

Rapport sur les menaces mondiales

2024 —

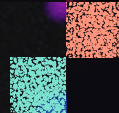
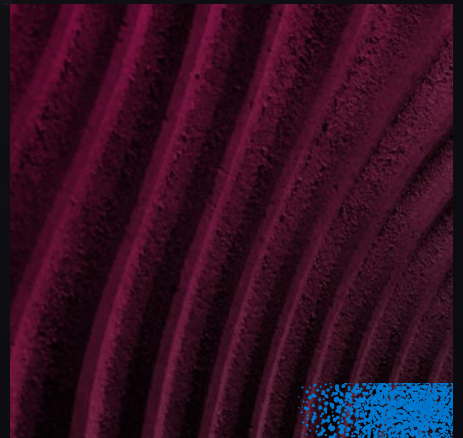


Table des matières

1	Introduction	03
2	Intelligence artificielle générative	04
	Aperçu des menaces	04
	Renforcer les défenseurs	05
3	Détections des malwares	06
	Distribution par système d'exploitation	06
	Catégories de malwares	07
4	Comportements des points de terminaison	11
	Distribution par système d'exploitation	11
	Distribution par tactique	12
5	Sécurité du cloud	36
	Distribution par fournisseur de services cloud	37
	Évaluation comparative de la posture de sécurité du cloud	47
6	Profil des menaces	57
	REF5961 : BLOODALCHEMY, RUDEBIRD, EAGERBEE, DOWNTOWN	58
	REF8207 : GHOSTPULSE	61
	REF4578 : GHOSTENGINE	64
	REF7001 : KANDYKORN	66
	REF6127 : WARMCOOKIE	69
7	Réponses aux prévisions de 2023	72
8	Prévisions et recommandations	75
9	Conclusion	79

Introduction

Grâce aux meilleures technologies, à la diffusion d'informations la plus large et à la plus grande sensibilisation du public aux menaces, l'environnement de sécurité est plus fort que jamais. Pourtant, presque en dépit de tout cela, les écosystèmes de menaces prospèrent comme jamais auparavant.

En vérité, le paysage des menaces est dynamique et réactif : une nouvelle technique donne du pouvoir à un groupe de menaces jusqu'alors inconnu, les fournisseurs fourmillent pour atténuer cette menace et créer de nouvelles technologies dans le processus, les opérateurs des deux côtés recherchent de nouvelles techniques ou de nouveaux outils, et ainsi de suite. Ce paysage est façonné quotidiennement par les efforts des attaquants et des défenseurs. Ce rapport est l'un des moyens par lesquels [Elastic Security Labs](#) se responsabilise en tant que force de changement pour le bien dans un environnement dynamique, en partageant ce que nous observons, ainsi que ce qui, selon nous, nécessite une plus grande visibilité.

L'objectif de notre rapport sur les menaces mondiales est le même que ces deux dernières années : démocratiser la connaissance, défendre des principes de transparence et identifier les impacts. Nous tirons parti de la puissante technologie mondiale d'Elastic afin de fournir des informations uniques qui éclairent nos priorités

pour la solution Elastic Security et servent l'ensemble de la communauté de la sécurité.

Ce rapport ne serait pas possible sans la communauté de la sécurité : nos observations sont basées sur des milliards d'événements de sécurité volontairement partagés par nos utilisateurs, enrichis d'open sources, représentant des dizaines de milliers d'entités distinctes dans pratiquement tous les secteurs d'activité. Le précieux partenariat que nous entretenons avec nos utilisateurs nous permet de découvrir des menaces jusqu'alors inconnues dans leurs données et de partager anonymement ces découvertes avec l'ensemble du secteur de la sécurité. Cette collaboration a donné lieu à des centaines de nouvelles protections, librement accessibles au public. Nous tenons à remercier chaleureusement nos utilisateurs : les enseignements tirés de ces données partagées profitent à l'ensemble de la communauté de la sécurité.

En tant que groupe de recherche, nous nous appuyons sur les technologies d'Elastic et les alimentons. À bien des égards, nous démontrons également ce qui peut être réalisé avec la solution [Elastic Security](#). La même visibilité et les mêmes fonctionnalités que celles fournies par nos utilisateurs sont à l'origine de ces informations exploitables, et nous sommes impatients de voir les autres contributions positives qu'elles apporteront au paysage des menaces dans son ensemble.

Intelligence artificielle générative

L'essor de l'[intelligence artificielle générative](#) (IA générative) a suscité un immense enthousiasme, avec l'espoir que cette technologie touchera bientôt, d'une manière ou d'une autre, presque tous les aspects de la vie. Cet enthousiasme s'est également accompagné d'une hésitation compréhensible et d'un désir de comprendre comment cette nouvelle technologie pourrait être utilisée à mauvais escient. Elastic n'est pas étranger à l'IA générative. Alors que nombre de nos collègues intègrent des [capacités incroyables](#) dans nos produits, Elastic Security Labs et nos partenaires chargés de la sécurité des informations ont également consacré beaucoup de temps à la compréhension de la technologie et des risques qui y sont associés.

Aperçu des menaces

Augmentation du phishing et de l'ingénierie sociale

Comme de nombreuses personnes, nous avons anticipé que l'un des premiers cas d'utilisation de l'IA générative serait la création de campagnes de phishing plus sophistiquées. Soudain, les acteurs malveillants peuvent scaler la création de documents personnalisés difficiles à distinguer des communications légitimes. Bien que cette

technique soit encore en cours de maturation, des exemples de ces incidents sont déjà à l'[étude](#). À plus grande échelle, des escroqueries basées sur le deepfake ont interféré avec des élections politiques et certains cas d'extorsion ([ABC](#), par exemple). L'utilisation d'outils d'IA générative pour créer des deepfakes, vidéo ou audio d'une personne qui a été manipulée pour diffuser de fausses informations, continuera à représenter une menace dans les années à venir. Il est toutefois important de noter que les deepfakes ont été limités en termes d'incidents de cybersécurité. Ces deux menaces vont continuer à s'accélérer, ce qui réaffirme l'importance de former les utilisateurs à identifier les créations d'IA. Les programmes de formation à la cybersécurité à l'échelle de l'organisation ont joué un rôle crucial pour mettre fin aux tentatives de phishing régulières. Il est donc important que les directeurs de la sécurité de l'information et les autres responsables de la sécurité mettent également en œuvre des formations axées sur l'IA dans leurs programmes.

Développement de malwares

Des [recherches](#) ont mis en évidence la façon dont l'IA a été utilisée pour créer des malwares plus adaptatifs, mais cette technologie n'a pas encore été adoptée à grande échelle. L'étendue de la disponibilité des malwares basés sur l'IA reste un sujet de préoccupation et, à mesure que les modèles et les services deviennent plus accessibles, ce phénomène continuera à se développer.

À l'instar du développement de malwares classiques, les équipes de sécurité doivent rester à jour sur les menaces et les tendances. De plus, il sera essentiel de maintenir une [bibliothèque de protections](#) robuste avec des règles constamment mises à jour et [ajustées](#).

Renforcer les défenseurs

Comme toute technologie, l'IA générative peut faire l'objet d'abus, mais cela ne veut pas dire qu'elle n'est pas un outil incroyablement puissant entre les mains des défenseurs.

