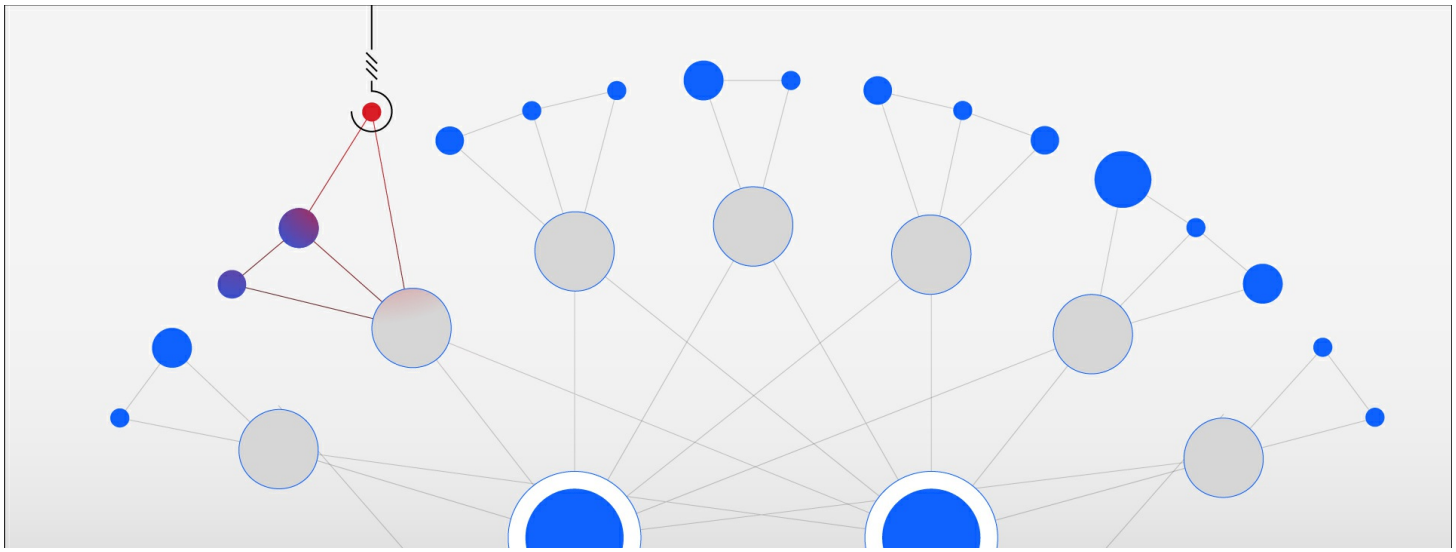
Communiqués de presse

Rapport IBM : Les ransomwares persistent malgré l'amélioration de la détection en 2022

L'industrie manufacturière est le secteur qui subit le plus d'extorsions ; les tentatives de détournement d'emails augmentent ; la réussite d'une attaque par ransomware passe de plusieurs mois à quelques jours



IBM annonce aujourd'hui les résultats de l'édition 2023 de son rapport annuel

X-Force Threat Intelligence Index sur le paysage mondial des menaces.

Voici l'extrait des données clés pour la France et l'Europe (le communiqué de presse ci-dessous présente les chiffres au niveau mondial) :

Données France

Les situations principales sur lesquelles les équipes X-Force ont été déployées au sein d'organisations françaises se répartissent entre la lutte contre des outils d'acquisition d'identifiants, les accès serveurs, les ransomwares, les portes dérobées (backdoors), et les outils de reconnaissance & analyse.

Les acteurs de la menace ont exploité des applications publiques et ont compromis des comptes de domaine et des comptes locaux valides pour obtenir un accès initial aux réseaux des victimes dans une proportion égale. Les impacts observés comprenaient la collecte d'identifiants et l'extorsion.

X-Force a répondu à des situations dans les secteurs du transport, de la finance et de l'assurance, de la santé et des services aux professionnels, aux entreprises et aux consommateurs.

