Trellix | ABC Co.

RAPPORT ADVANCED THREAT RESEARCH

JANV. 2022

Le présent rapport Advanced Threat Research vous est proposé par notre partenaire.

RAPPORT

Trellix

RAPPORT ADVANCED THREAT RESEARCH

JANV. 2022

RAPPORT

RAPPORT

SOMMAIRE

Le premier rapport sur les menaces de notre nouvelle société fait la lumière sur la vulnérabilité Log4j, qui a non seulement fait la une de l'actualité mais est aussi au cœur des préoccupations de toutes les équipes de sécurité.

Rédaction et recherches

Alfred Alvarado
Christiaan Beek
John Fokker
Douglas McKee
Tim Polzer
Steve Povolny
Raj Samani
Leandro Velasco

LETTRE DE NOTRE ANALYSTE EN CHEF

Bienvenue dans notre nouveau rapport sur le paysage des menaces ainsi qu'au sein de notre nouvelle société.

À l'aube de cette nouvelle année, il nous faut revenir sur un paysage des menaces particulièrement éprouvant fin 2021. Le premier rapport sur les menaces de notre nouvelle société fait la lumière sur la vulnérabilité Log4j, qui a non seulement fait la une de l'actualité mais est aussi au cœur des préoccupations de toutes les équipes de sécurité. Il se penche également sur les troisième et quatrième trimestres 2021 mais, avant de commencer, faisons le point sur les multiples ressources mises à votre disposition pour combattre la menace Log4j.

Compte tenu de l'accumulation d'informations sur la menace Log4j, il est essentiel que nous nous plongions dans nos recherches et nos ressources actualisées pour obtenir de l'aide. Outre le statut du produit, nous surveillons constamment toute campagne active exploitant cette vulnérabilité et faisons le point sur l'état de la protection pour les nouvelles charges actives.

Lorsque les premières informations sur la vulnérabilité Log4j ont commencé à circuler, nous avons réagi rapidement en mettant à disposition des signatures réseau et une description de la vulnérabilité. Celles-ci ont été suivies d'autres ressources présentées en détail dans ce rapport.

Pour mieux comprendre les activités malveillantes actuelles liées à Log4j ainsi que d'autres menaces prévalentes, vous pouvez vous référer à notre précieux tableau de bord sur les menaces.

Par ailleurs, n'hésitez pas à consulter les blogs de Trellix Threat Labs, qui proposent des informations à jour sur les menaces, des vidéos et des liens vers le bulletin de sécurité.

Il est clair que Log4j n'est pas la seule menace posée à la sécurité de votre entreprise. Ce rapport met également en lumière la menace et les interruptions causées par les ransomwares, et d'autres menaces et attaques prévalentes observées.

Tous mes vœux pour 2022 et bienvenue dans notre nouvelle entreprise.

— Raj Samani

Analyste en chef et Chargé de recherche

Twitter : @Raj_Samani

LOG4J : LA MÉMOIRE QUI EN SAVAIT TROP

Dans ce qui semble devenir une triste tradition, Log4j, une nouvelle vulnérabilité affectant une bibliothèque Log4j largement utilisée dans le monde, a été divulguée peu avant les fêtes. Cette vulnérabilité, considérée comme la faille de cybersécurité la plus grave des dernières décennies, a exigé la mobilisation de Trellix et du secteur de la cybersécurité au cours du quatrième trimestre 2021. Log4j promettait en effet d'avoir un impact majeur sur tous les produits intégrant la bibliothèque Log4j dans leurs applications et sites web, notamment des produits et services Apple iCloud, Steam, Samsung Cloud et bien d'autres.

Log4j a fait l'objet d'un suivi constant de la part de notre équipe depuis sa découverte. Nous avons publié la signature réseau KB95088 à l'intention des clients qui utilisaient la solution Network Security Platform (NSP). Cette signature détecte les tentatives d'exploitation de la vulnérabilité CVE-2021-44228 sur LDAP et peut être étendue pour inclure d'autres protocoles ou services. D'autres signatures peuvent par ailleurs être publiées pour compléter la couverture.

Chronologie de la vulnérabilité Log4j

Voici un petit rappel chronologique de la faille Log4j et de nos recherches :

