kaspersky 25 YEARS DREAM DIGITALLY. PROTECT FOR REAL.

Les 15 principales vulnérabilités, TTP, ransomwares et comment les contrer

Le paysage des menaces en constante évolution

Chaque année, les tactiques, techniques et procédures (TTP) utilisées par les cybercriminels ne cessent d'évoluer, la part des attaques ciblées d'origine humaine (y compris les ransomwares gérés par les humains) ne cesse d'augmenter, et l'éventail des vulnérabilités exploitées par les pirates ne cesse de s'élargir. Pour pouvoir y faire face, vous devez avoir une connaissance de base des vulnérabilités exploitées, des outils utilisés et des points à surveiller.

Les 15 principales vulnérabilités

En 2021, plus de 18 500 vulnérabilités et expositions courantes (CVE) ont été signalées par les experts en sécurité[1], contre un peu plus de 17 000 en 2020. Parmi celles-ci, plus de 65 étaient des attaques de type « zero-day », soit le double du nombre identifié en 2020.

En avril 2022, un avis conjoint de cybersécurité émis par des agences gouvernementales des États-Unis, de l'Australie, du Canada et du Royaume-Uni a détaillé les 15 CVE les plus couramment exploitées par des acteurs de menaces malveillants en 2021. Cela inclut :

CVE-2021-34523, CVE-2021-34473, CVE-2021-31207

(ProxyShell) exploitation de Microsoft Exchange Server pour l'élévation de privilèges, l'exécution de code à distance et le contournement des fonctionnalités de sécurité respectivement

CVE-2021-27065, CVE-2021-26858, CVE-2021-26857, CVE-2021-26855

exploitation du client VMware vSphere pour l'exécution de code à distance

CVE-2021-44228

(Log4Shell) exploitation de Apache Log4j pour l'exécution de code à distance

CVE-2021-40539

exploitation de Zoho ManageEngine AD SelfService Plus pour l'exécution de code à distance

CVE-2021-26084

exploitation d'Atlassian Confluence Server et Data Center pour l'exécution de code arbitraire

CVE-2021-21972

exploitation du client VMware vSphere pour l'exécution de code à distance

CVE-2020-1472

(ZeroLogon) exploitation de Microsoft Netlogon Remote Protocol (MS-NRPC) pour l'élévation de privilèges

CVE-2020-0688

exploitation de Microsoft Exchange Server pour l'exécution de code à distance

CVE-2019-11510

exploitation de Pulse Secure Pulse Connect Secure pour la lecture de fichiers arbitraires

CVE-2018-13379

exploitation de Fortinet FortiOS et FortiProxy pour la traversée de chemins d'accès

Les principales tactiques, techniques et procédures (TTP)

Selon les gourous des TTP, MITRE ATT&CK® :

Les tactiques illustrent le « pourquoi » d'une technique ou d'une sous-technique d'ATT&CK. Il s'agit de l'objectif tactique de l'adversaire : la raison pour laquelle il effectue une action, par exemple, l'accès à des identifiants.

Les techniques représentent la façon dont un adversaire atteint un objectif tactique en réalisant une action, par exemple en extrayant des identifiants pour y obtenir un accès.

Les procédures sont la mise en œuvre que l'adversaire utilise pour appliquer des techniques ou des sous-techniques, par exemple, l'utilisation de PowerShell pour injecter du code dans le processus lsass.exe afin d'extraire les identifiants en grattant la mémoire du processus LSASS auprès d'une victime.

Techniques les plus utilisées :

Phishing (TA0001 : Accès initial)

T1566

Exploitation de services à distance (TA0008 : Mouvement latéral)

T1210

Exécution par l'utilisateur (TA0002 : Exécution)

T1204

Préparez-vous à détecter les menaces de tous types de tactiques (phases de la chaîne de frappe de l'attaque). Toutes les attaques, même les plus complexes, reposent sur un enchaînement d'étapes simples (ou techniques). La détection d'une technique particulière peut révéler une attaque dans son ensemble[2].

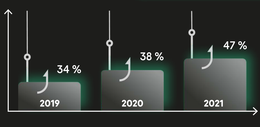
Outils les plus utilisés :

Les adversaires utilisent des outils non malveillants intégrés au système d'exploitation pour minimiser leurs chances d'être détectés pendant la transmission de leurs outils[2].

Les fichiers binaires LOLBins (Living off the Land Binaires) les plus populaires observés dans presque tous les incidents sont cmd.exe et powershell.exe. rundll32.exe est également populaire parmi les incidents de tous les niveaux de gravité.

Les incidents de niveau de gravité élevé se distinguent par une grande variété de fichiers binaires LOLBins utilisés. Outre cmd.exe, powershell.exe et rundll32.exe, dans les incidents de niveau de gravité élevé, certutil.exe, reg.exe et te.exe sont également très prisés.

Ransomwares – l'éléphant dans la pièce



Après une série d'attaques très médiatisées en 2021, les ransomwares constituent une menace sérieuse contre laquelle chaque organisation doit être prête à se défendre. Entre janvier et novembre 2021, 47 % des réponses aux incidents traitées par l'équipe Global Emergency Response Team (GERT) de Kaspersky étaient liées aux ransomwares, contre 38 % en 2020 et 34 % en 2019. Pour se protéger contre les ransomwares :

- N'exposez pas les services de bureau à distance (comme le service RDP) aux réseaux publics, sauf en cas de nécessité absolue, et utilisez toujours des mots de passe forts pour ces services.
- Installez rapidement les correctifs disponibles pour les solutions commerciales de VPN fournissant un accès pour les employés distants et agissant comme des passerelles dans votre réseau.
- Maintenez toujours les logiciels à jour sur tous les appareils que vous utilisez pour empêcher les ransomwares d'exploiter des vulnérabilités.
- Utilisez une solution de sécurité des terminaux fiable intégrant la prévention des exploits, la détection comportementale, un moteur de remédiation capable d'annuler les actions malveillantes et des mécanismes d'autodéfense robustes pour empêcher sa suppression par les cybercriminels.
- Concentrez votre stratégie de défense sur la détection des mouvements latéraux et l'exfiltration des données vers Internet. Portez une attention particulière au trafic sortant pour détecter les connexions des cybercriminels.
- Faites des sauvegardes régulières. Assurez-vous de pouvoir y accéder rapidement en cas d'urgence, si nécessaire. Utilisez les dernières informations en matière de Threat Intelligence pour rester au courant des TTP utilisées par les acteurs des menaces.
- Utilisez des solutions comme la détection et la réponse au niveau des terminaux (EDR) ainsi que la détection et la réponse managées (MDR) pour identifier et arrêter les attaques à leurs débuts, avant que les pirates informatiques atteignent leurs objectifs finaux.
- Pour protéger l'environnement de l'entreprise, formez vos employés à la cybersécurité.

Comment Kaspersky peut vous aider

Kaspersky Optimum Security

Kaspersky Optimum Security est une solution native du cloud qui complète vos compétences en cybersécurité en limitant les ressources nécessaires, grâce à des fonctionnalités EDR efficaces, associées à une recherche des menaces gérée ainsi qu'à des scénarios de réponse guidée et à distance, sans frais exorbitants ni complexité. Elle vous protège comme il faut contre les menaces nouvelles, inconnues et évasives, sans avoir besoin d'engager ou de former à nouveau des spécialistes de sécurité informatique ni d'y allouer des ressources supplémentaires.

Contactez-nous

[1] cybersecurityintelligence.com
[2] Rapport d'analyse de Kaspersky Managed Detection and Response 2021