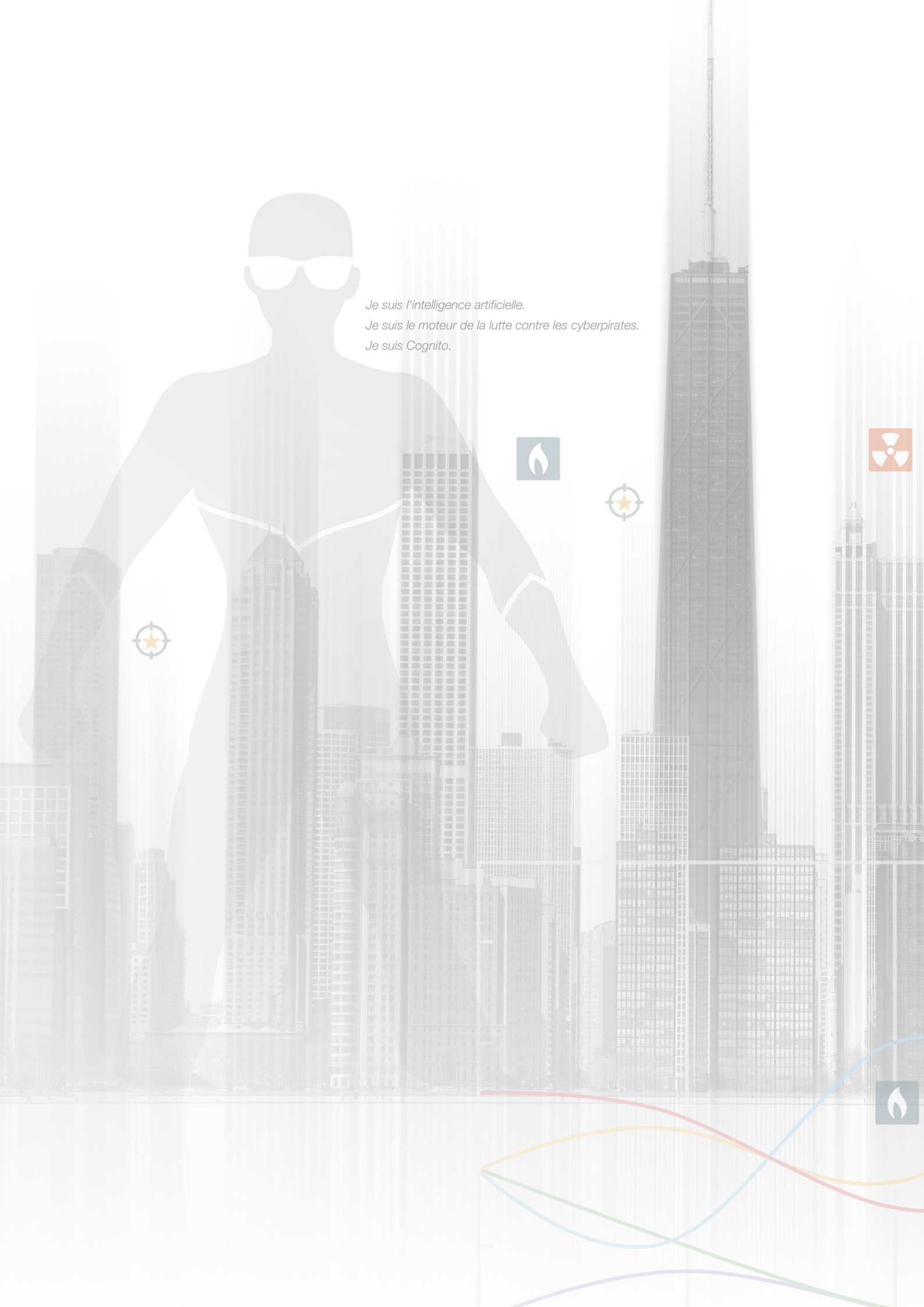
VECTRA

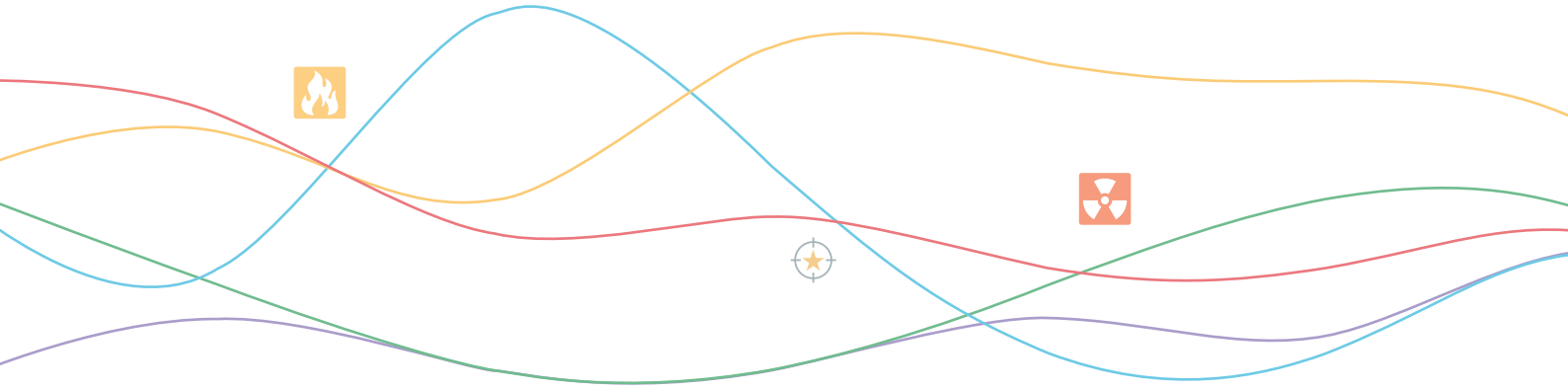
Tendances des comportements d'attaque en entreprise

Édition RSA Conference 2018


Je suis l'intelligence artificielle.
Je suis le moteur de la lutte contre les cyberpirates.
Je suis Cognito.

VECTRA

SOMMAIRE



Le rapport *Tendances des comportements d'attaque en entreprise* de Vectra®, édition RSA Conference 2018, examine les comportements d'attaque actifs et persistants observés chez nos clients d'août 2017 à janvier 2018, au sein de réseaux d'entreprises, de centres de données et d'environnements cloud.

Cette étude menée sur le terrain repose sur une approche multidisciplinaire couvrant toutes les phases stratégiques du cycle d'attaque. Vectra recourt à la plate-forme Cognito™, basée sur l'intelligence artificielle, pour détecter les comportements d'attaque. Nous pouvons ainsi identifier les points vulnérables et sources de risques au sein des entreprises et mettre en lumière des indicateurs signalant des compromissions potentiellement dommageables.

Principales observations

- Tous secteurs d'activités confondus, le volume moyen des détections de comportements d'attaque atteint 1 429 détections pour 10 000 systèmes.
- Le volume le plus élevé a été observé dans le secteur de l'enseignement supérieur (avec 3 715 détections pour 10 000 systèmes), suivi de celui de l'ingénierie (2 918 pour 10 000 systèmes). Ces volumes s'expliquent par l'activité liée aux communications C&C (Command & Control) dans le secteur de l'enseignement supérieur et aux opérations de reconnaissance dans le secteur de l'ingénierie.
- Dans l'enseignement supérieur, l'activité C&C est quatre fois plus importante que la moyenne de tous les secteurs (460 détections pour 10 000 systèmes), soit 2 205 détections pour 10 000 systèmes. Ces communications constituent des indicateurs précoces d'attaques en cours, car elles surviennent dès les premières phases du cycle. Elles sont souvent associées à des comportements opportunistes de botnets.
- Les secteurs de l'administration publique et des technologies présentent les taux de détection les plus faibles, avec respectivement 496 et 349 détections pour 10 000 systèmes. Ces bons résultats pourraient être la conséquence de politiques de sécurité plus rigoureuses, de procédures de résolution d'incidents abouties et d'un meilleur contrôle de la surface d'attaque.
- L'activité associée aux botnets est la plus fréquente dans le secteur de l'enseignement supérieur, avec 151 détections pour 10 000 systèmes, soit cinq fois plus que la moyenne tous secteurs confondus (33 détections pour 10 000 systèmes). Les botnets ont des comportements opportunistes : ils piratent des systèmes et les exploitent pour lancer des attaques contre d'autres cibles pour réaliser des profits, par exemple par l'envoi de spam ou par l'extraction de bitcoins.
- Les clients de Vectra ont vu la charge de travail de leurs analystes de niveau 1 divisée par 32 en ce qui concerne la détection, le tri, la corrélation et la classification par priorité des incidents de sécurité, ce qui leur a permis de se concentrer sur les systèmes compromis posant le risque le plus aigu.
- En normalisant les détections par rapport à l'année dernière sur la base d'un ratio de 10 000 systèmes, on constate, dans tous les secteurs, une nette augmentation des détections de type communications C&C, opérations de reconnaissance, déplacement latéral et exfiltration des données.