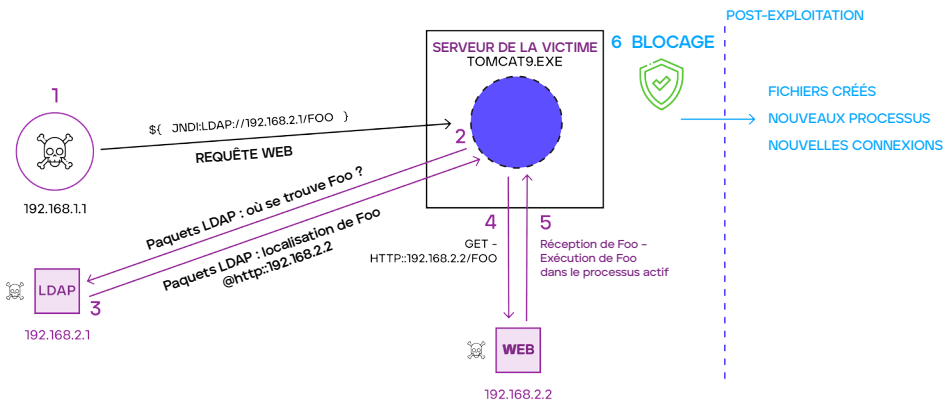
- **9 décembre** — La vulnérabilité Log4j (CVE-2021-44228) est publiée sur Twitter, en même temps qu'une preuve de concept sur GitHub pour la bibliothèque de journalisation Apache Log4j. Le bug avait été initialement porté à la connaissance d'Apache le 24 novembre.
- **10 décembre** — Steve Povolny et Douglas McKee publient un article de blog sur Log4j faisant le point sur nos découvertes. Notre objectif initial était de déterminer la facilité d'exploitation à l'aide de la preuve de concept publique, que nous avons reproduite et confirmée. Pour cela, nous avons utilisé le conteneur Docker public et une architecture client-serveur utilisant LDAP et RMI, ainsi que l'outil marshalsec pour exploiter la version 2.14.1 de Log4j.
- **14 décembre** — La vulnérabilité de la version 1.2 de Log4j à des attaques similaires lancées par l'intermédiaire du composant JMSAppender est confirmée et la vulnérabilité CVE-2021-4104 est publiée.
- **18 décembre** — Une nouvelle vulnérabilité de type déni de service (DoS), CVE-2021-45105, est découverte. Elle touche les versions 2.0-alpha1 à 2.16.0 de Log4j.

Consultez les blogs Trellix Threat Labs et nos tableaux de bord sur les menaces pour découvrir nos dernières recherches sur les mécanismes de défense possibles contre Log4j. Notre équipe recueille et analyse des informations issues de plusieurs sources ouvertes et fermées, avant de distribuer des rapports de cyberveille.

Attaque de la vulnérabilité Log4j

Notre équipe n'a pas traîné pour étudier et présenter les différentes activités intervenant dans l'exécution d'une attaque web Log4j classique :

FLUX D'EXÉCUTION DE LOG4J



- Étape 1 — Un cybercriminel envoie une chaîne spécialement conçue au serveur web hébergeant l'application vulnérable. Comme nous l'avons vu, cette chaîne peut être masquée afin de contourner les signatures réseau.
- Étape 2 — L'application entreprend d'exposer la chaîne pour la charger en mémoire. Une fois chargée en mémoire, l'application établit une connexion LDAP pour demander l'adresse de l'emplacement de la classe malveillante.
- Étape 3 — Le serveur LDAP contrôlé par le pirate envoie en réponse l'emplacement du fichier de la classe malveillante en indiquant l'adresse URL HTTP de l'endroit où elle est hébergée.
- Étape 4 — L'application vulnérable lance le téléchargement du fichier de la classe malveillante.
- Étape 5 — L'application vulnérable charge et exécute le fichier de la classe malveillante de l'étape 4.

Défenses mises en place par l'équipe ATR de Trellix contre Log4j

Pour protéger un environnement contre des attaques de type Log4j, une stratégie multiniveau associant sécurité réseau et analyses ciblées de la mémoire des terminaux permet aux équipes de sécurité de détecter et prévenir de façon efficace le flux d'exécution de l'attaque contre les systèmes vulnérables exposés via des vecteurs réseau. Certaines mesures, telles que les analyses personnalisées et les règles expert de la solution ENS, sont conçues pour permettre aux équipes d'appliquer des contre-mesures précises face à ces menaces émergentes.

Le site CISA.gov propose par ailleurs un analyseur Log4j pour aider les entreprises à identifier les services web potentiellement vulnérables affectés par les vulnérabilités Log4j.

RANSOMWARES

Au troisième trimestre 2021, plusieurs groupes de ransomwares connus ont disparu, sont réapparus, ont été restructurés ou ont changé d'image, mais cela ne les a pas empêchés de rester une menace réelle, prévalente et potentiellement destructrice ciblant un éventail toujours plus large de secteurs.

Même si les activités des ransomwares ont été dénoncées et bannies de nombreux forums cybercriminels au cours du deuxième trimestre 2021, notre équipe a observé une activité des mêmes cybercriminels sur plusieurs forums, sous d'autres profils fictifs.

Trellix participe aux arrestations des groupes de ransomwares et aux saisies des rançons

En décembre 2021, Trellix a fourni des renseignements qui ont aidé le FBI et Europol à arrêter des affiliés de REvil et ont conduit à la saisie de 2 millions de dollars de rançon.