Outils de cybersécurité améliorés

L'une des nombreuses perspectives intéressantes du développement de fonctionnalités d'IA générative spécifiquement destinées aux défenseurs était l'idée d'une détection avancée des menaces, en particulier un moyen de synthétiser automatiquement les alertes et de les transformer en attaques de la plus haute priorité. L'automatisation des tâches manuelles répétitives de tri permet aux professionnels de mettre fin à la monotonie et de concentrer leurs efforts sur des initiatives stratégiques. Nous sommes ravis qu'Elastic ait intégré cette fonction dans notre solution Security, et qu'elle existe pour aider les défenseurs dans leur quotidien avec [Attack Discovery](#).

Une autre utilisation intéressante pour les équipes de défense se présente sous la forme de tests de sécurité automatiques, dont l'adoption s'est accrue ces dernières années. Ils n'ont pas complètement remplacé les méthodologies de test traditionnelles, et nous ne pensons pas que ce sera un jour le cas, mais ils sont devenus utiles pour identifier plus efficacement les vulnérabilités et devraient continuer à s'améliorer.

Pour aller encore plus loin, l'IA générative permet d'améliorer la formation à la cybersécurité des équipes chargées de la sécurité des informations, les simulations devenant plus réalistes. Bien que cette approche soit très prometteuse, elle n'en est qu'à ses débuts et devra être affinée avant d'être adoptée à grande échelle.

Gouvernance et déontologie

L'IA générative est puissante et restera un outil important pour les équipes et les professionnels de la sécurité au fil du temps. Toutefois, l'utilisation de technologies puissantes nécessite une approche ferme et déontologique. Heureusement, les organisations et les gouvernements du monde entier s'empressent d'élaborer des lignes directrices en matière de sécurité, ainsi que des cadres responsables.

En voici quelques exemples :

- [Cadre de gestion des risques liés à l'IA du NIST](#) : ce cadre, élaboré par le National Institute of Standards and Technology, est axé sur la gouvernance, le mapping des risques, la mesure et la gestion de l'IA.
- [FAIR-AIR](#) : ce cadre de l'Institut FAIR aide les équipes à identifier l'exposition aux pertes liées à l'IA et à prendre des décisions basées sur les risques.
- [AI TRISM](#) : le cadre de Gartner garantit des mises en œuvre d'IA fiables, sûres et conformes, en mettant l'accent sur l'ensemble du cycle de vie.

Elastic Security Labs se réjouit de garder un œil sur cette technologie émergente et continuera à rendre compte de son évolution. Vous trouverez un examen plus approfondi des menaces et des protections pour les applications d'IA générative, en particulier les grands modèles de langage, dans notre [évaluation concernant la sécurité des LLM](#).

Détection des malwares

Elastic Security fournit des mécanismes permettant de détecter et d'atténuer les malwares sur tous les principaux systèmes d'exploitation de bureau. À ces fins, un malware est un logiciel développé pour faciliter les actions de l'utilisateur malveillant, perturber des activités légitimes ou causer des dommages à un ordinateur ou à un réseau. Dans cette section, vous trouverez des informations détaillées sur la distribution des malwares par système d'exploitation, catégorie et famille, ainsi qu'une ventilation des observations de ransomwares.

Cette année, Elastic Security Labs a examiné les alertes de protection contre les malwares et de protection de la mémoire contre les menaces d'Elastic Security. Afin d'améliorer la précision de nos observations de malwares, cette sous-section n'inclut que les événements de signatures YARA pour les familles de malwares nommées. Les signatures YARA sont un composant puissant d'Elastic Security, qui permet d'atténuer les malwares utilisant des séquences de chaînes ou

d'octets trouvées dans les exécutable. Ces signatures, qui s'appliquent à la fois au système de fichiers et aux logiciels résidant dans la mémoire, sont accessibles au public via le [référentiel Protections Artifacts d'Elastic](#), dans le cadre de notre engagement permanent en faveur des principes de gratuité et d'ouverture.

Les éléments présentés dans cette section du rapport d'Elastic sur les menaces mondiales comprennent les capacités et les phénomènes de menace les plus importants observés dans la télémétrie d'Elastic au cours de l'année écoulée. Les utilisateurs d'Elastic partagent volontairement ces alertes et d'autres données avec nous, fournissant à Elastic Security Labs un outil puissant pour découvrir, diminuer et perturber les menaces. Cette télémétrie se compose de données provenant d'Elastic Security, d'Elastic Agent et d'un large éventail d'instruments tiers.

Distribution par système d'exploitation

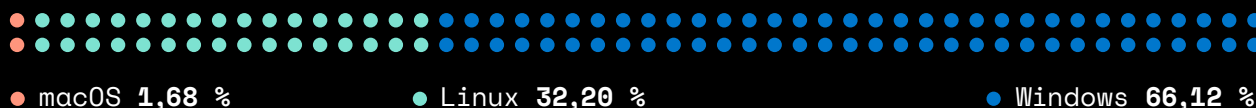


Figure 1 : infections par malwares par système d'exploitation

Windows

La distribution des événements YARA entre les différents systèmes d'exploitation suggère une certaine disparité dans la prévalence des menaces. Les hôtes Windows représentent la majorité des détections avec 66,12 % de tous les cas détectés. Ce résultat n'est pas totalement inattendu étant donné l'utilisation répandue de Windows dans les environnements d'entreprise et sa sensibilité, tant historique qu'actuelle, aux diverses techniques employées par les malwares. Bien qu'il soit trompeur d'affirmer qu'un système d'exploitation est "le plus susceptible" d'être infecté, des techniques telles que [Bring Your Own Vulnerable Driver \(BYOVD\)](#) représentent des conditions architecturales que les acteurs malveillants ciblent fréquemment pour atteindre leurs objectifs.

Linux

Les hôtes Linux représentent toujours une part importante des infections avec 32,20 %. Cela peut laisser penser que les utilisateurs malveillants [ciblent les systèmes Linux](#) de plus en plus, probablement en raison de leur prévalence dans les environnements de serveurs et les infrastructures stratégiques. Les conteneurs Linux, qui sont souvent destinés à exister pendant quelques minutes ou quelques heures plutôt que pendant des semaines ou des mois, peuvent contenir des vulnérabilités non corrigées que même des menaces naissantes peuvent exploiter.

Les lecteurs doivent noter que l'année dernière, nous avons signalé que 92 % des infections par malwares concernaient des points de terminaison Linux, en partie à cause de l'inclusion d'événements faiblement attribuables. Ce changement est dû en partie aux modifications apportées par notre équipe à la façon dont nous traitons la télémétrie d'Elastic, afin de fournir une représentation plus précise des observations courantes de malwares sur les points de terminaison, ainsi que des catégories plus larges de malwares décrites.

macOS

Les hôtes macOS représentent la plus petite proportion de points de terminaison dont Elastic reçoit la télémétrie. Dans cette optique, macOS représente également le plus petit nombre d'observations de malwares avec 1,68 %. Elastic Security Labs n'en conclut pas que macOS est plus sûr, moins répandu dans les entreprises ou moins susceptible d'être ciblé. En réalité, les recherches que nous avons menées en début d'année sur les [applications macOS piratées](#) ont révélé que plusieurs méthodes simples d'infection de ces systèmes étaient largement utilisées.