Contexte et méthodologie

Les données figurant dans ce rapport s'appuient sur des métadonnées anonymisées collectées auprès de clients de Vectra qui ont accepté de nous communiquer leurs indicateurs de détection. Afin d'identifier les comportements révélant une attaque en cours, Vectra surveille directement tout le trafic et les journaux pertinents. Citons par exemple le trafic Internet entrant et sortant, le trafic interne entre les équipements réseau, ou encore les charges de travail virtualisées dans les centres de données privés et les clouds publics.

Cette analyse nous procure une visibilité importante sur les phases avancées des attaques. La plate-forme Cognito de Vectra détecte les menaces qui contournent les contrôles de sécurité périmétriques et observe la progression de l'attaque après la compromission initiale.

Ce rapport présente également des données classées par secteur et met en évidence les différences pertinentes entre secteurs.

Entre **août 2017 et janvier 2018**, Vectra a surveillé quelque **4,6 millions de systèmes et charges de travail**. Sur ceux-ci, nous avons détecté plus de **12 millions de comportements d'attaque différents**, que nous avons ensuite examinés pour aboutir à **652 000 détections**.

Ces détections ont ensuite été triées pour ramener le nombre de **systèmes et charges de travail à 373 000**. Sur l'ensemble des clients qui ont pris part à cette étude, en un mois, plus de **6 000** systèmes et charges de travail ont été classés dans la catégorie « **critique** » et plus de **9 000** dans la catégorie « **risque élevé** ». Cette classification a permis aux analystes en sécurité de réagir rapidement à ces menaces et de les neutraliser.

Efficacité opérationnelle et retour sur investissement

En matière de cybersécurité, l'efficacité opérationnelle optimale ne s'obtient qu'au prix d'efforts constants. Les entreprises sont appelées à contrer un nombre infini de risques, de menaces et de cyberpirates à l'aide de ressources limitées. Dès lors, les produits de sécurité doivent toujours être évalués selon deux critères : leur efficacité, bien sûr, mais aussi leur incidence sur le bon fonctionnement opérationnel de l'entreprise.

Le temps est le facteur le plus important dans la détection des intrusions réseau. Pour limiter les dommages éventuels, il est nécessaire de déceler les attaques en temps réel, avant que des données essentielles n'aient pu être volées ou détruites. Cependant, identifier et neutraliser les attaques ciblées prend un temps considérable et oblige les équipes de sécurité à examiner manuellement d'innombrables alertes.

Grâce à l'intelligence artificielle, Vectra exécute une traque continue et automatisée des menaces pour détecter les comportements d'attaque en temps réel. Ces comportements sont mis en corrélation avec les systèmes compromis, qui sont à leur tour corrélés avec les vecteurs d'attaque courants et les campagnes d'attaque de grande envergure. Plusieurs milliers d'indicateurs de menaces sont distillés de façon à obtenir quelques centaines

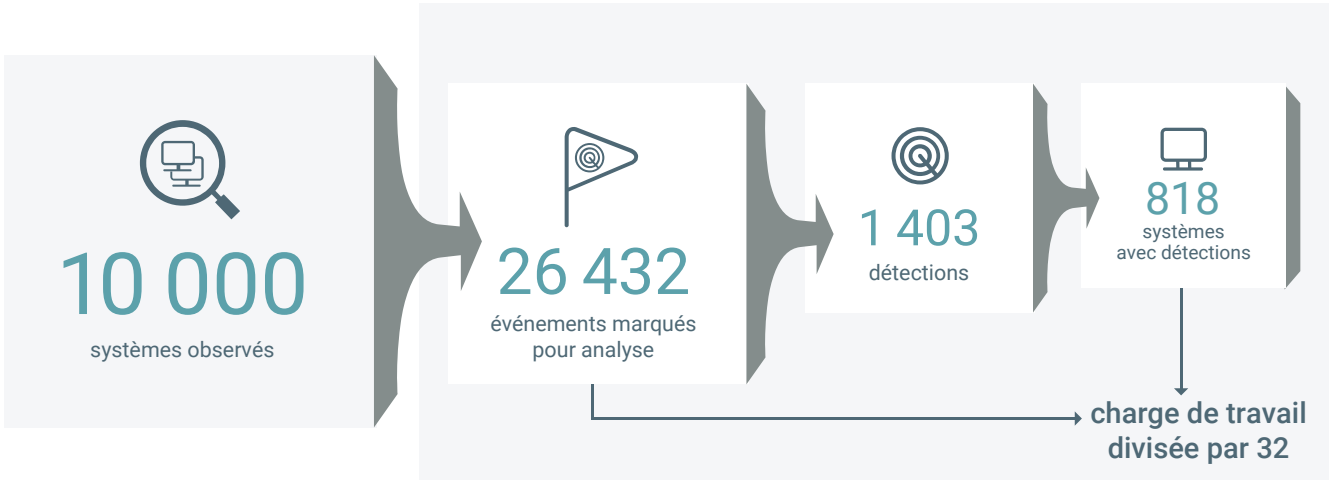
de comportements d'attaque sur des dizaines de systèmes susceptibles de faire partie d'une campagne de grande ampleur.

Il est important de noter que les comportements caractéristiques des cyberpirates constituent des indicateurs de compromission. Les analystes en sécurité doivent déterminer de façon concluante si une attaque est effectivement en cours. Cognito leur fournit les informations cruciales et le contexte nécessaires pour prendre une décision avant qu'une attaque ne cause des dommages.

Les réseaux que nous avons analysés étaient très différents en termes de taille, allant de quelques centaines de systèmes à plus de 400 000 pour les plus grands d'entre eux.

Pour prendre en compte ces écarts, nous avons normalisé les données en prenant comme référence un réseau constitué de 10 000 systèmes et charges de travail. Cette normalisation a permis de comparer plus facilement la prévalence des menaces dans un réseau en considérant le nombre de systèmes. Dans le cadre de cette étude, un « système » est un équipement doté d'une adresse IP, ce qui inclut les appareils connectés à l'Internet des objets (IoT), les smartphones, les tablettes et les ordinateurs portables. La surveillance porte sur ces systèmes ainsi que sur les serveurs et les charges de travail virtualisées.

Réduction de la charge de travail des analystes en sécurité de niveau 1



Globalement, Vectra a permis de diviser par 32 la charge de travail d'investigation des analystes en sécurité par rapport aux procédures manuelles requises pour analyser tous les comportements d'attaque et les systèmes compromis.

Attribution de scores

La plate-forme Cognito de Vectra surveille les systèmes individuels et les charges de travail pendant des périodes prolongées, identifie tous ceux qui présentent un comportement suspect et évalue ces détections. Les scores de détection attribués et le moment où la détection a lieu sont des paramètres essentiels pour déterminer les scores des systèmes.

Ces scores sont composés de deux indicateurs dynamiques : le score de risque et le score de certitude, appliqués à chaque détection et aux systèmes auxquels ils se rapportent.

Le score de risque d'une détection exprime le potentiel de danger si l'événement de sécurité est validé (p. ex. en cas d'activité de spam ou d'exfiltration de données). Puisqu'il s'agit d'une mesure du dommage potentiel, il est calculé selon une perspective pessimiste.

Le score de certitude d'une détection traduit la probabilité qu'un événement de sécurité se soit produit (p. ex. la probabilité que du spam soit envoyé ou que des données soient exfiltrées), à la lumière des indices observés à ce stade.

La certitude est fondée sur l'importance de l'écart entre le comportement malveillant qui a conduit à la détection et un comportement normal. Ainsi, le score de certitude d'une détection évolue au fil du temps.

Étant donné la nature dynamique des détections, l'évolution des scores de détection a des répercussions sur les scores affectés aux systèmes. Les scores critiques ou élevés permettent aux analystes en sécurité d'établir des priorités en matière d'investigation, puisque ces scores correspondent à des comportements d'attaque dont le degré de certitude et le potentiel dommageable sont les plus élevés.

D'autres facteurs influencent les scores des systèmes, notamment la répétition d'une détection observée, ou la combinaison de détections indiquant qu'une cyberattaque progresse vers la réalisation de son objectif.