Voici quelques tendances et campagnes de ransomwares majeures observées au 3e trimestre 2021 :

- BlackMatter — Découvert fin juillet 2021, ce ransomware a commencé par une campagne d'attaques majeure qui menaçait de révéler des données commerciales propriétaires de New Cooperative, une société de la chaîne logistique agricole basée aux États-Unis. New Cooperative a annoncé le blocage des fonctions de gestion de la chaîne logistique et des programmes d'alimentation des animaux et a estimé que 40 % de la production céréalière américaine pouvaient être affectés. Même si BlackMatter a prétendu utiliser les éléments les plus efficaces d'autres logiciels malveillants, tels que GandCrab, LockBit et DarkSide, nous doutons sérieusement que la campagne soit gérée par un nouveau groupe de développeurs. Le logiciel malveillant BlackMatter présente trop de points communs avec DarkSide, le logiciel malveillant associé à l'attaque de Colonial Pipeline.
- Nous avons la conviction que le groupe Groove est associé au groupe Babuk, soit en tant qu'ancien affilié ou que sous-groupe.
- REvil/Sodinokibi a revendiqué la responsabilité de l'infection de plus d'un million d'utilisateurs grâce à une attaque par ransomware contre le fournisseur de services managés Kaseya VSA. La demande de rançon de 70 millions de dollars constitue, selon les allégations de REvil, le montant le plus important révélé publiquement à ce jour. L'attaque a notamment forcé plusieurs centaines de supermarchés à fermer leurs portes pendant plusieurs jours.
- LockBit 2.0 a fait son apparition en juillet 2021 et a publié sur son site de divulgation de données une liste de plus de 200 victimes.

Réaction des pouvoirs publics aux ransomwares

Au troisième trimestre, le gouvernement américain a démarré une campagne proactive visant à réduire la prévalence des ransomwares, avec le lancement de StopRansomware.gov, une plate-forme offrant des primes pouvant atteindre 10 millions de dollars pour toute information susceptible d'identifier ou de localiser des cybercriminels à la solde d'États impliqués dans des cyberattaques contre des infrastructures américaines critiques.

Pour savoir comment ces ransomwares et les nouvelles campagnes pourraient menacer les entreprises dans les mois à venir, consultez le rapport Prévisions 2022 en matière de menaces de Trellix.

Recherches de Trellix sur les ransomwares

Pour aider les entreprises à mieux comprendre les attaques par ransomware et à s'en protéger dans le paysage actuel des menaces, notre équipe présente ses observations et les conclusions de ses recherches sur la prévalence d'un large éventail de ransomwares, y compris les familles, les techniques, les pays, les secteurs et les vecteurs concernés.