Catégories de malwares

La sous-catégorisation des malwares sera nécessairement subjective, définie du point de vue de chaque fournisseur ou entité déclarante. Les catégories présentées ici correspondent aux collections de signatures YARA et sont expliquées plus en détail ci-dessous.

Catégorie de malware	Somme
Cheval de Troie	82,03 %
Générique	8,03 %
Mineur de cryptomonnaie	4,39 %
Ransomware	2,10 %
Porte dérobée	1,01 %
Autre	2,44 %

Tableau 1 : catégories de malwares observées

Les chevaux de Troie représentent 82,03 % de tous les types de malwares observés, une proportion attribuée à l'utilité de se faire passer pour des logiciels légitimes. Une fois exécutés, les chevaux de Troie déploient souvent des charges utiles malveillantes supplémentaires telles que des [infostealers](#) (voleurs d'informations), servant ainsi de mécanisme de diffusion pour divers types de malwares.

L'année dernière, nous avons signalé que les chevaux de Troie représentaient environ 61 % de tous les types de malwares que nous avons observés. L'augmentation de 21 % est attribuée à un nombre restreint mais largement distribué d'applications ciblées par des chevaux de Troie. Bien que de nombreuses organisations qui choisissent de partager des données utilisent des contrôles au niveau des applications, rares sont celles qui ont adopté des listes de blocage ou d'autorisation de manière à limiter l'exécution de logiciels inconnus.

La catégorie "Générique" comprend 8,03 % des infections, ce qui représente des menaces largement identifiées qui ne correspondent pas à une classification spécifique des malwares, mais qui présentent tout de même des risques importants. Par exemple, un malware générique peut être développé par un développeur de malwares en herbe, nouveau dans l'écosystème. Nous avons observé un changement significatif dans les identifications de mineurs de cryptomonnaie cette année, passant de 21,80 % à 4,39 %. Les logiciels de cryptomining tirent parti de la scalabilité des ressources pour calculer les cryptomonnaies et jouent un rôle de plus en plus important dans les scénarios à motivation financière. Des familles comme [GHOSTENGINE](#), découverte en mai 2024, contiennent une application de cryptomining qui peut être installée lors d'intrusions. Vous trouverez plus d'informations sur GHOSTENGINE dans la section *Profils des menaces* de ce rapport.

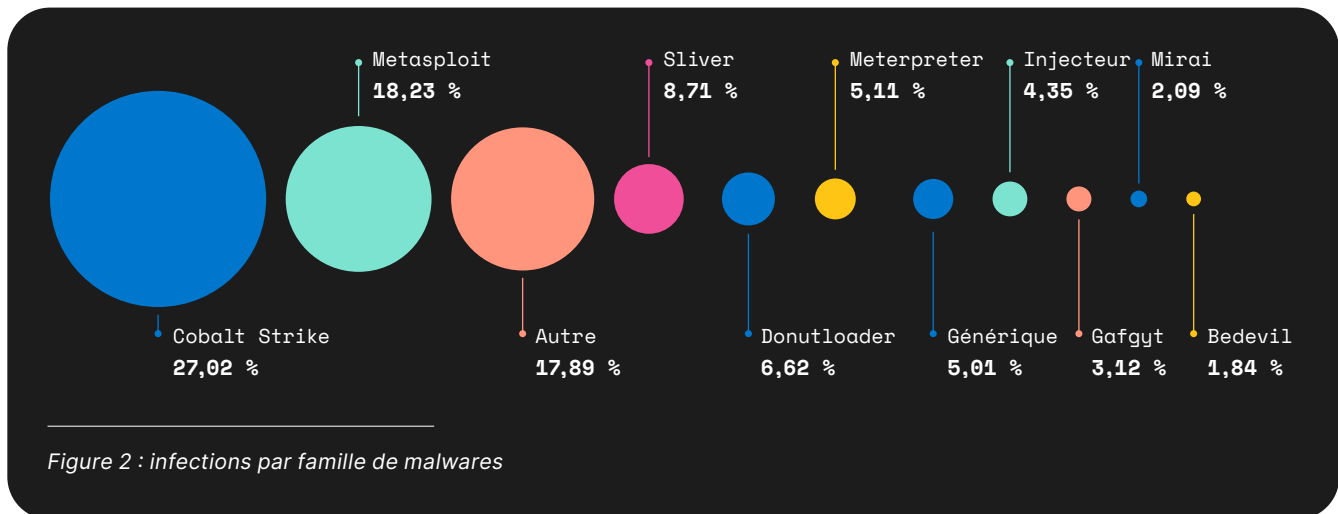
Les observations de ransomwares basés sur YARA représentent 2,10 % des détections et renforcent le fait que les ransomwares restent une menace critique, principalement en raison des conséquences de l'extorsion, du vol et de la perte de réputation qui en résultent. YARA fonctionne en complément des protections contre les ransomwares et autres logiciels malveillants, avec un intervalle de distribution plus court, idéal pour répondre rapidement aux menaces émergentes.

Les portes dérobées représentent 1,01 % des malwares observés et seront familières à de nombreux lecteurs. Elles sont souvent utilisées comme des chevaux de Troie pour fournir des mécanismes d'intrusion. Tous les lecteurs ne savent peut-être pas que les logiciels de suivi et de gestion à distance, moins de la moitié du 1 %, sont l'outil de prédilection de nombreux escrocs qui utilisent l'urgence parallèlement à d'autres approches d'ingénierie sociale pour convaincre les utilisateurs de s'auto-infecter.

Familles de malwares

Nous pouvons examiner la distribution des correspondances de signatures YARA pour constater qu'un petit nombre de familles de malwares apparaissent régulièrement : Cobalt Strike, Metasploit, Sliver, DONUTLOADER et Meterpreter représentent environ les deux tiers de tous les malwares que nous avons observés l'année dernière. La distribution des malwares par catégorie (figure 2) révèle un chevauchement important entre les logiciels ciblés par des chevaux de Troie et la présence de ces familles de malwares. Nous présentons les informations de cette manière (en excluant les familles de ransomwares), car celles-ci étaient le plus souvent observées lors des étapes ultérieures des intrusions, après que bon nombre de ces familles de malwares répandues étaient déjà présentes dans l'environnement. Les entreprises doivent donner la priorité aux malwares à toutes les étapes du cycle de vie des intrusions afin de réduire les risques de conséquences néfastes.

Les outils de sécurité offensifs font régulièrement l'objet de débats animés en ce moment, en grande partie à cause de la fréquence à laquelle ils sont utilisés de manière abusive par des acteurs malveillants. Les familles de malwares les plus fréquemment observées sont principalement liées aux outils de sécurité offensifs, ce qui représente une augmentation significative par rapport à l'année dernière. Cependant, il est essentiel que les lecteurs comprennent que la communauté de la sécurité offensive existe dans leur intérêt.



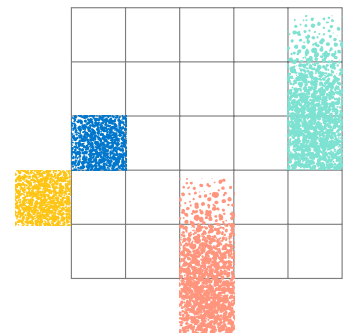
La famille de malwares la plus répandue que nous avons observée cette année est [Cobalt Strike](#), qui représente de 27,02 % des infections. Cobalt Strike est un framework commercial de post-exploitation très mature doté d'une équipe de recherche et de développement expérimentée. Il est tellement efficace que les [acteurs malveillants](#) volent et utilisent fréquemment ce produit pour atteindre leurs objectifs malveillants plutôt que l'objectif bénin pour lequel il était destiné.