Chaque type de détection a une durée de vie maximale, qui va de quelques jours à un mois. Lorsqu'une détection ne présente aucune activité récurrente, son effet sur le score du système décline lentement pour finalement devenir nul. Au terme de sa durée de vie, une détection devient inactive et n'a plus aucun impact sur le score du système.

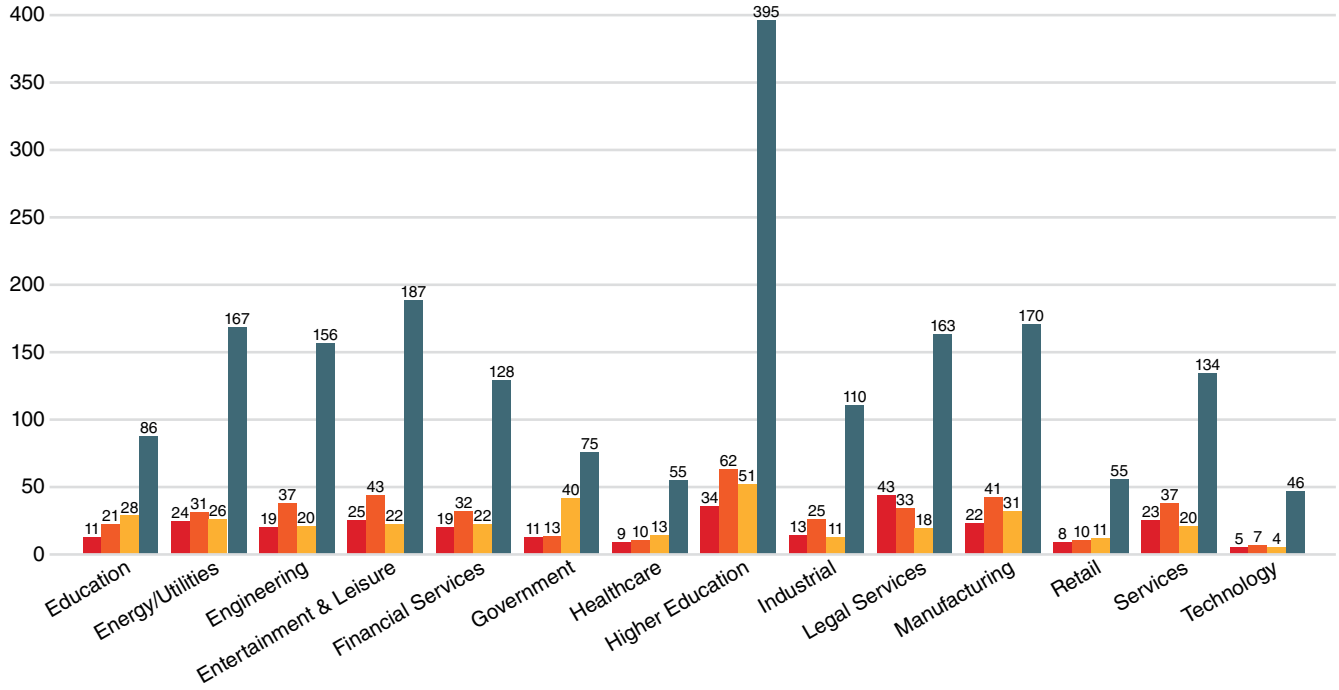
Sur 10 000 systèmes et charges de travail surveillés pendant un mois, 13 en moyenne ont été classés dans la catégorie « *critique* » et 21 dans la catégorie « *élevé* ». Ces éléments représentent la plus grave menace pour l'organisation et nécessitent l'attention immédiate des analystes en sécurité.

Vectra a classé par niveau de gravité le volume de systèmes et de charges de travail, pour chaque secteur et par rapport à la moyenne générale, comme illustré dans le diagramme ci-dessous.

Par exemple, le nombre d'alertes de niveau faible dans le secteur de l'enseignement supérieur est plus de trois fois supérieur au taux normal, ce qui indique des comportements d'attaque opportunistes.

Inversement, le secteur des technologies affiche un faible volume de systèmes présentant des alertes de niveau élevé ou critique. En d'autres termes, les cyberpirates qui ciblent ce secteur progressent rarement jusqu'aux phases ultérieures du cycle d'attaque.

An overview of detections per 10,000 devices and workloads



Tendances globales en matière de détection

- **Taux de détection :** Pour chaque série de 10 000 systèmes surveillés en un mois, nous avons identifié des détections de menaces sur 818 systèmes en moyenne. Le nombre d'événements de sécurité à investiguer et à trier a donc été divisé par 32.
- **L'activité liée aux communications C&C représente les plus hauts pourcentages de détections :** Ce trafic constitue une composante fondamentale des attaques par botnet ainsi qu'un vecteur pour l'exécution des phases ultérieures d'une attaque ciblée. Il est souvent le premier signe d'une attaque dans le cadre d'activités ciblées et opportunistes.
- **Cognito de Vectra assure un gain d'efficacité aux équipes de sécurité :** Même si les symptômes d'attaques ciblées se manifestent toujours fréquemment, des signes encourageants portent à croire que les équipes de sécurité détectent et bloquent les attaques plus rapidement, avant qu'elles ne causent des dommages.
- **Les bitcoins posent un problème grandissant :** Bien que le minage de bitcoins soit considéré comme une activité opportuniste, il connaît une forte hausse, sans doute liée à la montée en flèche du prix du bitcoin. Ces comportements sont observés essentiellement dans le secteur de l'enseignement supérieur, du fait de la vulnérabilité des systèmes des étudiants, mais aussi du minage réalisé par ces derniers.

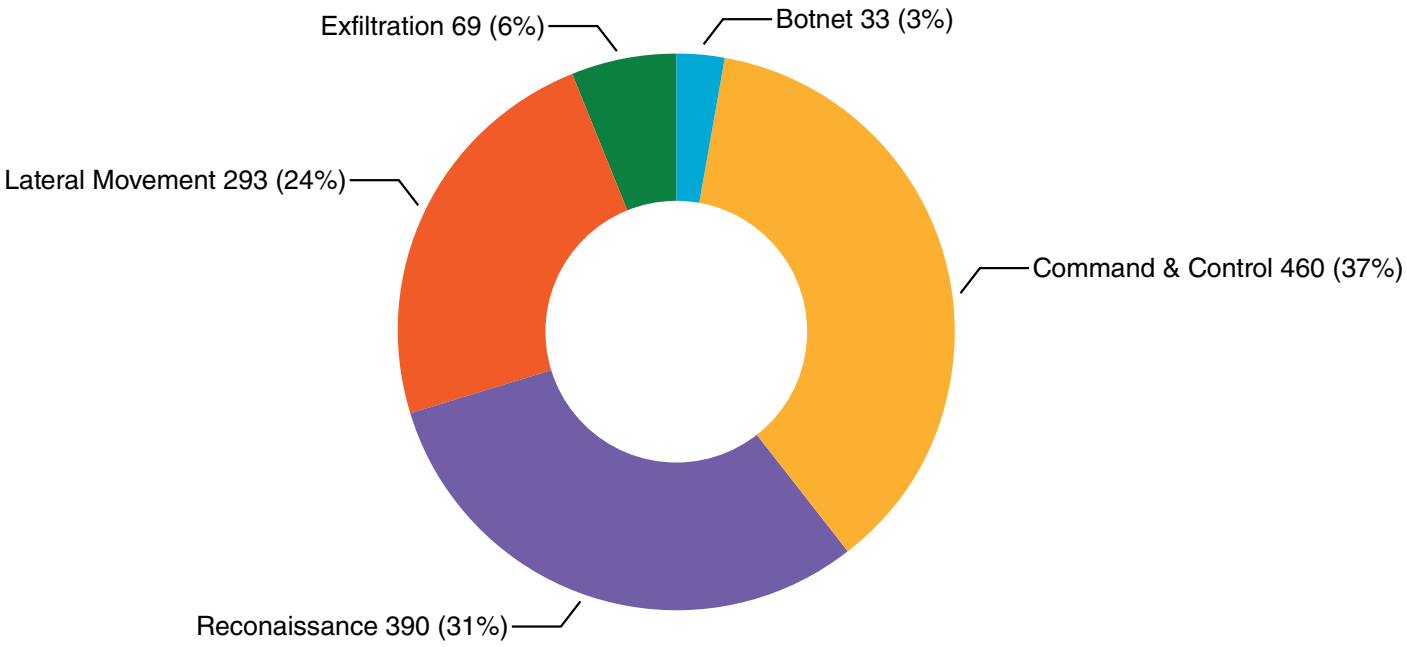
Menaces pour 10 000 systèmes, par type

Afin d'approfondir l'analyse, Vectra présente également les statistiques de détection réparties par secteur. Les diagrammes ci-dessous illustrent les comportements malveillants tout au long du cycle d'attaque. Ces comportements constituent des indicateurs fiables d'exposition et de risque d'une entreprise : ils permettent aux analystes en sécurité de focaliser leur temps et leurs efforts sur les menaces et ressources prioritaires.