Détections par famille de ransomwares

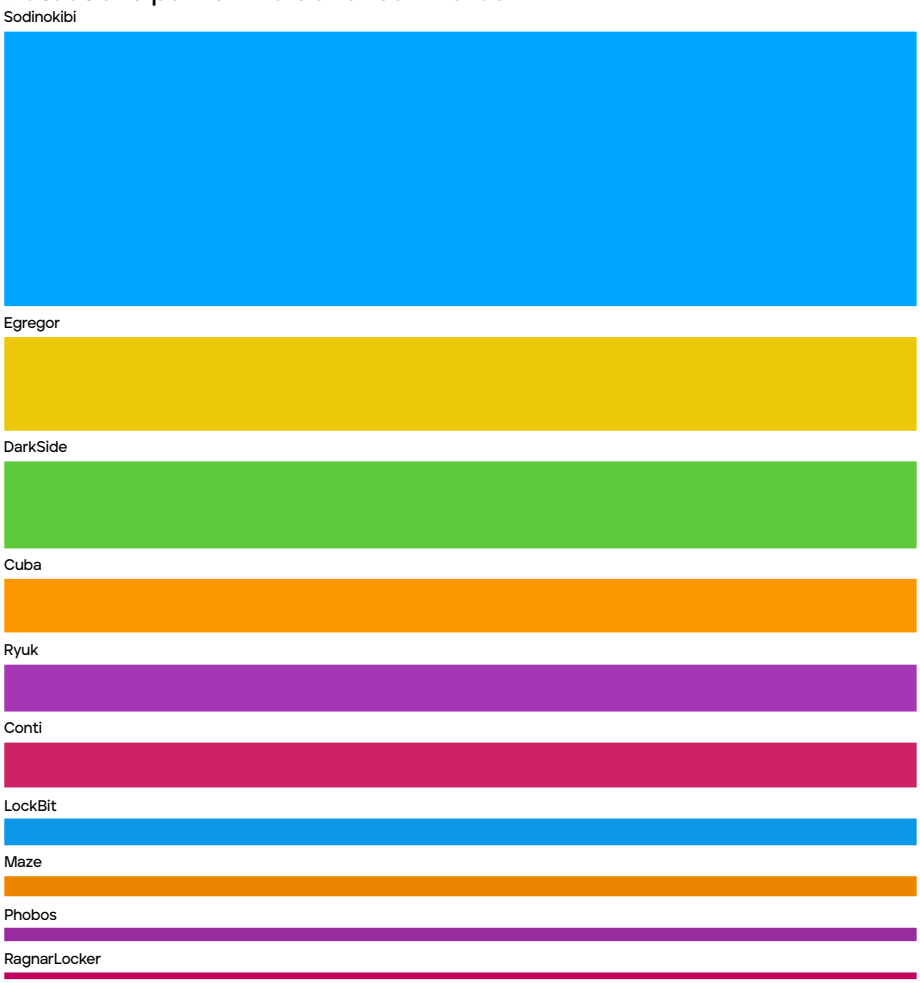


Figure 1. Sodinokibi (41 %) est la famille de ransomwares la plus prévalente détectée au 3e trimestre 2021, suivie de DarkSide (14 %) et d'Egregor (13 %).

Consultez la section Ransomwares : secteurs et pays des clients ciblés par les ransomwares, et techniques MITRE ATT&CK ci-après.

MODÈLES ET TECHNIQUES D'ATTAQUE

L'équipe assure un suivi et une surveillance des campagnes APT, ainsi que des indicateurs et techniques qui leur sont associés. Les recherches de notre équipe portent sur les cybercriminels APT, leurs outils, les pays et les secteurs des clients ciblés ainsi que les techniques MITRE ATT&CK du 3e trimestre 2021.

Groupes cybercriminels APT

Figure 2. Au 3e trimestre 2021, APT41 (24 %) et APT29 (22 %) ont été les groupes cybercriminels APT les plus prolifiques, et près de la moitié des activités APT surveillées leur ont été attribuées.

Outils APT

L'équipe a identifié des indicateurs de compromission appartenant aux campagnes APT suivies, auxquelles sont associés les outils suivants. Les groupes APT sont connus pour employer des utilitaires système courants afin de contourner les contrôles de sécurité et mener leurs activités malveillantes :

Figure 3. Cobalt Strike (34 %) a été l'outil malveillant le plus souvent détecté au 3e trimestre 2021, suivi de Mimikatz (27 %), Net.exe (26 %) et PsExec (20 %). La suite d'attaques Cobalt Strike exploitée par des pirates à la solde d'États a été identifiée dans plus d'un tiers des activités APT.

Consultez la section APT : secteurs et pays des clients ciblés par des attaques, et techniques MITRE ATT&CK ci-après.

ADVANCED THREAT RESEARCH

Notre équipe a suivi plusieurs catégories de menaces au 3e trimestre 2021. Les résultats des recherches indiquent les pourcentages de détection par type de malware ATR, les pays et secteurs des clients ciblés, ainsi que les techniques MITRE ATT&CK utilisées.