Données Europe

- L'Europe a été la 2ème région du monde la plus attaquée en 2022
- 28 % des attaques en 2022 ont eu lieu dans la région européenne, contre 24 % en 2021
- Les pays attaqués ont été la France, le Royaume-Uni, le Portugal, l'Italie et l'Allemagne

- L'Europe a connu une hausse significative du déploiement des portes dérobées (backdoors) à partir de mars 2022, juste après l'invasion de l'Ukraine par la Russie. Les déploiements de backdoors ont représenté 21 % des cas dans la région et les ransomwares 11 %. Les outils d'accès à distance ont été identifiés dans 10 % des incidents auxquels X-Force a répondu. En ce qui concerne l'impact sur les clients, 38 % des cas observés par X-Force en Europe étaient liés à l'extorsion, 17 % au vol de données et 14 % à la récolte d'identifiants.

- L'exploitation d'applications publiques a été le principal vecteur d'infection utilisé contre les organisations européennes. Ce vecteur a représenté 32 % de tous les incidents auxquels X-Force a remédié dans la région, dont plusieurs ont conduit à des infections par ransomware. L'utilisation abusive de comptes locaux valides arrive en deuxième position (18 %), suivie par les liens de spear phishing (14 %), en baisse de façon significative par rapport aux 42 % enregistrés en 2021. Cette diminution des liens de spear phishing peut être le résultat d'une meilleure sensibilisation des utilisateurs, du renforcement des défenses en matière de sécurité des emails, ou de défenses plus efficaces pour détecter les logiciels malveillants après leur installation.

- Les services aux professionnels, aux entreprises et aux consommateurs sont à égalité avec la finance et l'assurance en ce qui concerne le secteur le plus attaqué, chacun représentant 25 % des cas auxquels X-Force a répondu. L'industrie manufacturière arrive en deuxième position avec 12 % des cas, tandis que l'énergie et les soins de santé se partagent la troisième place avec 10 % chacun.

Rapport IBM : Les ransomwares persistent malgré l'amélioration de la détection en 2022

L'industrie manufacturière est le secteur qui subit le plus d'extorsions ; les tentatives de détournement d'emails augmentent ; la réussite d'une attaque par ransomware passe de plusieurs mois à quelques jours

ARMONK, NY, le 22 février 2023 : IBM Security a publié aujourd'hui son rapport annuel X-Force Threat Intelligence Index, qui révèle que la part des ransomwares dans les incidents a légèrement diminué (4 points de pourcentage) entre 2021 et 2022, et que les défenseurs ont mieux réussi à détecter et à prévenir les ransomwares. Malgré cela, les attaquants ont continué à innover, le rapport montrant que le temps moyen pour mener à bien une attaque par ransomware est passé de 2 mois à moins de 4 jours.

Selon le rapport 2023, le déploiement de portes dérobées (backdoors), qui permettent un accès distant aux systèmes, est apparu comme la méthode la plus utilisée par les attaquants l'année dernière. Environ 67 % de ces cas de backdoors étaient liés à des tentatives de ransomware, les défenseurs ayant pu détecter la backdoor avant le déploiement dudit ransomware. La hausse des déploiements de backdoors peut être partiellement attribuée à leur valeur marchande élevée. X-Force a observé que les acteurs de la menace vendaient l'accès à une backdoor existante pour un montant pouvant atteindre 10 000 $, alors que les données liées aux cartes de crédit volées peuvent se vendre aujourd'hui pour moins de 10 $.

« L'évolution vers la détection et la réponse a permis aux défenseurs de déjouer les tentatives de leurs adversaires plus tôt dans la chaîne d'attaque - tempérant ainsi la progression des ransomwares à court terme », a déclaré **Charles Henderson, Head of IBM Security X-Force** *. « Mais ce n'est qu'une question de temps avant que le problème des backdoors d'aujourd'hui ne devienne la crise du ransomware de demain. Les attaquants trouvent toujours de nouveaux moyens d'échapper à la détection. Une bonne défense ne suffit plus. Pour s'affranchir de l'interminable course contre les attaquants, les entreprises doivent mettre en place une stratégie de sécurité proactive, axée sur les menaces ».*

Le rapport IBM Security X-Force Threat Intelligence Index suit des tendances et des modèles d'attaque, nouveaux et existants, en s'appuyant sur des milliards de points de données issus du réseau et des terminaux, nos missions de réponses aux incidents, et bien d’autres sources.