Si une attaque ne comporte pas nécessairement toutes les phases du cycle, ces phases sont étroitement liées et il arrive souvent qu'une attaque progresse d'une phase à la suivante pour parvenir à son objectif final — qu'il s'agisse de gain financier, d'exfiltration ou de destruction de données.

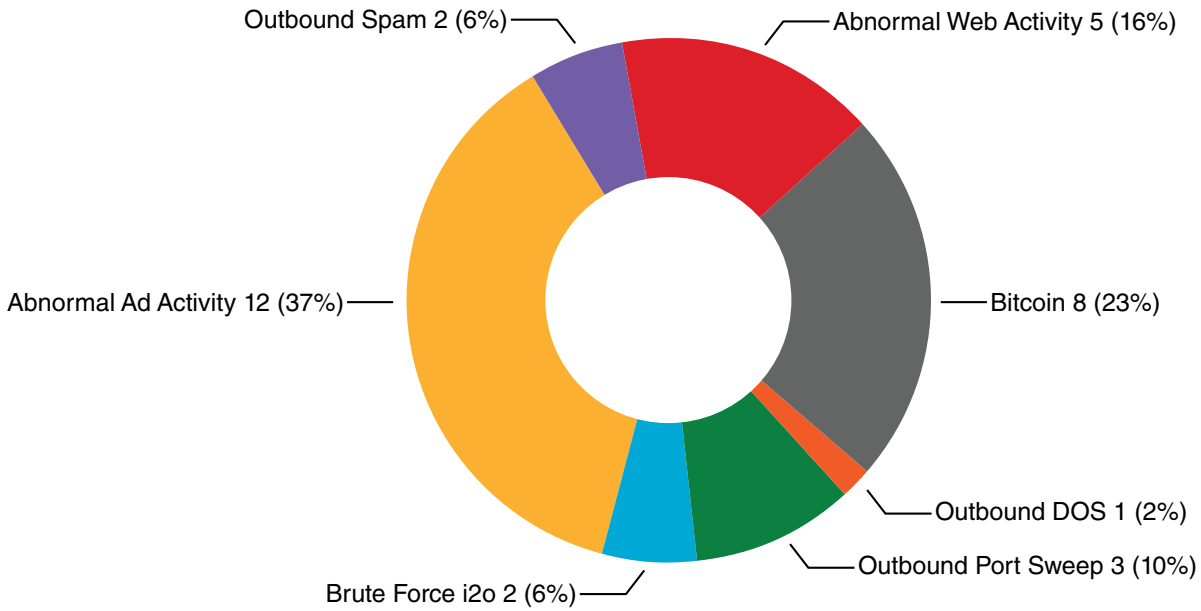
Les chiffres présentés ici représentent des comportements d'attaque en cours. L'activité liée aux communications C&C et aux opérations de reconnaissance, par exemple, intervient lors des premières phases d'une attaque. La détection permet donc aux entreprises de neutraliser rapidement la menace avant qu'elle ne puisse se propager. Il s'agit des comportements le plus souvent détectés.

Des comportements tels que le déplacement latéral surviennent plus tard dans le cycle d'attaque, au moment où les cybercriminels renforcent leur présence dans l'entreprise en dérobant des identifiants d'administrateur pour accéder aux serveurs. Ces types de détection exigent des équipes d'intervention qu'elles prennent des mesures le plus rapidement possible, pour prévenir tout dommage irréversible pouvant résulter d'une exfiltration de données.



Botnets

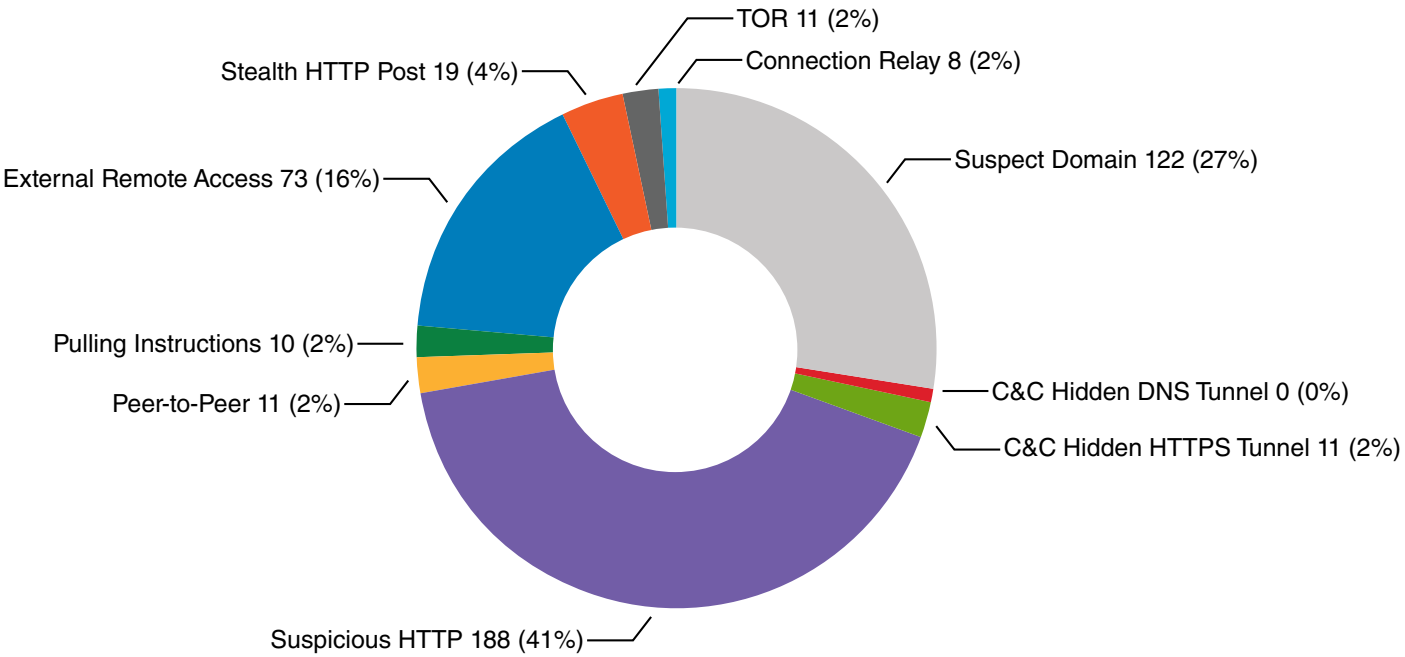
Les botnets présentent des comportements d'attaque opportunistes, qui consistent à enrôler un système afin qu'il rapporte de l'argent au pirate qui gère le réseau de robots. Un système infecté peut produire de la valeur de plusieurs façons, notamment par le minage de bitcoins, l'envoi de spam ou la production de faux clics engendrant des revenus publicitaires. Pour réaliser des profits, le gestionnaire du botnet se sert des systèmes, de leur connexion réseau et, surtout, de la bonne réputation des adresses IP qui leur sont affectées.