Les variantes de Metasploit représentent 18,2 % des correspondances YARA et constituent un autre exemple d'utilisation abusive des outils de sécurité offensifs par les acteurs malveillants. [Meterpreter](#), le shell inversé fourni avec Metasploit, figure également dans le top 10 des familles les plus courantes, avec 5,1 % des signaux. Elastic Security Labs [maintient la visibilité](#) de ces familles, qui apparaissent régulièrement ensemble. [Sliver](#), avec 8,71 % des infections, est un outil de sécurité offensif conçu pour la simulation d'utilisateurs malveillants. Son utilisation dans les activités de post-exploitation démontre la

puissance de ses capacités. Les observations de Sliver ont augmenté de manière significative par rapport à l'année dernière. [DONUTLOADER](#), qui représente 6,62 % des infections, sert de programme de chargement pour exécuter des charges utiles malveillantes supplémentaires en mémoire, ce qui permet d'éviter les mécanismes de détection sur disque.

Les familles de malwares telles que Gafgyt (3,12 %), Mirai (2,09 %) et Bedevil (1,84 %) sont apparues moins souvent que les années précédentes, ce qui peut s'expliquer par les tentatives de neutralisation de la propagation des botnets. Ces familles de malwares sont généralement distribuées sur des appareils de l'Internet des objets, tels que les routeurs résidentiels à haut débit, en utilisant des identifiants codés en dur ou des vulnérabilités non corrigées, et sont utilisées pour lancer des attaques par déni de service (DDoS) et pour détourner des réseaux publicitaires ou DNS.

La distribution des familles de malwares rappelle l'importance d'une instrumentation des points de terminaison capable d'identifier et d'atténuer les logiciels malveillants, et les entreprises qui misent sur la visibilité plutôt que sur les capacités peuvent obtenir de moins bons résultats que celles qui ne le font pas. L'utilisation des outils de sécurité offensifs par les menaces est un indicateur fort que les innovations techniques, la maturité procédurale, l'adoption du moindre privilège et le partage d'informations ont un impact sur les acteurs malveillants.

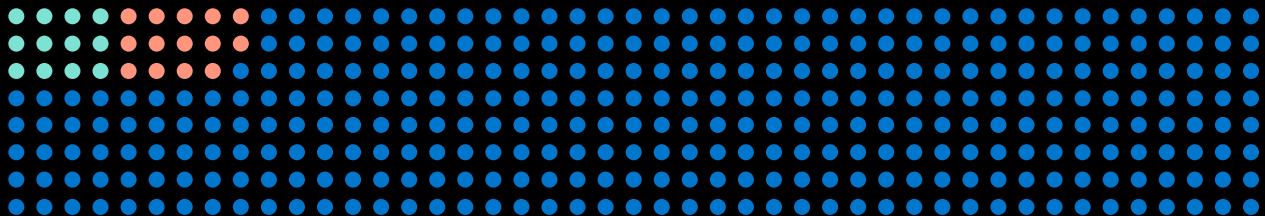


Comportements des points de terminaison

Les professionnels de la sécurité définissent souvent une menace en termes de tactiques, de techniques et de procédures. Autrement dit, quelles sont les méthodes axées sur les objectifs utilisées par les menaces ? Cette section décrit les tactiques, techniques et procédures les plus couramment observées sous Windows, macOS et Linux.

Distribution par système d'exploitation

● Linux 3,30 % ● macOS 3,97 %



● Windows 92,73 %

Figure 3 : alertes de comportement des points de terminaison par système d'exploitation

Windows

La majorité des comportements des points de terminaison que nous avons observés l'ont été sur des hôtes Windows, soit 92,73 % de toutes les observations. Il s'agit d'une légère baisse par rapport aux 94,2 % de l'année dernière, soit une diminution d'environ 1,5 %. Ces statistiques reflètent les proportions des systèmes partageant

la télémétrie avec nous, des populations qui fluctuent régulièrement à de faibles degrés.

Linux et macOS

Les événements Linux sont passés de 2,80 % l'année dernière à 3,30 %, soit une fluctuation d'un demi pour cent. Avec 3,97 %, les événements macOS ont augmenté d'à peine 1 % par rapport à

l'année dernière. L'augmentation des détections sous macOS peut être attribuée à l'intérêt croissant des utilisateurs malveillants pour l'exploitation des vulnérabilités de macOS, comme nous l'avons souligné dans nos [recherches](#) en début d'année.

Étant donné que des phénomènes relativement rares peuvent être artificiellement amplifiés dans de petites populations de systèmes, les lecteurs doivent savoir que les statistiques relatives à macOS et Linux ne sont pas significatives et peuvent ne pas ressembler à ce que vous observez. Ils ont été inclus en tant que points de données et n'influencent pas les recommandations.

Distribution par tactique

Les tactiques sont parfois mieux considérées comme des *objectifs*, et les techniques organisées en leur sein peuvent être considérées comme des moyens de les atteindre. Chaque protection

comportementale prédéfinie et développée par Elastic est alignée sur [MITRE ATT&CK®](#), la taxonomie des tactiques, techniques et procédures la plus largement acceptée, et cette section en tiendra compte.

En règle générale :

- *Les attaques par persistance* ont augmenté de près de 8 %.
- *Les événements d'évasion de défense* ont diminué à 38 %, soit une différence de près de 6 % par rapport à l'année dernière.
- *L'exécution* est restée courante, représentant environ 16 % des tactiques détectées.

Les tactiques de *persistance*, d'*évasion de défense* et d'*exécution* sont couramment employées dans une certaine combinaison par les utilisateurs malveillants lors d'intrusions. Ces trois tactiques représentent près de 70 % de tous les comportements observés au cours de l'année écoulée, soit une diminution par rapport à l'année dernière où elles représentaient plus de 81 %.