Voici quelques-unes des principales conclusions du rapport 2023 :

- **L'extorsion : la méthode préférée des acteurs de la menace.** L'impact le plus courant des cyberattaques en 2022 était l'extorsion, qui a été principalement réalisée par le biais d’attaques par ransomware ou par compromission d’emails professionnels. L'Europe était la région la plus ciblée par cette méthode, représentant 44 % des cas d'extorsion observés, les acteurs de la menace cherchant à exploiter les tensions géopolitiques.

- **Les cybercriminels exploitent les conversations par email**. Le détournement d’emails a connu une hausse significative en 2022, les attaquants utilisant des comptes de messagerie compromis pour s’immiscer au sein de conversations existantes en se faisant passer pour l’expéditeur initial. X-Force a observé que le taux de tentatives mensuelles a augmenté de 100 % par rapport aux données de 2021.

- **Les anciennes techniques d’attaque fonctionnent toujours**. La proportion de techniques connues utilisées pour exploiter les vulnérabilités a diminué de 10 points de pourcentage entre 2018 et 2022, en raison du fait que le nombre de vulnérabilités a atteint un nouveau record en 2022. Les résultats indiquent que les anciennes techniques ont permis à d'anciennes méthodes d’infections par logiciels malveillants,

telles que WannaCry et Conficker, de continuer d’exister et de se propager.

Les attaquants visent majoritairement l’extorsion (mais de manière inégale)

Les cybercriminels ciblent souvent les industries, les entreprises et les régions les plus vulnérables avec des systèmes d'extorsion, en appliquant une forte pression psychologique pour forcer les victimes à payer. L'industrie manufacturière a été l'industrie la plus victime d'extorsion en 2022, et elle est l'industrie la plus attaquée pour la deuxième année consécutive. Les entreprises manufacturières sont une cible attrayante pour l'extorsion, étant donné leur tolérance extrêmement faible aux temps d'arrêt.

Les ransomwares sont une méthode d'extorsion bien connue, mais les acteurs de la menace explorent sans cesse de nouveaux moyens de s’enrichir au détriment de leurs victimes. L'une des dernières tactiques consiste à compromettre et dérober les données de victimes dans la chaine du business model d’une organisation. En impliquant les clients et les partenaires dans l’équation, les attaquants accentuent la pression sur ladite organisation ciblée. Les acteurs de la menace continueront à mettre la pression aux victimes en aval afin d'augmenter les coûts potentiels et l'impact psychologique d'une intrusion. Il est donc essentiel que les entreprises disposent d'un plan de réponse aux incidents personnalisé qui prenne également en compte l'impact d'une attaque sur les victimes en aval.

Le détournement de messagerie est en hausse

Le détournement de fils de discussion par email a bondi l'an dernier, les tentatives mensuelles des acteurs de la menace ayant doublé par rapport aux données de 2021. Au cours de l'année, X-Force a constaté que les attaquants ont utilisé cette tactique pour diffuser Emotet, Qakbot et IcedID, des logiciels malveillants qui entraînent souvent des infections par ransomware.

Le phishing étant la principale cause de cyberattaques l'année dernière, et le détournement de messagerie étant en forte hausse, il est clair que les attaquants exploitent la confiance accordée aux emails. Les entreprises devraient sensibiliser leurs employés sur le sujet du détournement de messagerie afin de réduire le risque qu'ils en soient victimes.