Trafic Command & Control (C&C)

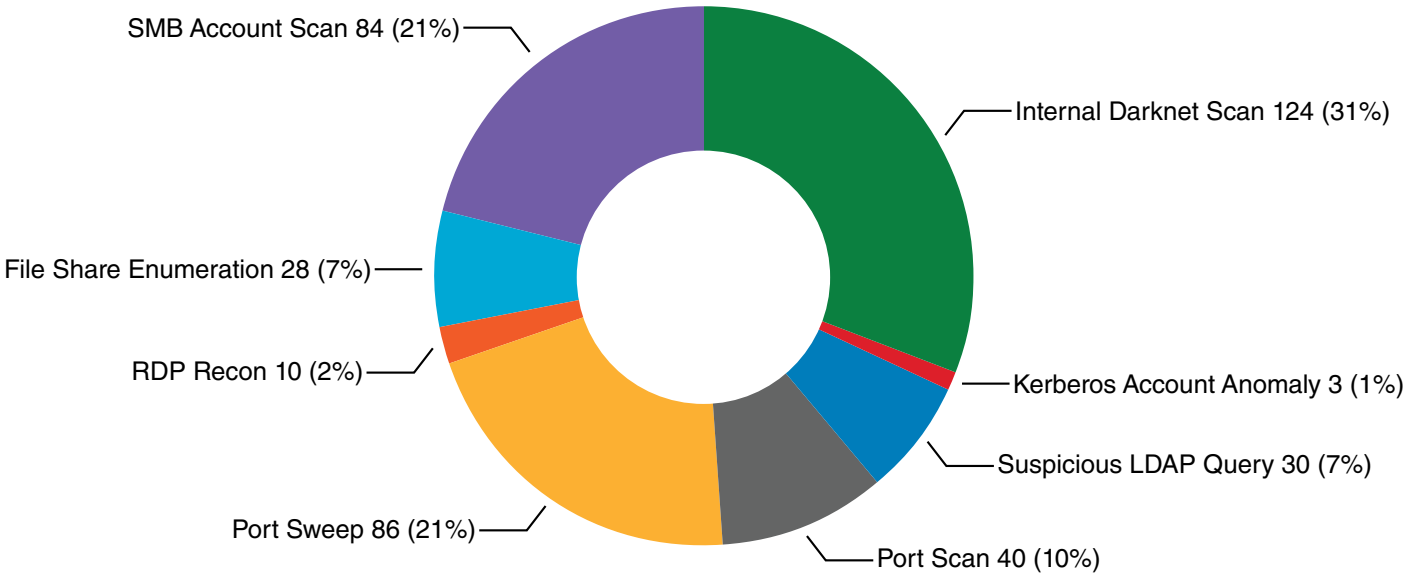
Le trafic C&C a lieu lorsqu'un système est sous le contrôle d'une entité malveillante externe. Dans la plupart des cas, ce contrôle est exercé de façon automatisée, car le système fait partie d'un botnet ou a été infecté par un adware ou un spyware.

Dans des cas plus rares, mais bien plus préoccupants, il arrive que le système soit contrôlé manuellement par un pirate externe. Ce scénario particulièrement dangereux implique souvent une attaque ciblée, visant une organisation précise.



Reconnaissance

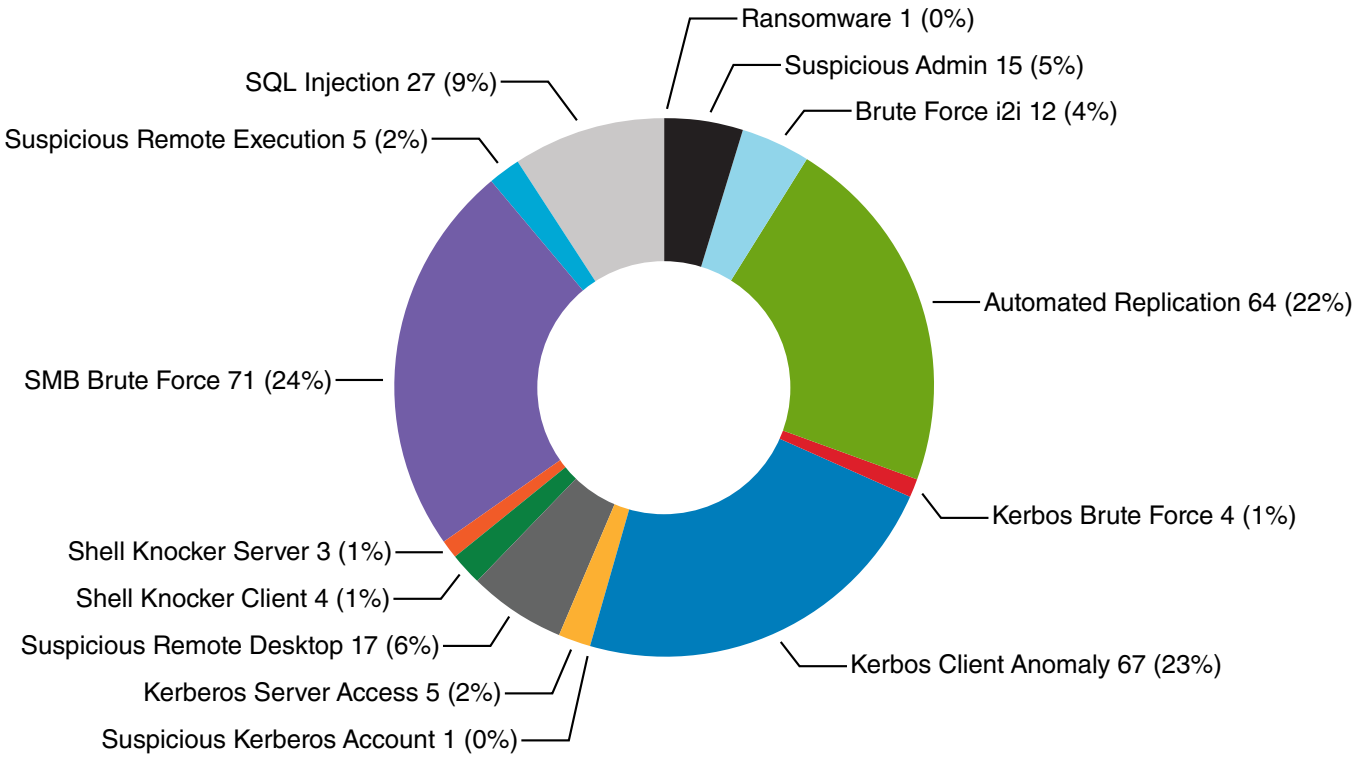
La reconnaissance est un comportement d'attaque consistant à utiliser un système pour cartographier l'infrastructure d'entreprise. Cette activité fait souvent partie d'une attaque ciblée, mais elle peut aussi indiquer que des botnets tentent de se propager en interne vers d'autres systèmes. Parmi les types de détection pertinents, citons les analyses rapides et lentes des systèmes, des ports réseau et des comptes d'utilisateur.



Déplacement latéral

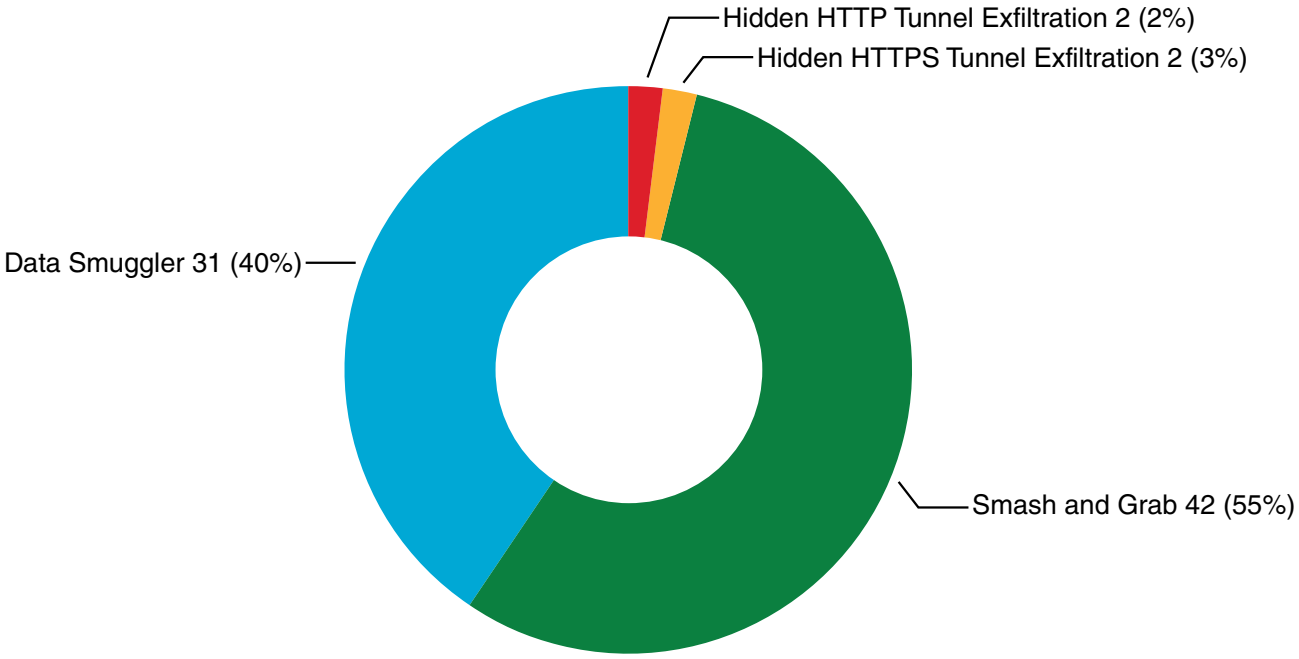
Le déplacement latéral désigne divers comportements visant à étendre la portée d'une attaque ciblée. Il peut s'agir de tentatives de vol d'identifiants ou d'extraction de données situées sur d'autres systèmes.