Menaces posées par les outils ATR

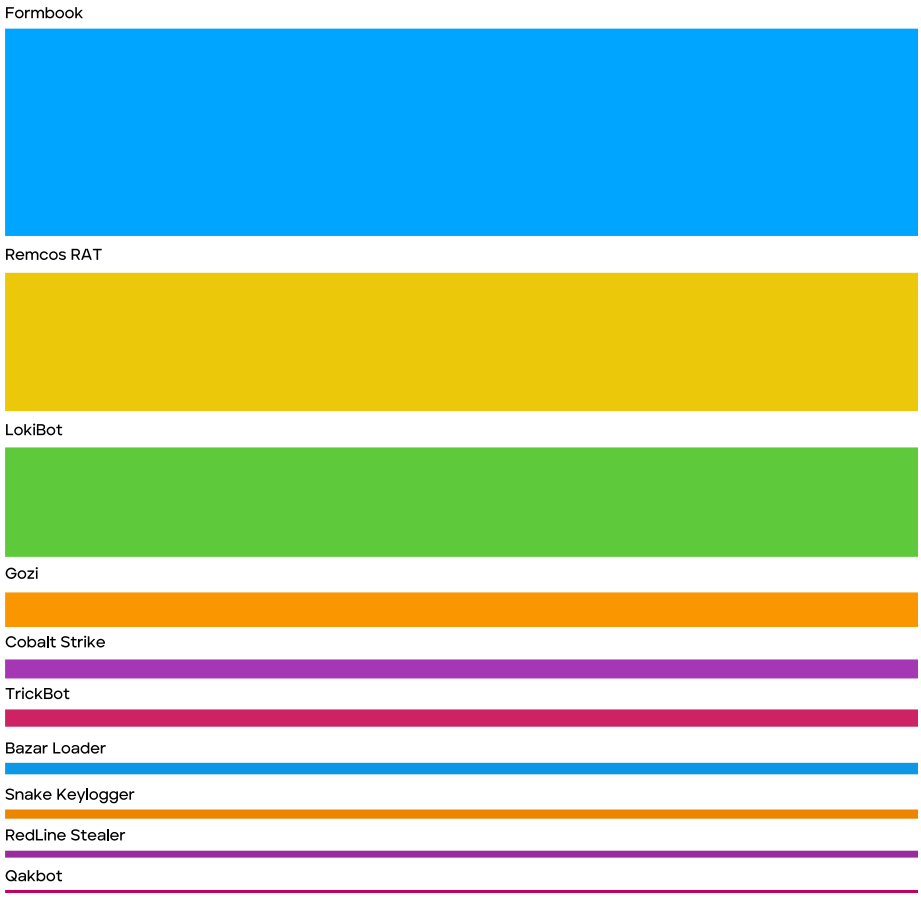


Figure 4. Formbook (36 %), Remcos RAT (24 %) et LokiBot (19 %) représentent près de 80 % des détections de menaces ATR au 3e trimestre 2021.

Consultez la section ATR : secteurs et pays des clients ciblés par des menaces, et techniques MITRE ATT&CK ci-après.

MENACES À L'ENCONTRE DES PAYS, DES CONTINENTS ET DES SECTEURS D'ACTIVITÉ ET VECTEURS D'ATTAQUE

Pays et continents : 3e trim. 2021

Des hausses notables du nombre d'incidents rendus publics par pays et par continent ont été observées au 3e trimestre 2021 :

- L'Amérique du Nord est le continent le plus touché en termes d'incidents, mais il a enregistré une baisse de 12 % entre le 2e et le 3e trimestre 2021.
- Les États-Unis ont enregistré le plus grand nombre d'incidents signalés au 3e trimestre 2021, mais ceux-ci ont diminué de 9 % par rapport au 2e trimestre 2021.
- C'est la France qui a connu l'augmentation la plus forte (400 %) du nombre d'incidents signalés au 3e trimestre 2021.
- La Russie a enregistré la baisse la plus importante (-79 %) du nombre d'incidents au 3e trimestre 2021 par rapport au 2e trimestre.

Secteurs ciblés : 3e trim. 2021

Les incidents notables rendus publics par secteur au 3e trimestre 2021 incluent notamment les suivants :

- Diverses industries (28 %) ont enregistré une augmentation de la fréquence des attaques, suivies des soins de santé (17 %) et du secteur public (15 %).
- Les augmentations les plus significatives entre les 2e et 3e trimestres 2021 concernent les secteurs Finance/Assurances (21 %) et Soins de santé (7 %).

Vecteurs d'attaque : 3e trim. 2021

Les incidents notables rendus publics par vecteur au 3e trimestre 2021 incluent notamment les suivants :

- Le malware a été la technique la plus souvent utilisée dans les incidents signalés au 3e trimestre 2021, même si ceux-ci ont diminué de 24 % par rapport au 2e trimestre.
- Les augmentations les plus significatives entre les 2e et 3e trimestres 2021 concernent le déni de service distribué (112 %) et les attaques ciblées (55 %).

EXPLOITATION DES RESSOURCES LOCALES

Les cybercriminels ont recours à des ressources locales qui utilisent des logiciels et des fonctions légitimes d'un système pour mener des activités malveillantes sur ce système. Sur la base des événements du troisième trimestre, Trellix a identifié certaines tendances dans les outils utilisés par les pirates tentant d'échapper à la détection. Si les collectifs à la solde d'États et les groupes cybercriminels plus importants possèdent les ressources nécessaires pour développer des outils en interne, nombre d'entre eux se tournent vers les fichiers binaires et les logiciels installés par les administrateurs déjà présents sur le système ciblé pour lancer différentes phases d'une attaque.

Pour identifier les fichiers binaires natifs et les logiciels d'administration au cours de la phase de reconnaissance d'une cible majeure, les cyberpirates peuvent recueillir des informations sur les technologies utilisées à partir d'offres d'emploi ou de témoignages clients publiés par les fournisseurs, ou encore grâce à un complice interne.

