Principaux points à retenir du rapport Attack Intelligence Report 2024 (rapport de renseignements sur les attaques)

Le monde de la cybersécurité a changé. Depuis fin 2020, Rapid7 a enregistré une forte hausse des cas d'attaques de type zero-day, d'attaques par ransomware et d'incidents de compromission de masse affectant de nombreuses organisations à travers le monde. Le comportement des adversaires a évolué, les attaquants et les groupes de ransomware parrainés par des États tirant parti de chaînes d'exploitation zero-day complexes et de nouveaux mécanismes de persistance. Alors que la surface d'attaque continue de croître dans les environnements cloud et sur site à l'échelle mondiale, les entreprises sont plus que jamais pressées de faire de la sécurité un élément central de leurs stratégies.

Ci-dessous les principales conclusions du rapport Attack Intelligence Report 2024 (Rapport de renseignements sur les attaques) publié par Rapid7.

Zero-day et exploitation des appareils en périphérie du réseau

Pour la deuxième fois en trois ans, plus d'incidents de compromission de masse sont survenus à partir de vulnérabilités zero-day que de vulnérabilités à n-day. Cela signifie que de nombreuses attaques se produisent avant même que les organisations n'aient conscience de leur vulnérabilité. Nous avons également constaté un changement dans l'exécution de ces événements de compromission de masse. Au lieu de suivre le schéma habituel « beaucoup d'attaquants, beaucoup de cibles », près d'un quart (23 %) des failles et expositions (CVE) aux menaces de grande ampleur résultent d'attaques zero-day bien planifiées et orchestrées de main de maître, au cours desquelles un seul adversaire a compromis des dizaines ou des centaines d'organisations, souvent en utilisant des exploits propriétaires ou des portes dérobées.

Le nombre de compromissions à grande échelle résultant de l'exploitation d'appareils en périphérie du réseau a presque doublé en 2023. 36 % des vulnérabilités largement exploitées suivies par Rapid7 concernaient des technologies en périphérie du réseau. 60 % d'entre elles étaient des attaques de type zero-day. Les technologies de pointe sont essentielles au fonctionnement de nombreux réseaux modernes, mais elles constituent également un point faible important de nos défenses collectives en matière de cybersécurité, comme l'ont démontré des années d'exploitation.

Les ransomwares, un problème majeur

Les paiements de ransomware auraient dépassé le milliard de dollars dans le monde en 2023, et on ne parle là que les paiements connus. Les groupes de ransomwares réalisent des dizaines de millions de bénéfices en frappant les organisations avec des ransomwares à double extorsion.

Notre analyse a également montré une augmentation des attaques « smash-and-grab » ciblant les solutions de transfert de fichiers. Lors de ces attaques, les adversaires cherchent à accéder rapidement aux données sensibles et à les exfiltrer le plus vite possible. Alors que la plupart des incidents par ransomware observés par Rapid7 étaient toujours des attaques « traditionnelles » impliquant le chiffrement des données, les extorsions par "smash-and-grab" sont de plus en plus courantes.

Rapid7 Labs a suivi plus de

5 600

incidents par ransomware

signalés entre janvier 2023 et février 2024. Ce chiffre est probablement en deçà de la réalité, car de nombreuses attaques de ransomware ne sont toujours pas signalées.

De nombreuses organisations ne disposent pas de la MFA (authentification multifacteur)

Grâce à la bonne mise en oeuvre de MFA, les attaques contre les VPN et les infrastructures de postes de travail virtuels, qui sont une cible privilégiée, auraient pu être évitées ou ralenties. L'exploitation des vulnérabilités était également un vecteur d'accès initial courant dans les incidents auxquels la solution MDR de Rapid7 a répondu en 2023 et au début de 2024.

Comment les organisations peuvent-elles se protéger ?

La mise en œuvre et l'application de l'authentification multifactorielle doivent être une priorité absolue pour les équipes de sécurité. Avec plus de 40 % des incidents résultant de l'absence de la MFA, c'est la solution que nous recommandons. Dans le contexte actuel des menaces, il est également essentiel d'être proactif et agressif dans la réduction de la surface d'attaque exposée à Internet.

Compte tenu des attaques fréquentes contre les technologies de transfert de fichiers, nous recommandons également aux organisations de mettre en place des mesures permettant d'identifier et de prévenir plus rapidement l'exfiltration de données. Il s'agit notamment de surveiller ou de bloquer les sites connus de partage de fichiers ou les utilitaires de transfert de données, d'alerter sur (ou de restreindre) les téléchargements de fichiers volumineux et les accès inhabituels au cloud, et de mettre en œuvre un filtrage des sorties.

Enfin, comme toujours, un programme robuste de gestion des vulnérabilités est un élément essentiel de toute stratégie de sécurité, tant dans le cloud que sur site. L'importance de solides bases de gestion des vulnérabilités et des correctifs n'a pas diminué avec l'évolution des techniques et des modes opératoires des attaquants. Au contraire, ces pratiques fondamentales font partie des éléments proactifs essentiels que les entreprises doivent mettre en œuvre pour minimiser leur exposition aux menaces modernes.

Ressources supplémentaires

Lorsqu'une nouvelle menace survient, des conseils de Rapid7 sont disponibles dans la section sur les menaces émergentes (Emergent threats) du blog Rapid7, avec les informations correspondantes pour les clients de Rapid7. Les chercheurs et les membres de la communauté de Rapid7 publient une analyse des vulnérabilités sur la plateforme de recherche open source de Rapid7, AttackerKB. Ces analyses comprennent souvent des exemples de code de preuve de concept et des indicateurs de compromission, en plus des chronologies d'exploitation et de l'analyse de la chaîne d'attaque. La recherche sur les vulnérabilités zero-day de Rapid7 est régulièrement publiée ici.

Plus de
40 %

des incidents que les équipes de détection et de réponse gérées par Rapid7 ont constatés en 2023 provenaient d'une authentification multifactorielle (MFA) manquante ou inopérante.

RAPID7

PRODUITS

Sécurité Cloud
XDR et SIEM
Threat intelligence
Gestion des risques liés aux vulnérabilités
Sécurité des applications
Orchestration et automatisation
Services managés

CONTACTEZ-NOUS

rapid7.com/contact

Pour en savoir plus ou commencer un essai gratuit, rendez-vous sur www.rapid7.com/try/insight