De même, le déplacement latéral peut se traduire par la compromission d'un autre système pour renforcer sa présence dans l'entreprise ou se rapprocher des données convoitées. Cette phase du cycle d'attaque est le prélude à l'infiltration dans les centres de données privés et les clouds publics.



Exfiltration de données

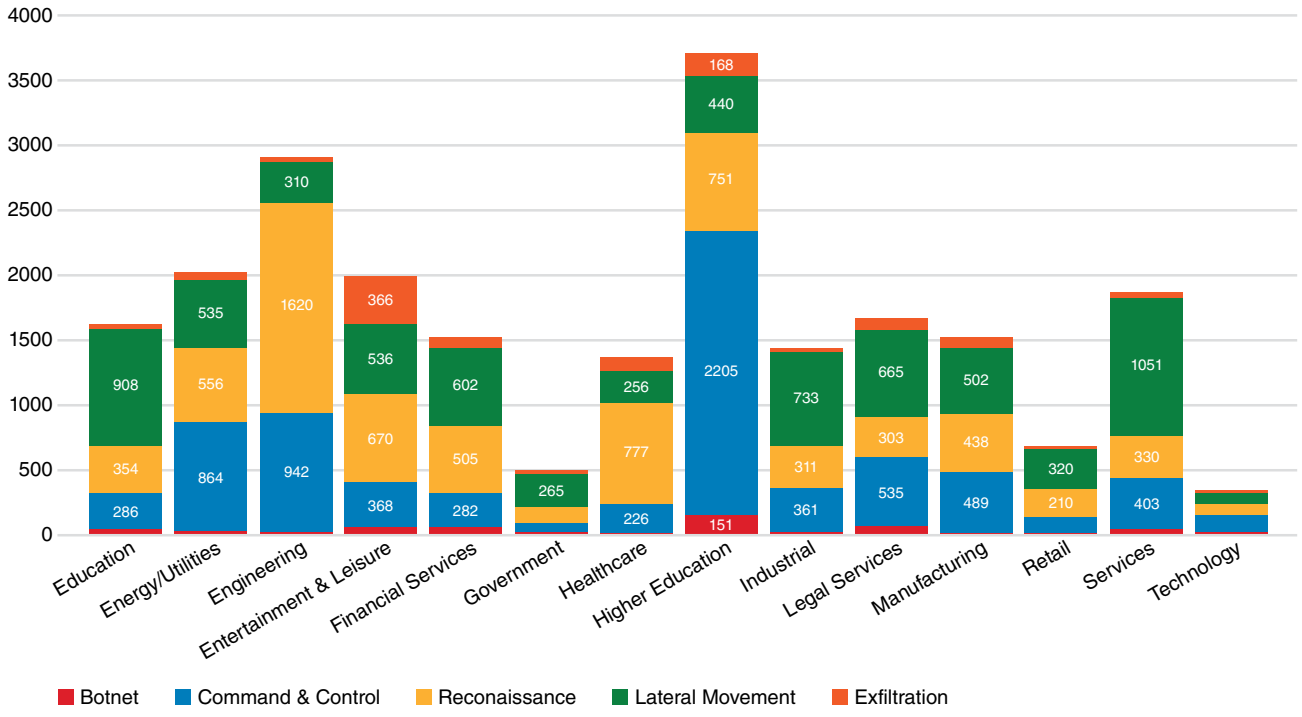
Les comportements d'exfiltration de données se manifestent par l'envoi de données vers l'extérieur, associé à une volonté de dissimulation du transfert. Généralement, un transfert de données légitime n'implique pas de technique visant à dissimuler l'opération. Le système qui transmet les données, la destination de ces dernières, le volume de données et les techniques utilisées pour les transférer sont des indicateurs signalant une exfiltration.



Menaces pour 10 000 systèmes, par secteur

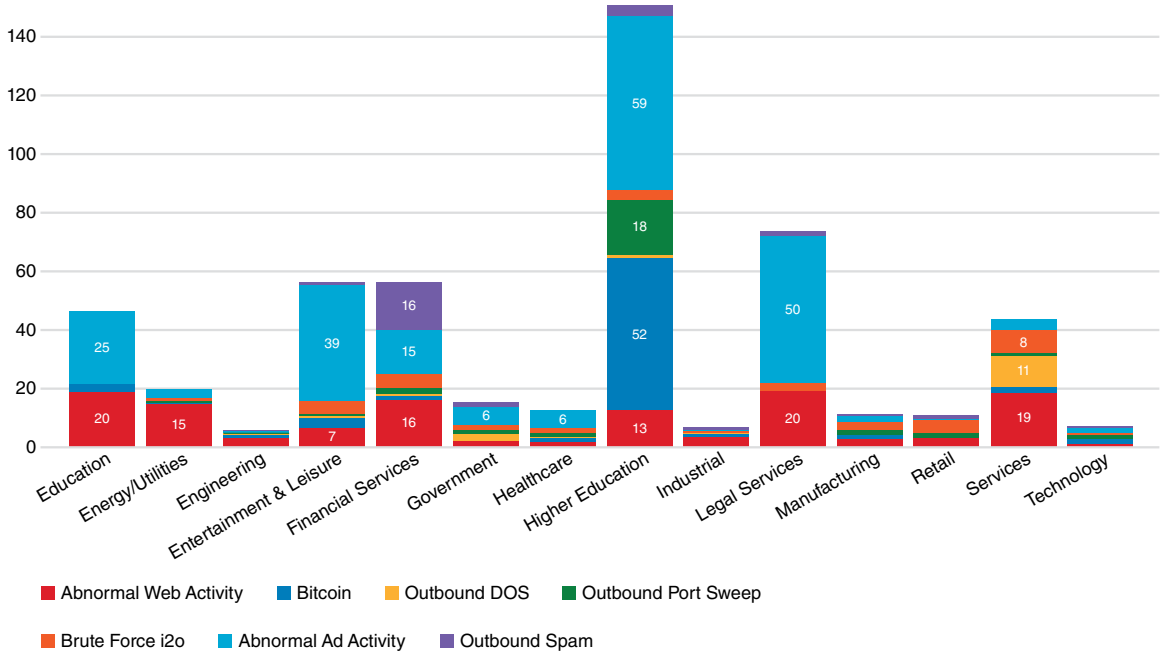
Le graphique ci-dessous affiche les volumes de détections de menaces déclenchées dans chacun des secteurs d'activité. Il montre les résultats par catégorie de comportement pour chaque secteur, ainsi que les secteurs où les volumes de détections ont été les plus élevés.

De tous les secteurs, ce sont ceux de l'enseignement supérieur et de l'ingénierie qui affichent les plus hauts pourcentages de détections. Ces volumes élevés sont principalement dus aux communications C&C (enseignement supérieur) et aux opérations de reconnaissance (ingénierie).