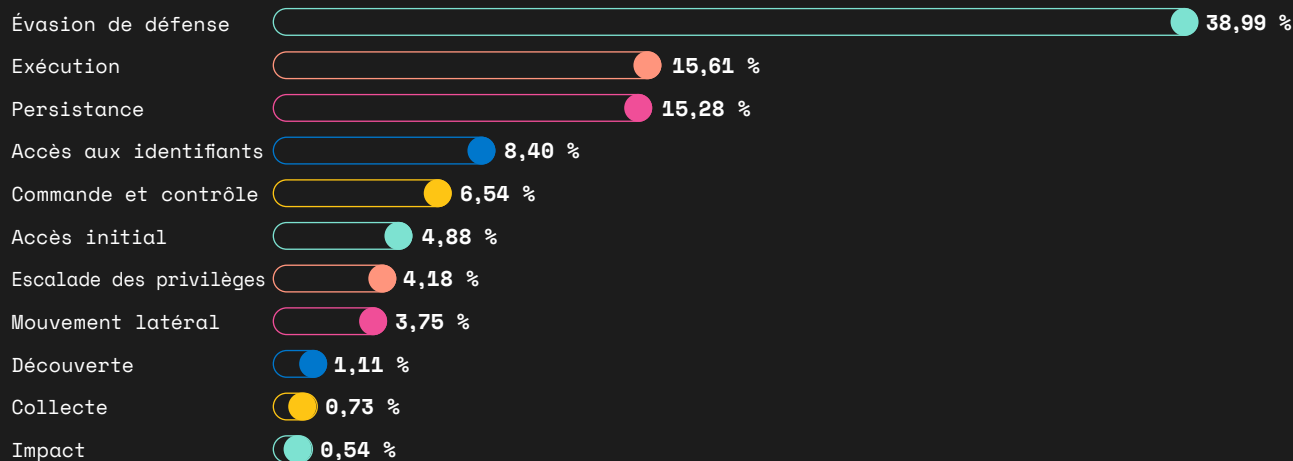


Figure 4 : alertes de comportement EDR par tactique

Étonnamment, nous avons observé une diminution de près de 2 % des détections liées à l'*escalade des privilèges* par rapport à l'année précédente. La menace croissante des voleurs d'informations et la distribution généralisée des identifiants volés ont peut-être réduit la nécessité de cette tactique. Par exemple, nous avons constaté une légère augmentation de 3 % des détections d'*accès aux identifiants*, comme [décrit](#) dans notre analyse plus tôt cette année.

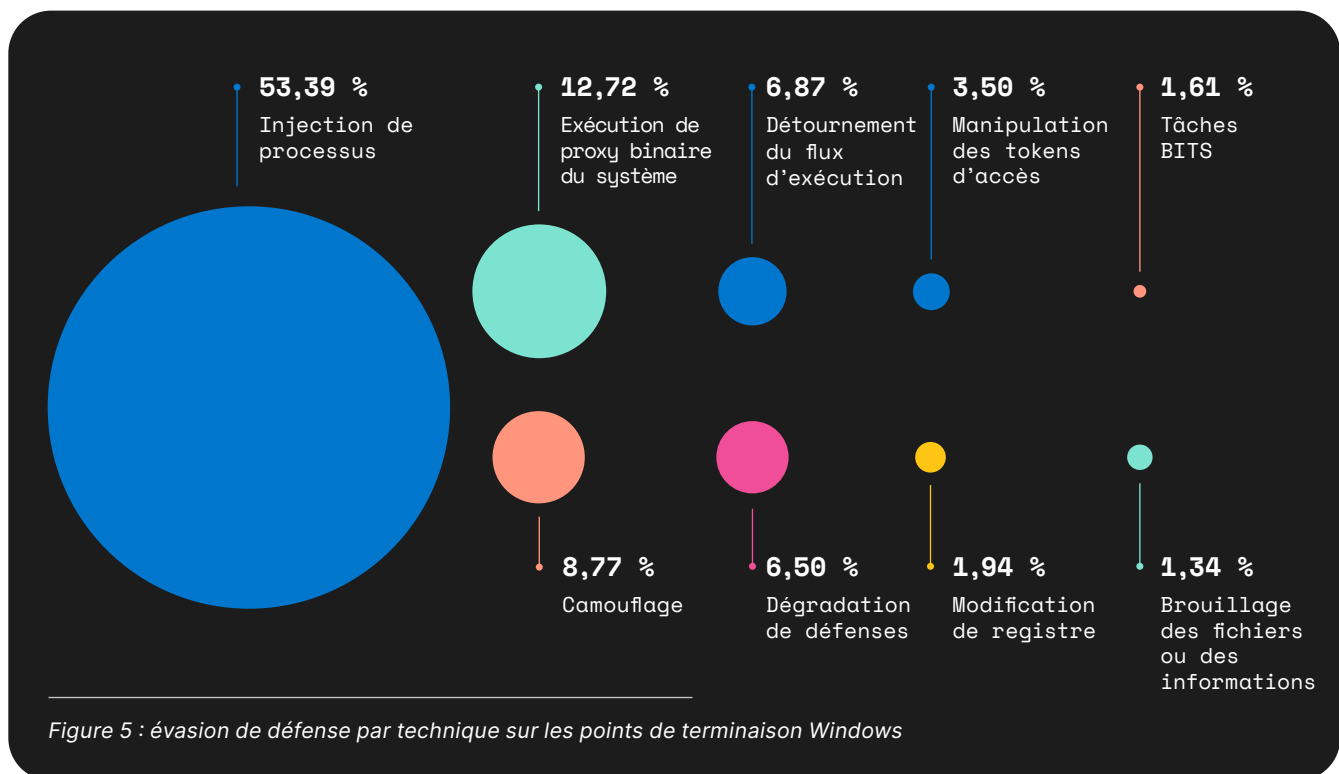
Évasion de défense

L'évasion de défense reste la principale tactique des utilisateurs malveillants. Représentant environ 38 % de toutes les détections, il s'agit de techniques utilisées pour contourner ou aveugler les fonctionnalités de sécurité.

Windows

Les techniques les plus courantes de cette catégorie, à savoir l'*injection de processus*, l'*exécution de proxy binaire du système* et la *dégradation de défenses*, décrivent collectivement des chaînes d'attaque entières : un acteur malveillant exploite une vulnérabilité dans une application cliente, injecte un code malveillant dans

un processus privilégié et génère `rundll32.exe` pour exécuter une bibliothèque de liens dynamiques (DLL) contrôlée par l'utilisateur malveillant, qui écrit sur le disque un pilote vulnérable utilisé pour désactiver les capteurs EDR (Endpoint Detection & Response, Détection et réponse aux points de terminaison).



Cette année, les détections d'*injection de processus* ont augmenté d'environ 31 %, représentant désormais 53,39 % de toutes les détections d'*évasion de défense*. L'*injection de processus* est une méthode couramment utilisée

pour injecter un code malveillant dans d'autres processus, ce qui le rend plus difficile à détecter et lui permet potentiellement de contourner les contrôles de sécurité.

L'exécution de proxy binaire du système, qui représentait près de 47 % des détections l'année dernière, a diminué d'environ 35 % pour atteindre 12 %. Cette technique consiste à utiliser des binaires de systèmes fiables pour exécuter par procuration des charges utiles malveillantes, une méthode qui est devenue moins courante à mesure que les capacités

de détection se sont améliorées. La diminution de cette technique suggère que les utilisateurs malveillants adaptent leurs stratégies en réponse aux mesures de sécurité renforcées.

La technique de *dégradation de défenses* a légèrement augmenté pour atteindre 9,56 %. Nous l'associons le plus souvent à la désactivation d'outils de sécurité ou de sources de données.

rule_name	Pourcentage
Network Module Loaded from Suspicious Unbacked Memory	13,67 %
Suspicious Memory Write to a Remote Process	6,05 %
Potential Masquerading as Windows Error Manager	5,07 %
Remote Thread Context Manipulation	4,22 %
Potential Injection via an Exception Handler	3,88 %
Potential Remote Code Injection	3,87 %
Potential Evasion via Sleep Obfuscation	3,63 %
Suspicious Remote Memory Allocation	3,30 %
Microsoft Common Language Runtime Loaded from Suspicious Memory	3,23 %
Suspicious Windows API Call via ROP Gadgets	3,07 %

Tableau 2 : top 10 des injections de processus par règle sur les points de terminaison Windows

Comment expliquer cette augmentation significative des techniques d'*injection de processus* ? Si l'on décompose les injections de processus par règles de comportement prédéfinies d'Elastic Security, on constate que la majorité d'entre elles sont dues à des intrusions suspectes dans la mémoire provenant des gestionnaires d'exceptions Windows et qu'elles représentent 9 % des détections. Cette logique de détection se concentre sur un ensemble spécifique de comportements de l'API Windows et de routines de la pile d'exécution où des symboles liés aux gestionnaires d'exceptions sont présents. Elastic Security Labs a analysé un comportement similaire avec le téléchargeur basé sur un shellcode [GULoader](#).