Fichiers binaires natifs du système d'exploitation		Commentaires
PowerShell *(41,53 %)*	T1059.001	PowerShell est souvent utilisé pour exécuter des scripts et des commandes PowerShell.
Windows Command Shell (CMD) *(40,40 %)*	T1059.003	Windows Command Shell est la principale interface de ligne de commande Windows et est souvent utilisé pour exécuter des fichiers et des commandes dans un autre flux de données.
Rundll32 *(16,96 %)*	T1218.011, T1564.004	Rundll32 peut servir à exécuter des fichiers DLL locaux, des fichiers DLL à partir d'un partage, des fichiers DLL obtenus sur Internet et d'autres flux de données.
WMIC *(12,87 %)*	T1218, 1564.004	WMIC est une interface de ligne de commande du service WMI qui peut être utilisée par les cybercriminels pour exécuter des commandes ou des charges actives virtuelles en local, dans d'autres flux de données ou sur un système distant.
Excel *(12,30 %)*	T1105	Même en l'absence d'une installation native, de nombreux systèmes possèdent une application de tableur. Les pirates informatiques peuvent donc envoyer à des utilisateurs des pièces jointes contenant du code ou des scripts malveillants qui, une fois exécutés, permettent de récupérer des charges actives depuis un site distant.
Schtasks *(11,70 %)*	T1053.005	Un pirate peut planifier des tâches pour assurer sa persistance, exécuter d'autres malwares ou effectuer des tâches automatisées.
Regsvr32 *(10,53 %)*	T1218.010	Regsvr32 peut être utilisé par des cybercriminels pour enregistrer des fichiers DLL, exécuter du code malveillant et contourner les listes blanches d'applications.
MSHTA *(8,78 %)*	T1218.005	MSHTA peut être utilisé par les cybercriminels pour exécuter des fichiers JavaScript, JScript et VBScript qui peuvent être dissimulés dans des fichiers HTA du système local et dans d'autres flux de données, ou encore être récupérés à partir d'un site distant.
Certutil *(4,68 %)*	T1105, 1564.004, T1027	L'utilitaire de commandes Windows permet d'obtenir des informations sur les autorités de certification et de configurer des services de certificats. Par ailleurs, les pirates peuvent utiliser certutil pour obtenir des outils et du contenu distants, coder et décoder des fichiers ou encore accéder à d'autres flux de données.
Net.exe *(4,68 %)*	T1087 et sous-techniques	L'utilitaire de ligne de commande Windows permet aux cybercriminels de se livrer à des opérations de reconnaissance, par exemple l'identification d'utilisateurs, de réseaux et de services sur l'ordinateur d'une victime.

Reg.exe *(4,10 %)*	1003.002, 1564.004		Reg.exe permet aux pirates d'ajouter, de modifier, de supprimer et d'exporter des valeurs de Registre qui peuvent être enregistrées dans d'autres flux de données. En outre, reg.exe peut servir à exfiltrer des identifiants d'un fichier SAM.

Outils d'administration			Commentaires
Services distants *(15,21 %)*	T1021.001, T1021.004, T1021.005	AnyDesk ConnectWise Control RDP UltraVNC PuTTY WinSCP	Les cybercriminels peuvent exploiter des services distants, à la fois natifs à Windows et de logiciels tiers, avec des comptes valides pour accéder à distance à un ordinateur ou une infrastructure, introduire des outils et des malwares ou encore exfiltrer des données.
Utilitaires d'archivage *(4,68 %)*	T1560.001	7-Zip WinRAR WinZip	Les pirates peuvent exploiter les utilitaires d'archivage pour compresser les données collectées en vue de leur exfiltration, de même que pour décompresser des fichiers et des exécutables.
PsExec *(4,68 %)*	T1569.002		PsExec est un outil utilisé pour exécuter des commandes et des programmes sur un système distant.
BITSAdmin *(2,93 %)*	T1105, T1218, T1564.004		BITSAdmin est généralement utilisé pour assurer la persistance, nettoyer des artefacts et appeler des actions supplémentaires lorsqu'un critère déterminé est satisfait.
fodhelper.exe *(1,17 %)*	T1548.002		Fodhelper.exe est un utilitaire Windows qui peut être exploité par les cybercriminels pour exécuter des fichiers malveillants avec des privilèges élevés sur l'ordinateur d'une victime.
ADFind *(0,59 %)*	T1016, T1018, T1069 et sous-techniques, T1087 et sous-techniques, T1482		Cet utilitaire de ligne de commande peut être utilisé par les pirates pour découvrir des informations d'Active Directory, telles que les approbations de domaines, les groupes d'autorisations, les systèmes distants et les configurations réseau.

RAPPORT SUR LES BUGS

Bugs en circulation

(Douglas McKee, ingénieur en chef et chargé de recherche, et d'autres blogueurs surveillent et analysent des vulnérabilités dans le rapport mensuel de bugs.)

La fin de l'année a vu l'apparition de nombreux bugs. Certains ont pu être facilement éliminés, tandis que d'autres ont laissé des traces plus durables. L'équipe suit et évalue chaque mois les nouvelles vulnérabilités — ou bugs — dès leur publication et signale celles qu'elle juge susceptibles d'avoir un impact important. Il ne s'agit pas ici d'un score CVSS ou d'un classement OWASP, mais d'une intuition fondée sur des années d'expérience.