Botnets par secteur

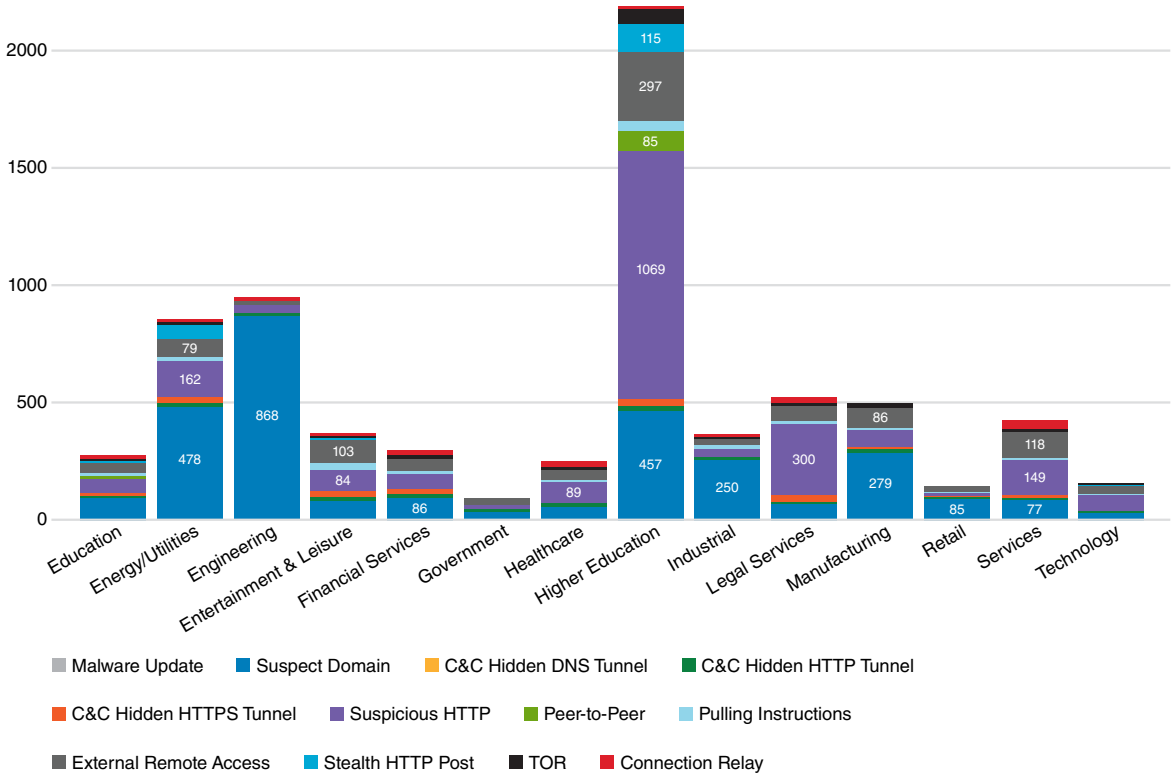
Cognito de Vectra a observé une évolution surprenante des opérations de minage de bitcoins et des activités Web anormales dans le secteur de l'enseignement supérieur. Le minage de bitcoins connaît une forte hausse de popularité auprès des cybercriminels, en particulier parmi la population estudiantine. Ces chiffres s'expliquent probablement par le manque de contrôles de sécurité, qui fait des étudiants des cibles lucratives pour les gestionnaires de botnets.



C&C par secteur

En raison de l'association entre les botnets et le trafic C&C, Cognito de Vectra a observé le plus grand volume de comportements C&C (principalement liés à un trafic HTTP suspect) dans le secteur de l'enseignement supérieur.

Les systèmes des étudiants font rarement l'objet de contrôles de sécurité qui, en temps normal, détecteraient et bloqueraient ce type de comportement. Par conséquent, les attaques C&C sont beaucoup plus faciles à mener dans les environnements d'étudiants.

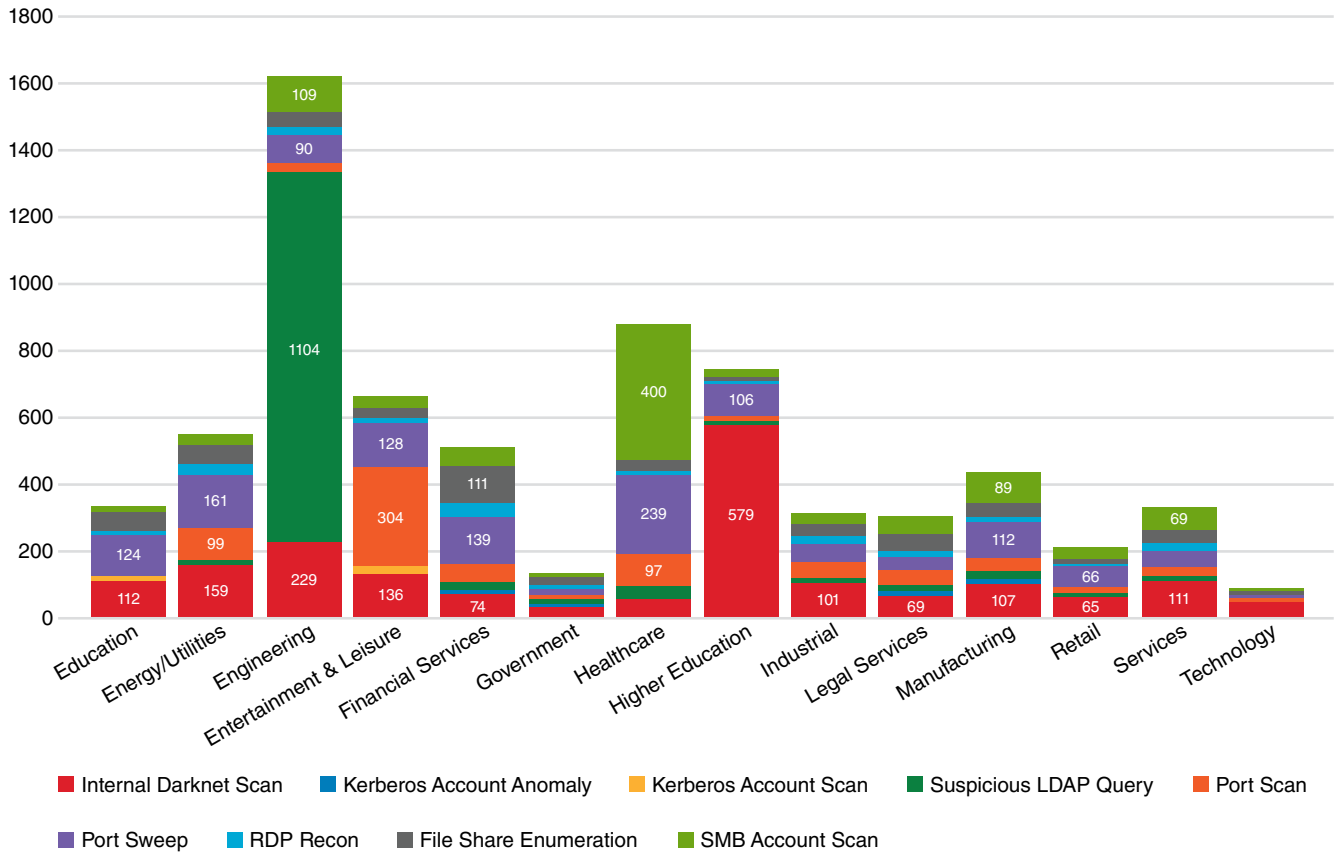


Reconnaissance par secteur

Tous secteurs confondus, Cognito de Vectra a détecté un volume important d'analyses darknet, c'est-à-dire des analyses d'adresses IP non existantes sur le réseau. Les pirates recourent assez fréquemment à ce type d'activité comme première opération de reconnaissance. Celle-ci intervient dès que les communications C&C sont établies, alors que le pirate s'introduit dans le réseau à la recherche de cibles.

Cognito a également observé des volumes considérables de requêtes LDAP suspectes dans le secteur de l'ingénierie. En effet, l'analyse des informations stockées sur un serveur Active Directory est un moyen efficace d'identifier les comptes avec privilèges, ainsi que les noms des serveurs et des composants d'infrastructure.