Nous avons également observé un nombre important de comportements de points de terminaison suspects liés à la détection de régions de mémoire non sauvegardées dans l'espace d'adressage de processus : près de 14 % des détections d'*injection de processus* étaient du code non sauvegardé, ce qui signifie qu'elles n'étaient pas directement liées à un fichier exécutable sur le disque. Les acteurs

malveillants utilisent fréquemment la mémoire non sauvegardée pour injecter ou exécuter du code malveillant dans des processus existants. Cela peut se faire via l'*injection de processus* ou l'*exécution de shellcodes*.

Les agents Windows d'Elastic Security ont une visibilité sur les appels d'API et les piles d'exécution, ce qui permet une détection basée sur les bibliothèques de liens dynamiques

natives chargées lorsque l'analyse de la pile d'exécution montre des trames indiquant des régions de mémoire qui ne sont pas soutenues par une image exécutable connue sur le système de fichiers. Sliver, l'un des principaux frameworks de *commande et contrôle* (C2) décrits précédemment dans ce rapport, utilise *l'injection de processus* et le code non sauvegardé, comme décrit dans [Hunting in Memory](#) et [Upping the Ante](#).

L'exécution de proxy binaire du système reste répandue pour les utilisateurs malveillants, bien distribuée entre différentes techniques pour y parvenir. D'après les détections d'Elastic Security, il est évident que près de 20 % de toutes ces activités sont liées à l'utilisation abusive de

[rund1132.exe](#). Elastic Security Labs en a pris note lors de l'analyse de [LATRODECTUS](#). Plus précisément, des familles de malwares similaires téléchargent une bibliothèque de liens dynamiques à partir des serveurs C2 respectifs, écrivent sur le disque avec un nom de fichier généré de manière aléatoire et exécutent simplement le code malveillant dans la bibliothèque de liens dynamiques à l'aide de [rund1132.exe](#). Par ailleurs, lors de la découverte de [WARMCOOKIE](#) par Elastic Security Labs, un script PowerShell a invoqué l'utilitaire de service de transfert intelligent en arrière-plan (BITS) pour télécharger et exécuter une bibliothèque de liens dynamiques malveillante.

rule_name	Pourcentage
Script Execution via Microsoft HTML Application	13,71 %
Unusual DLL Extension Loaded by Rundll32 or Regsvr32	11,55 %
Suspicious Execution via DCOM	10,68 %
Binary Proxy Execution via RunDLL32	8,30 %
Suspicious MsiExec Child Process	8,04 %
Regsvr32 with Unusual Arguments	7,75 %
Execution via Renamed Signed Binary Proxy	7,01 %
RunDLL32 with Unusual Arguments	6,85 %
Suspicious Execution via DotNet Remoting	2,90 %
Potential Evasion via DotNet Framework Installation Utility	2,64 %

Tableau 3 : top 10 des exécutions de proxy binaire du système par règle sous Windows

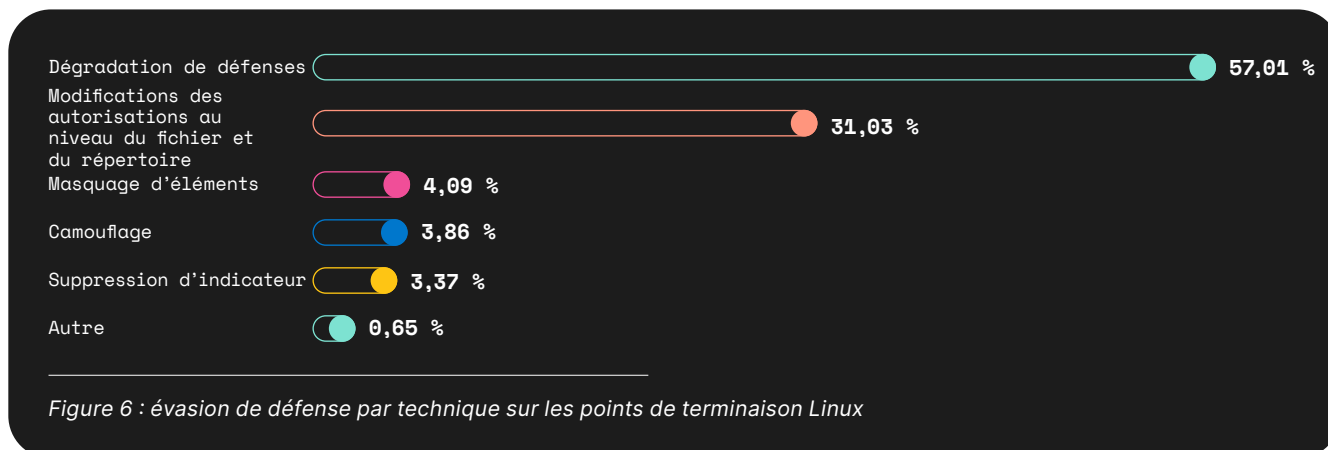
L'exécution via des applications HTML Microsoft était également courante, diminuant d'environ 4 % à 14 % du total des détections d'*exécution de proxy binaire du système*. Ceci identifie l'exécution de scripts via des applications HTML utilisant soit [rund1132.exe](#), soit [mshta.exe](#). Les utilisateurs malveillants peuvent contourner les défenses basées sur les processus et/ou les signatures en exécutant par procuration des contenus malveillants à l'aide de

ces binaires Microsoft signés, présents par défaut sur tous les systèmes Windows.

L'utilisation abusive de [mshta.exe](#) était notamment plus fréquente que celle de [rund1132.exe](#). Les chercheurs ont remarqué que les codes malveillants étaient hébergés dans des fichiers portant l'extension [.hta](#), tandis que dans le cas de [rund1132.exe](#), les interprètes de Windows Script Host (WSH) étaient souvent utilisés pour exécuter des scripts malveillants.

Linux

Bien que l'évasion de défense soit la tactique la plus courante observée sous Windows, elle représente 10,67 % de toutes les tactiques dans les environnements Linux.



En décomposant les évacions de défense par techniques sous Linux, nous avons observé que 57,01 % d'entre elles étaient liées à la dégradation de défenses. Les modifications des autorisations au niveau du fichier et du répertoire représentaient 31,03 % et la suppression d'indicateur 3,37 %.

En ce qui concerne le tableau 4, les utilisateurs malveillants ont le plus souvent tenté de désactiver les services iptables et/ou de pare-feu via des outils natifs `ufw` ou `iptables`. Les mineurs de cryptomonnaies et les variantes de botnets suppriment ou ajoutent généralement des règles `iptables` une par une, ce qui déclenche ces alertes plusieurs fois au cours d'une infection.

