Communiqués de presse

Rapport IBM : Le secteur manufacturier a été le plus touché par les cyberattaques en 2021, alors que les difficultés liées à la chaîne d'approvisionnement se sont accrues

Autres résultats : L'Asie-Pacifique est désormais la région la plus attaquée ; la durée de vie moyenne des groupes de ransomware est de 17 mois ; le vishing (phishing par la voix) triple le taux de clics d'un phishing

CAMBRIDGE, Massachusetts, le 23 février 2022 : IBM (NYSE: IBM) Security a publié aujourd'hui son rapport annuel X-Force Threat Intelligence Index, qui révèle comment les ransomwares et les exploitations de vulnérabilités ont pu « emprisonner » des entreprises en 2021, alourdissant davantage les chaînes d'approvisionnement mondiales, l'industrie manufacturière apparaissant comme le secteur le plus ciblé. Alors que le phishing était la méthode la plus courante des cyberattaques l'année dernière, IBM Security X-Force a observé une augmentation de 33 % des attaques par exploitation de vulnérabilités de logiciels non patchés, un point d'entrée sur lequel les acteurs du ransomware se sont appuyés plus que tout autre pour mener leurs attaques en 2021, représentant 44 % des attaques par ransomware.

Le rapport 2022 détaille comment, en 2021, les acteurs du ransomware ont tenté de « fracturer » l'épine dorsale des chaînes d'approvisionnement mondiales en ciblant le secteur manufacturier, qui est devenu le secteur le plus attaqué en 2021 (23 %), détrônant les services financiers et d'assurance après un long règne. Employant davantage d'attaques par ransomware que tout autre secteur, les attaquants ont parié sur l'effet d'entraînement que la perturbation des organisations manufacturières provoquerait sur leurs chaînes d'approvisionnement en aval pour les pousser à payer la rançon. Un pourcentage alarmant de 47 % des attaques contre l'industrie manufacturière ont été causées par des vulnérabilités que les organisations victimes n'avaient pas encore ou ne pouvaient pas corriger, ce qui souligne la nécessité pour les organisations de donner la priorité à la gestion des vulnérabilités.

Et c'est ce que nous confirme sur le marché français notre partenaire Capgemini :

« L'année 2021 a été une année particulièrement agitée pour les entreprises et administrations françaises sur le plan de la menace cyber. D'une part la menace de ransomwares reste forte et d'autre part les risques liés aux failles non corrigées ou difficiles à l'être explosent. Avec une accélération de la transformation du secteur manufacturier et une supply chain de plus en plus complexe, la surface d'attaque s'étend fortement. La connaissance des risques et des menaces, en particulier celles spécifiques au monde industriel devient désormais un enjeu stratégique pour les directions des entreprises » explique **Nolwenn Le Ster, Directrice des activités Cybersécurité de Capgemini en France.**

Le rapport IBM Security X-Force Threat Intelligence Index 2022 présente les nouvelles tendances et les schémas d'attaque qu'IBM Security a observés et analysés à partir de ses données - en s'appuyant sur des milliards de points de données provenant de matériels réseaux et de terminaux, des missions de réponse à incidents, de la

veille sur les kits de phishing et plus encore - y compris les données fournies par Intezer.

Voici quelques-uns des principaux faits saillants du rapport de cette année :

- **Les gangs de ransomwares résistent aux tentatives de démantèlement** : les ransomwares sont restés la principale méthode d'attaque observée en 2021, les groupes de ransomwares ne montrent aucun signe de ralentissement, malgré la hausse des démantèlements. Selon le rapport 2022, la durée de vie moyenne d'un groupe de ransomware avant sa cessation d'activité ou son changement de nom est de 17 mois.

- **Les vulnérabilités sont le plus grand "vice" des entreprises** : X-Force montre que pour les entreprises d'Europe, d'Asie et de la région Moyen-Orient et Afrique, les vulnérabilités non corrigées ont été à l'origine d'environ 50 % des attaques en 2021, révélant ainsi le plus gros défi des entreprises : la correction des vulnérabilités.

- **Signes précurseurs d'une cybercrise dans le Cloud** : Les cybercriminels préparent le terrain pour cibler les environnements Cloud, le rapport 2022 révélant une augmentation de 146 % de nouveau code de ransomware Linux et une évolution vers un ciblage axé sur Docker, ce qui pourrait permettre à davantage d'acteurs de la menace d'exploiter les environnements Cloud à des fins malveillantes.

« Les cybercriminels courent généralement après l'argent. Maintenant, avec les ransomwares, ils courent après l'effet de levier", a déclaré **Charles Henderson, responsable d'IBM X-Force***. "Les entreprises devraient reconnaître que les vulnérabilités les maintiennent dans une impasse - car les acteurs du ransomware utilisent cela à leur avantage. Il s'agit d'un défi non binaire. La surface d'attaque ne fait que grandir, donc au lieu de partir du principe que toutes les vulnérabilités de leur environnement ont été corrigées, les entreprises devraient partir du principe qu'elles sont compromises et renforcer leur gestion des vulnérabilités par une stratégie de zero trust. »*

Les "neuf vies" des groupes de ransomware

En réponse à la récente accélération des démantèlements par les forces de l'ordre de groupes de pirates

utilisant notamment les ransomwares, lesdits groupes pourraient activer leurs propres plans de reprise après sinistre. L'analyse de X-Force révèle que la durée de vie moyenne d'un groupe de ransomware avant sa cessation d’activité ou son changement de nom est de 17 mois. Par exemple, REvil, qui était responsable de 37 % de toutes les attaques par ransomware en 2021, a subsisté pendant quatre ans en changeant de nom, ce qui laisse penser qu'ils pourraient refaire surface malgré leur démantèlement par une opération multi-gouvernementale à la mi-2021.