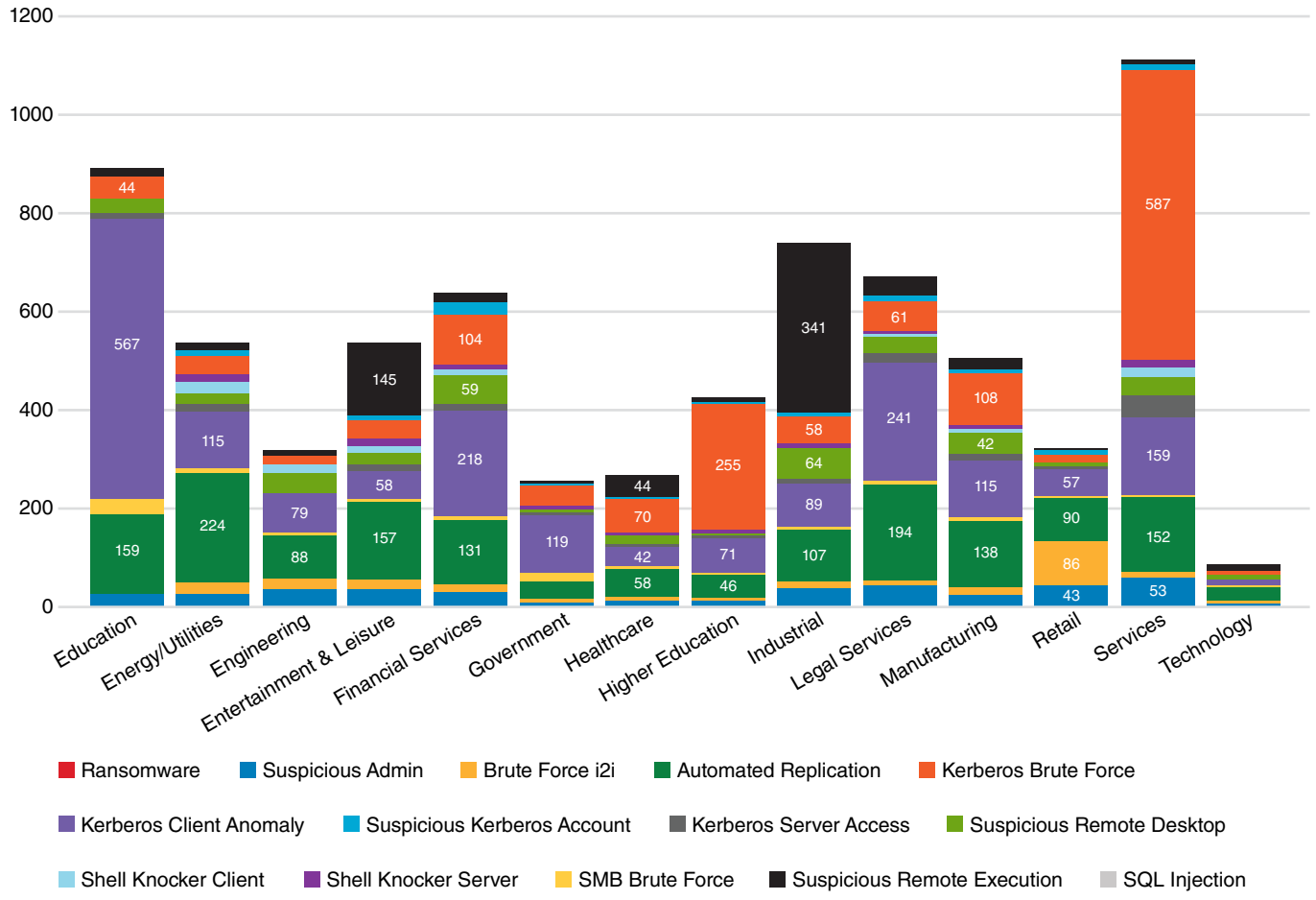
Les cyberpirates préfèrent utiliser cette forme de reconnaissance car elle est plus discrète qu'une analyse ou un balayage de ports, et le risque de détection est assez faible.



Déplacement latéral par secteur

Dans le secteur de l'enseignement, Cognito a observé une hausse importante des comportements anormaux liés aux clients Kerberos. Il s'agit d'une utilisation de compte Kerberos différente du comportement normal enregistré : connexion à des contrôleurs de domaine inhabituels ; utilisation d'équipements inhabituels ; accès à des services inhabituels ; ou génération de volumes exceptionnels de requêtes Kerberos à l'aide de contrôleurs de domaine, systèmes ou services habituels.

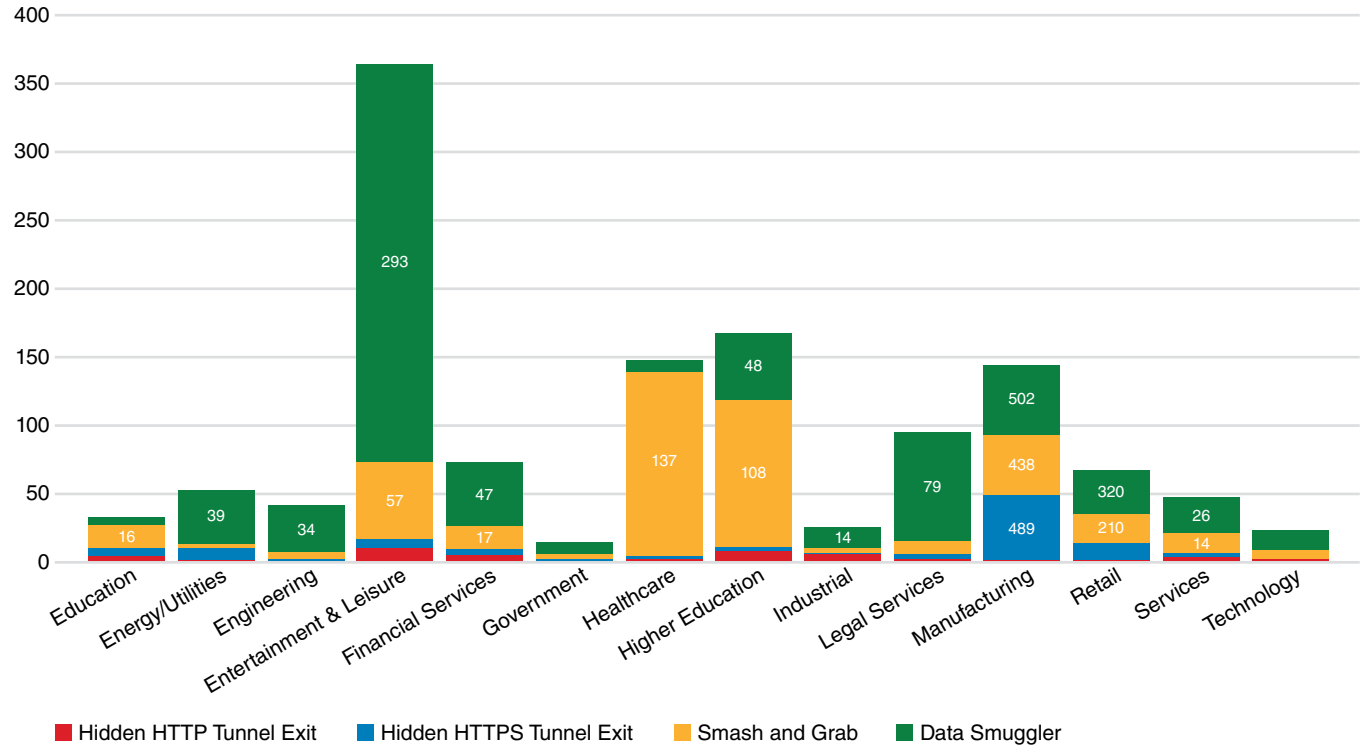
Dans le secteur des services, Cognito a détecté un volume élevé de comportements d'attaque en force du protocole SMB, ce qui signifie qu'un système tente de se connecter à de multiples reprises à l'aide des mêmes informations de compte pour accéder à un serveur de fichiers.



Exfiltration par secteur

Le vol avec destruction constitue le comportement d'exfiltration le plus répandu dans tous les secteurs. La détection intervient lorsqu'un système transmet des volumes de données inhabituellement importants vers des destinations considérées comme anormales pour l'environnement.

Le trafic illicite de données est le deuxième comportement d'exfiltration le plus fréquent, principalement observé dans le secteur des divertissements et des loisirs. Il est détecté lorsqu'un système interne acquiert un volume important de données à partir d'un ou de plusieurs serveurs et transmet de grands volumes de données vers un système externe.



Conclusion

Pour élaborer cette édition du rapport *Tendances des comportements d'attaque en entreprise*, Vectra a considérablement élargi la portée de son étude en augmentant le nombre d'entreprises participantes et leur taille moyenne. Au total, ce sont plus de 4,6 millions de systèmes qui ont été examinés — plus du double de la précédente édition.

Vectra tient à remercier ses clients qui ont accepté de partager leurs métadonnées analysées pour les besoins de ce rapport. Globalement, les tendances montrent une multiplication des détections et des comportements d'attaque, ce qui suscite des préoccupations.

Dans la mesure où les auteurs d'attaques sophistiquées automatisent et optimisent leurs propres technologies, il devient urgent d'automatiser les outils de sécurisation des informations, de détection et de résolution des incidents afin de neutraliser les menaces plus rapidement.

Parallèlement, il existe à l'échelle mondiale une pénurie de spécialistes en cybersécurité hautement qualifiés, capables d'assurer la détection et la résolution avec la rapidité nécessaire. L'utilisation de l'intelligence artificielle est donc essentielle pour renforcer les équipes de cybersécurité en place afin qu'elles puissent détecter les menaces et les neutraliser plus rapidement, tout en gardant une longueur d'avance sur les cyberpirates.

Je suis l'intelligence artificielle.
Je suis le moteur de la lutte contre les cyberpirates.
Je suis Cognito.

VECTRA®
Security that thinks®

E-mail : Info_France@vectranetworks.com / info_DACH@vectranetworks.com **Téléphone :** +41 43 810 47 52 / +33 (0)6 29 12 41 19
www.vectra.ai