Dégradation de défenses, Linux	Pourcentage
Tentative de désactivation des tables IPTables ou du pare-feu	59,98 %
Suppression du module noyau	19,71 %
Résiliation du service Elastic Agent	6,24 %
Désactivation potentielle de SELinux	6,21 %
Tentative de désactivation des contrôles de sécurité et de logging de Linux	4,34 %
Tentative de désactivation du service Syslog	3,51 %
Autre	0,02 %

Tableau 4 : techniques de dégradation de défenses sur les points de terminaison Linux

La manipulation des modules noyau Linux était relativement courante, utilisant `modprobe` et/ou `rmmmod` pour supprimer des modules spécifiques

via la ligne de commande. Il était également très courant que les menaces tentent de modifier les autorisations de fichiers dans les répertoires

accessibles en écriture, ce qui représentait 26,74 % de toutes les *évasions de défense*. Plus précisément, les utilisateurs malveillants modifiaient les autorisations de fichiers dans les répertoires courants accessibles en écriture par un utilisateur non racine sous Linux.

Les utilisateurs malveillants tentent souvent de déposer des fichiers ou des charges utiles malveillantes dans un répertoire accessible en écriture et de modifier les autorisations avant l'*exécution*. Les commandes courantes utilisées à cette fin sont `chattr`, `chgrp`, `chmod` et `chown`, qui dirigent vers le répertoire de travail `/dev/shm` ou `/var/tmp`.

rule_name	Pourcentage
File Deletion via Shred	34,16 %
System Log File Deletion	33,07 %
Tampering of Bash Command-Line History	20,43 %
Tampering of Shell Command-Line History	8,98 %
WebServer Access Logs Deleted	3,16 %
Autre	0,20 %

Tableau 5 : suppression d'indicateur par règle sur les points de terminaison Linux

Les chercheurs d'Elastic Security Labs ont observé une *suppression d'indicateur* sur des hôtes Linux qui impliquait la suppression de fichiers, l'altération de l'historique de la ligne de

commande et la suppression des logs d'accès. Les organisations devraient monitorer les événements de suppression de logs, en particulier par des comptes inattendus.

macOS

Sous macOS, l'*évasion de défense* représentait 27,59 % de toutes les tactiques. Ces alertes se répartissent entre plusieurs techniques :

le *chargement de code réflexif* à 34,19 %, le *sabotage des contrôles de confiance* à 12,87 % et la *suppression d'indicateur* qui comprend près de 60 % de l'ensemble des *évasions de défense*.

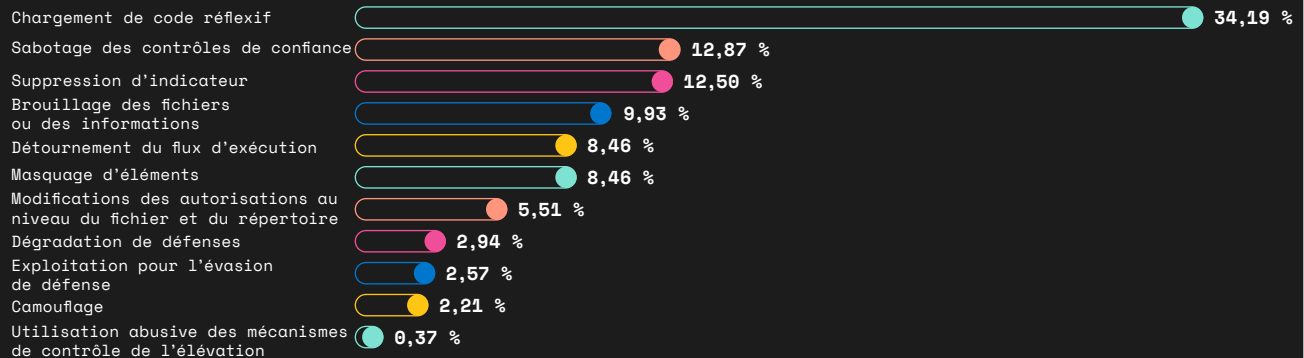


Figure 7 : évacion de défense par technique sur les points de terminaison macOS

Pour aller plus loin, il a été observé que le chargement de code réflexif, en particulier le chargement de bibliothèques dynamiques réfléchies, était utilisé par des menaces avancées pour charger des charges utiles supplémentaires dans des processus précédemment compromis ou malveillants. Cette technique a été observée

lors de la découverte par Elastic Security Labs du malware [KANDYKORN](#), qui a été attribué à l'activité de l'État-nation de la République populaire démocratique de Corée (RPDC) en octobre 2023 et continue d'être une approche furtive pour l'évasion de défense sous macOS.

Exécution

L'exécution, comme prévu, continue d'être une tactique courante dans les stratégies des utilisateurs malveillants via des binaires malveillants et des boîtes à outils. En termes généraux, toutes les techniques organisées dans cette catégorie impliquent des méthodes d'exécution du code de l'utilisateur malveillant, directement ou indirectement. Même lors du déploiement d'un outil d'accès à distance par ailleurs légitime, les menaces emploient des *techniques d'exécution*.

Windows

Bien qu'ayant diminué d'environ 13 % depuis 2023, les *interprètes de script et de commande* restent la technique de la catégorie *Exécution* la plus courante, avec environ 58 % de toutes les exécutions. Windows Management Instrumentation

(WMI) représente environ 24 % : l'importance ici est la montée en puissance de l'utilisation abusive de WMI pour exécuter des commandes et des charges utiles malveillantes, ainsi que de nouvelles techniques qui n'avaient pas été signalées les années précédentes, telles que l'*API native*.

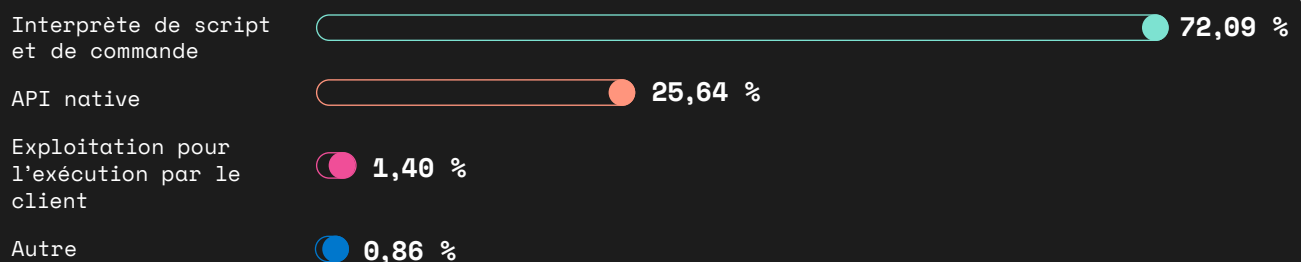


Figure 8 : exécution par technique sur les points de terminaison Windows

Il est important de noter que les tactiques d'exécution affichent une large distribution des règles par rapport aux autres tactiques, ce qui met en évidence les diverses méthodes utilisées par les utilisateurs malveillants pour atteindre leurs objectifs d'exécution. Cela met également en évidence les approches multidimensionnelles employées par les attaquants.