Si les démantèlements par les forces de l'ordre peuvent ralentir les attaquants, ils les accablent également de dépenses nécessaires pour financer leur changement de nom ou reconstruire leur infrastructure. À mesure que les règles du jeu changent, il est important que les entreprises modernisent leur infrastructure pour placer leurs données dans un environnement capable de les protéger, que ce soit en local ou dans des Clouds. Cela peut aider les entreprises à gérer, contrôler et protéger leurs applications, et à supprimer l'influence des acteurs de la menace en cas de compromission en rendant plus difficile l'accès aux données critiques dans les environnements Cloud hybride.

Les vulnérabilités deviennent une crise existentielle pour certains

Le rapport X-Force met en évidence le nombre record de vulnérabilités divulguées en 2021, les vulnérabilités dans les systèmes de contrôle industriels ayant augmenté de 50 % d'une année sur l'autre. Bien que plus de 146 000 vulnérabilités aient été divulguées au cours de la dernière décennie, ce n'est que ces dernières années que les organisations ont accéléré leur parcours numérique, en grande partie sous l'effet de la pandémie, ce qui suggère que le défi de la gestion des vulnérabilités n'a pas encore atteint son apogée.

Dans le même temps, l'exploitation des vulnérabilités en tant que méthode d'attaque gagne en popularité. X-Force a observé une augmentation de 33 % depuis l'année précédente, les deux vulnérabilités les plus exploitées observées en 2021 se trouvant dans des applications d'entreprise largement utilisées (Microsoft Exchange, Apache Log4J Library). Le défi des entreprises en matière de gestion des vulnérabilités pourrait continuer à s'exacerber à mesure que les infrastructures numériques se développent et que les entreprises peuvent se retrouver submergées par les exigences d'audit et de maintenance, ce qui souligne l'importance pour elles d’opérer dans l'hypothèse d'une compromission et d'appliquer une stratégie « zero trust » pour aider à protéger leur architecture.

Les attaquants ciblent les points communs entre les Clouds

En 2021, X-Force a constaté que les attaquants étaient de plus en plus nombreux à cibler les conteneurs tels que Docker, de loin le moteur d'exécution de conteneur le plus répandu selon RedHat. Les attaquants savent que les conteneurs sont un point commun entre les organisations, ils redoublent donc d'efforts pour maximiser leur retour sur investissement avec des logiciels malveillants qui peuvent traverser les plateformes et servir de point de départ vers d'autres composants de l'infrastructure de leurs victimes.

Le rapport 2022 met également en garde contre l'investissement continu des acteurs de la menace dans des logiciels malveillants Linux uniques, qui n'avaient pas été observés auparavant, les données fournies par Intezer révélant une augmentation de 146 % des ransomwares Linux dotés d'un nouveau code. Alors que les attaquants continuent de chercher des moyens d'étendre leurs opérations par le biais des environnements Cloud, les entreprises doivent se concentrer sur l'extension de la visibilité de leur infrastructure hybride. Les environnements Cloud hybride qui reposent sur l'interopérabilité et des normes ouvertes peuvent aider les organisations à détecter les angles morts et à accélérer et automatiser les réponses de sécurité.

Voici d’autres conclusions du rapport de 2022 :

- **L’Asie est la région la plus ciblée :** Subissant plus d'une attaque sur quatre observée par IBM à l'échelle mondiale en 2021, l'Asie a connu plus de cyberattaques que toute autre région l'année dernière. Les services financiers et les entreprises manufacturières ont subi ensemble près de 60 % des attaques en Asie.

- **Combinaison efficace du phishing et des appels téléphoniques** - Le phishing a été la cause la plus courante des cyberattaques en 2021. Dans les tests de pénétration de X-Force Red, le taux de clics dans ses campagnes de phishing a triplé lorsqu'il était combiné à des appels téléphoniques.

Le rapport présente les données collectées par IBM à l'échelle mondiale en 2021 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 2022 IBM Security X-Force Threat Intelligence Index ici.

Sources supplémentaires

- Vous pouvez vous inscrire ici au webinaire sur le rapport IBM Security X-Force Threat Intelligence Index 2022, qui aura lieu le jeudi **3 mars 2022 à 17h00**.
- Vous pouvez lire un billet de blog des auteurs du rapport pour en savoir plus sur trois des principales conclusions du rapport, sur le blog d'IBM Security Intelligence.

À propos d'IBM Security

IBM Security offre 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/security, suivez IBMSecurity 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

Jennifer Tshidibi / Eric Chauvelot

Tél. : + 33 (0)6 13 94 26 58 / + 33 (0)6 21 64 28 68

ibmfrance@webershandwick.com