Un moment de réflexion

Si l'on passe en revue les principaux bugs signalés au cours des derniers mois, plusieurs sortent du lot. Apache a connu une année difficile, tant avec son serveur web (CVE-2021-41773) qu'avec le composant Log4j (CVE-2021-44228), qui n'ont pas été épargnés par des bugs jugés critiques. Palo Alto n'y a pas échappé non plus avec la découverte d'un bug dans son VPN GlobalProtect (CVE-2021-3064), qui a eu un impact unique pendant la pandémie. Mais le grand gagnant reste le bug Log4j. En effet, la vulnérabilité d'Apache remporte la palme en étant de loin le bug le plus important de 2021, et risque de conserver sa première place pendant de longues années. Si vous n'en avez pas encore entendu parler, pensez à lire notre rapport sur les bugs de décembre. N'oubliez pas de revenir chaque mois pour découvrir toute l'actualité sur les vulnérabilités les plus critiques.

Intéressons-nous aux raisons de la gravité de ces bugs. En bref, ces bugs peuvent être exploités à distance, sans authentification, sur les outils installés à la périphérie de votre réseau. Ils peuvent servir de point d'entrée initial au réseau sans qu'un pirate doive se concentrer sur un composant particulier. En d'autres termes, ils ouvrent grand la porte à une attaque de grande envergure.

Si votre RSSI aime les risques et vous demande de ne corriger qu'un seul produit, nous vous conseillons vivement de remédier en priorité à la vulnérabilité Log4j, étant donné qu'elle est facile à exécuter et qu'elle a été activement exploitée par de nombreux groupes cybercriminels. Même si la faille observée dans le VPN de Palo Alto est grave et si les VPN ont enregistré une augmentation des tentatives d'exploitation depuis 2020, ce n'est rien par rapport à Log4j et aux autres vulnérabilités Apache, car la faille de Palo Alto affecte une version plus ancienne du logiciel VPN et aucune exploitation active n'a encore été observée.

Les « termites »

Certains bugs, à l'instar des termites, peuvent passer inaperçus pendant longtemps, mais avoir un effet dévastateur.

Un bug d'élévation de privilèges locaux de Microsoft Windows Installer Service, baptisé CVE-2021-41379, a remporté la palme parmi les bugs de novembre. Microsoft a indiqué que le bug nécessitait un accès local et y a soi-disant remédié avec un correctif officiel, mais cette stratégie s'est retournée contre la société après un dysfonctionnement du correctif en question.

Compte tenu du correctif défaillant et de la preuve de concept rendue publique, les cybercriminels n'ont pas tardé à l'intégrer à leurs scénarios d'attaque, comme l'a révélé l'étude Insights. Pour ne rien arranger, notre équipe a observé des versions opérationnelles de l'exploit en vente sur le Dark Web.

AUTRES SECTEURS ET PAYS DES CLIENTS CIBLÉS, ET TECHNIQUES MITRE ATT&CK

Pays des clients ciblés par les ransomwares

Figure 5. Les clients basés aux États-Unis représentent plus d'un tiers du nombre total de détections de ransomwares au 3e trimestre 2021.

Secteurs d'activité des clients ciblés par les ransomwares

Figure 6. Les secteurs Banques/Finance (22 %), Services d'utilité publique (20 %) et Vente au détail (16 %) représentent près de 60 % du nombre total de détections de ransomwares chez nos clients au 3e trimestre 2021.

Techniques MITRE ATT&CK de ransomware

Figure 7. La saisie de données (2,6 %), la découverte de fichiers et de répertoires (2,5 %) et la dissimulation de fichiers/d'informations (2,4 %) figurent parmi les principales techniques MITRE ATT&CK de ransomware détectées au 3e trimestre 2021.

Pays des clients ciblés par des menaces APT

Figure 8. Les détections de techniques APT chez les clients turcs représentent 17 % du nombre total de détections au 3e trimestre, suivies des États-Unis (15 %) et d'Israël (12 %).

Secteurs d'activité des clients ciblés par des menaces APT

Figure 9. Les principales détections de menaces APT au 3e trimestre 2021 ont été observées dans le secteur bancaire/financier (37 %), suivi des services d'utilité publique (17 %), de la vente au détail (16 %) et des administrations publiques (11 %).