Attention aux écarts : l’exploitation de vulnérabilité latentes en « R&D »

Le ratio de techniques d’attaques connues sur les vulnérabilités a diminué au cours des dernières années, de 10 points de pourcentage depuis 2018. Les cybercriminels ayant déjà accès à plus de 78 000 attaques connues,

cela facilite l'exploitation d'anciennes vulnérabilités non corrigées. Même après 5 ans, les vulnérabilités menant aux infections WannaCry restent une menace importante ; X-Force a récemment signalé une augmentation de 800 % du trafic du ransomware WannaCry au sein des données de télémétrie MSS depuis avril 2022. L'utilisation continue d'anciennes attaques souligne la nécessité pour les organisations d'affiner et de mûrir les programmes de gestion des vulnérabilités, notamment en comprenant mieux leur surface d'attaque et en hiérarchisant les correctifs en fonction des risques.

Les autres conclusions du rapport 2023 sont les suivantes :

- **Les hameçonneurs "abandonnent" les données de carte de crédit** . Le nombre de cybercriminels ciblant les informations relatives aux cartes de crédit a chuté de 52 % en un an, ce qui indique que les attaquants donnent la priorité aux informations permettant d'identifier les personnes, telles que les noms, les emails et les adresses personnelles, qui peuvent être vendues à un prix plus élevé sur le dark web ou utilisées pour mener d'autres opérations.

- **Le secteur de l'énergie nord-américaine a été nettement ciblé** . Le secteur de l'énergie a conservé sa place de 4ème industrie la plus attaquée l'année dernière, alors que la pression économique & géopolitique mondiale sur le secteur ne fait que croître. Les organisations énergétiques nord-américaines ont été la cible de 46 % de toutes les attaques observées sur le secteur l'an dernier, soit une augmentation de 25 % par rapport à 2021.

- **L'Asie en tête de liste des cibles.** Représentant près d'un tiers de toutes les attaques auxquelles X-Force a répondu en 2022, l'Asie a connu plus de cyberattaques que toute autre région. Le secteur manufacturier a représenté près de la moitié de tous les cas observés en Asie l'année dernière.

Le rapport présente les données collectées par IBM à l'échelle mondiale en 2022 pour fournir des informations pertinentes sur le paysage mondial des menaces et informer les professionnels de la sécurité sur les menaces les plus significatives pour leurs organisations. Vous pouvez télécharger une copie du rapport 2023 IBM Security X-Force Threat Intelligence Index ici.

Sources supplémentaires

- Pour en savoir plus sur les principales conclusions du rapport, vous pouvez consulter le blog d'IBM Security Intelligence.
- Vous pouvez vous inscrire ici au webinaire sur le rapport IBM Security X-Force Threat Intelligence Index 2023, qui aura lieu le jeudi **2 mars 2023 à 17h00** .
- Vous pouvez planifier un rendez-vous avec l'équipe IBM Security X-Force

À propos d’IBM Security

IBM Security fournit aux entreprises l’une des gammes de produits et services de sécurité les plus performantes et intégrées du marché. Ce portefeuille, qui repose sur les recherches du mondialement célèbre IBM X-Force®, permet aux organisations de gérer efficacement les risques et de se défendre face aux menaces émergentes. IBM compte parmi les plus grandes organisations mondiales dédiées à la recherche, au développement et à la conception de solutions de sécurité, gère plus de 150 milliards d’évènements de sécurité par jour dans plus de 130 pays, et possède plus de 10 000 brevets dans le domaine de la sécurité. Pour de plus amples informations, rendez-vous sur https://www.ibm.com/fr-fr/about/secure-your-business, suivez IBM Security sur Twitter ou consultez le blog IBM Security Intelligence.

Contacts Presse :

IBM
Gaëlle Dussutour
Tél. : + 33 (0)6 74 98 26 92
dusga@fr.ibm.com

Weber Shandwick pour IBM

Louise Weber / Jennifer Tshidibi

Tél. : + 33 (0)6 89 59 12 54 / + 33 (0)6 13 94 26 58

ibmfrance@webershandwick.com