Techniques MITRE ATT&CK APT

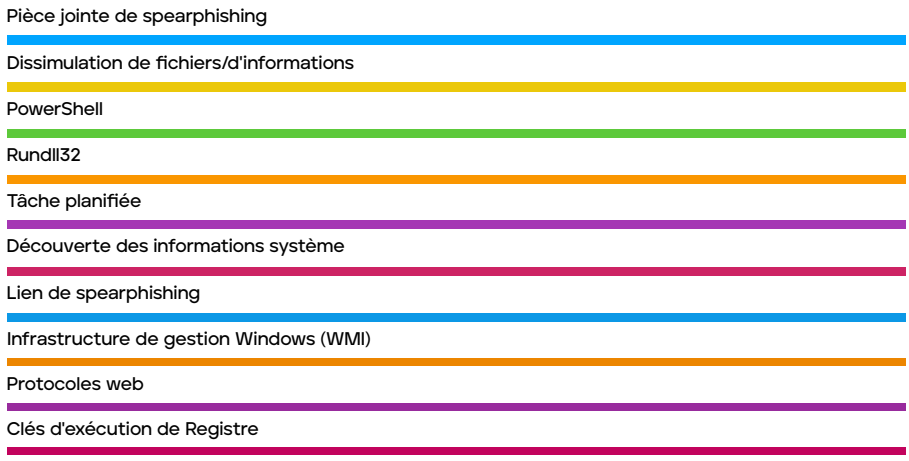


Figure 10. Les techniques MITRE ATT&CK APT les plus prévalentes au 3e trimestre 2021 sont la pièce jointe de spearphishing (16,8 %), la dissimulation de fichiers/d'informations (16,7 %) et PowerShell (16 %).

Pays des clients ciblés par des menaces ATR

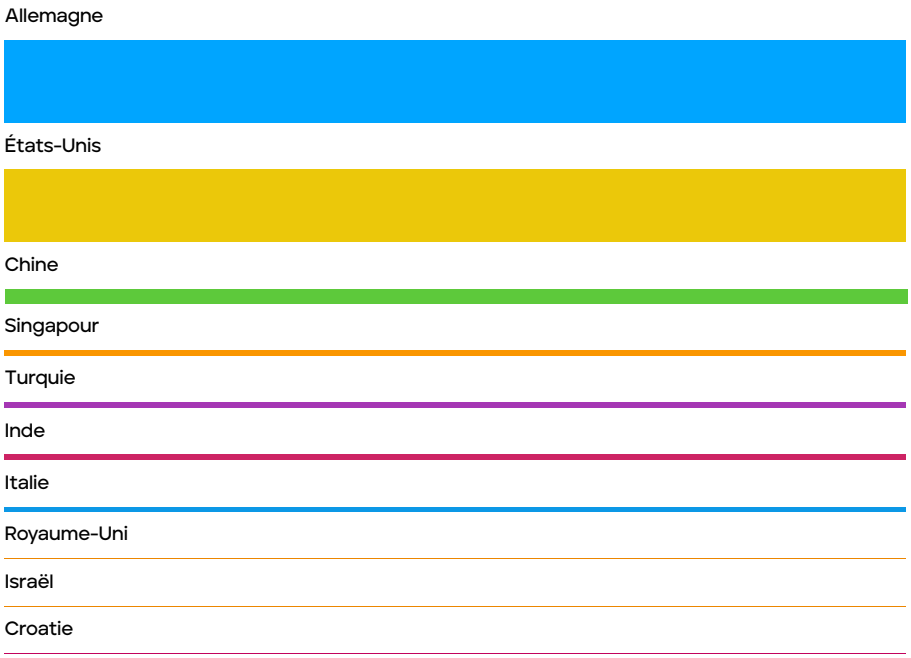


Figure 11. Plus de la moitié des menaces ATR du 3e trimestre ont été observées en Allemagne (32 %) et aux États-Unis (28 %).

Secteurs d'activité des clients ciblés par des menaces ATR

Figure 12. C'est dans le secteur bancaire/financier que l'on a observé le plus grand nombre de détections (45 %) au 3e trimestre 2021.

Figure 13. La dissimulation de fichiers/d'informations représente 5 % de toutes les détections de techniques MITRE ATT&CK ATR pour le 3e trimestre 2021.

RESSOURCES

Pour suivre l'évolution des menaces et des recherches, consultez les ressources suivantes de notre équipe :

Centre sur les menaces — Menaces actuelles les plus dévastatrices identifiées par notre équipe.

Twitter :

Trellix Labs

Raj Samani

Christiaan Beek

John Fokker

Steve Povolny

Douglas McKee

À propos de Trellix

Trellix est une société d'envergure internationale qui a pour vocation de redéfinir l'avenir de la cybersécurité. Sa plate-forme ouverte et native eXtended Detection and Response (XDR) aide les entreprises confrontées aux menaces actuelles les plus évoluées à avoir davantage confiance dans la sécurité et la résilience de leurs opérations. Les experts en sécurité de Trellix, soutenus par un vaste écosystème de partenaires, accélèrent l'innovation technologique grâce à l'apprentissage automatique et à l'automatisation afin de renforcer la protection de plus de 40 000 clients des secteurs privé et public. Plus d'infos sur www.trellix.com.

Trellix Threat Labs

S'abonner à nos informations sur les menaces

Trellix

6220 American Center Drive,
San Jose, Californie 95002