Interprète de script et de commande d'exécution, Windows	Pourcentage
Command and Scripting Interpreter from Suspicious Parent	18,05 %
Execution of a Windows Script with Unusual File Extension	11,27 %
JAVA Application with Unusual File Extension	9,04 %
Empire Stager Execution	7,44 %
Suspicious Windows Script File Name	6,66 %
EggShell Backdoor Execution	5,38 %
Linux Reverse Shell	4,58 %
Suspicious Execution via SQL PowerShell	3,86 %
Linux Reverse Shell via Child	3,20 %
User Discovery Command Execution from Volume Mount	2,76 %
Execution of a Windows Script Downloaded via a LOLBIN	2,53 %
Executable File Extracted to Temporary Directory	2,48 %
Potential Obfuscated Script Execution	2,23 %
Initial Access via OSA Shell Script Piped to Python Interpreter	1,90 %
Suspicious PowerShell Downloads	1,70 %
Suspicious Execution from MSSQL Service	1,66 %
Execution via SyncAppvPublishingServer	1,24 %
Embedded Executable via Windows Shortcut File	1,22 %
Suspicious Oversized Script Execution	1,11 %
Suspicious Image Load via Windows Scripts	1,05 %
Autre	10,63 %

Tableau 6 : alertes de l'interprète de script et de commande par règle sur les points de terminaison Windows

Bien que de nombreux autres résultats de règles comportementales d'Elastic Security soient analysés dans ce rapport, nous nous concentrerons sur les 10 premiers en termes de volume. *Suspicious PowerShell Execution* (Exécution suspecte de PowerShell) se classe au premier rang, représentant 23 % de toute l'activité de *l'interprète de script et de commande*. L'utilisation abusive de PowerShell est une technique bien connue des utilisateurs malveillants, ce n'est donc pas surprenant.

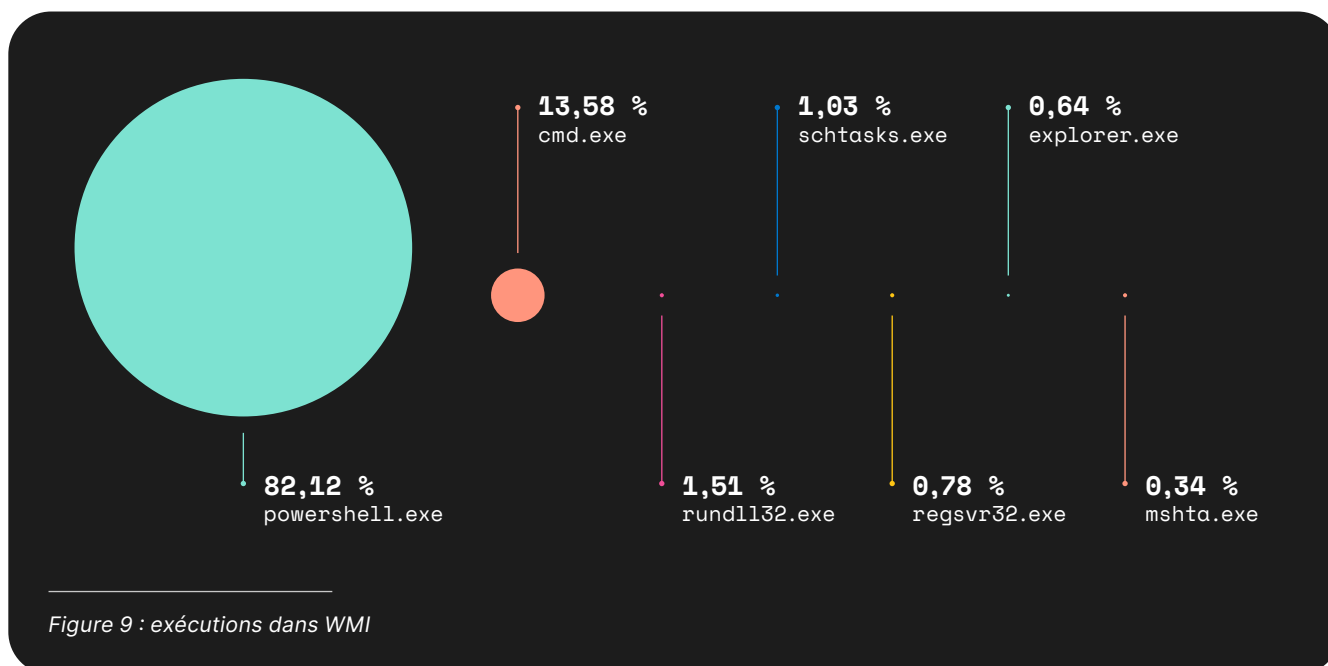
Sur la base de notre analyse de l'exécution de la ligne de commande, les résumés suivants mettent en évidence les principales activités malveillantes (sans ordre particulier) :

- **Collecte de données via WMI** : interrogation de divers espaces de noms et classes liés au clustering, à la virtualisation et aux informations sur le système
 - **Chargement de bibliothèques de liens dynamiques réflexives malveillantes et invocation de méthodes** : chargement de bibliothèques de liens dynamiques en mémoire et invocation de leurs méthodes
 - **Téléchargement et exécution de scripts distants** : utilisation de la cmdlet `Net.WebClient` pour télécharger et exécuter des scripts distants
 - **Techniques de brouillage** : utilisation d'une casse mixte, de caractères spéciaux et d'autres méthodes pour brouiller les commandes
 - **Chargement et exécution de bibliothèques de liens dynamiques en mémoire** : utilisation de `[Reflection.Assembly]::Load([System.IO.File]::ReadAllBytes())` pour charger et exécuter des bibliothèques de liens dynamiques spécifiques directement en mémoire
 - **Shells inversés et communications réseau** : utilisation de sockets TCP pour les shells inversés et autres communications réseau
 - **Tentatives d'escalade des privilèges** : utilisation d'arguments `runas` et de tâches planifiées pour obtenir des privilèges élevés
- **Accès au registre et à la configuration système** : utilisation de la cmdlet `Get-ItemProperty` pour accéder aux paramètres du registre et les manipuler, en ciblant en particulier la ruche `HKEY_LOCAL_MACHINE` (HKLM)

Plus tôt en 2024, Elastic Security Labs a noté un comportement similaire lors de la découverte et de l'analyse du code de [GHOSTENGINE](#) où un script PowerShell a orchestré l'ensemble du flux d'exécution de cette intrusion.

En ce qui concerne l'exécution de fichiers de script Windows écrits par des processus suspects, une part importante de cette activité impliquait l'exécution de `WScript.exe` ciblant des fichiers Visual Basic Scripting Edition (VBScript), généralement stockés dans les répertoires `%AppData%` de l'utilisateur. Cela indique que des malwares basés sur des scripts ou des macros malveillantes tirent parti de VBScript pour s'exécuter. Lorsque Elastic a décrit la découverte de [GrimResource](#), une nouvelle technique d'accès initial et d'évasion de défense, les chercheurs ont fourni un exemple de WSH.

Bien que cela soit rare dans notre ensemble de données, il a également été observé `mshta.exe` ciblant des fichiers HTA (HTML Application). Les fichiers HTA sont souvent utilisés pour exécuter des scripts dans un framework HTML, dont les utilisateurs malveillants abusent souvent à des fins malveillantes. Bien que l'exécution de `mshta.exe` puisse être bénigne dans certaines circonstances, les scripts identifiés dans notre analyse ont été abandonnés par des processus dont le profil était suspect. Ces profils excluaient les activités des processus associés à l'identificateur de sécurité de l'utilisateur Windows (SID) S-1-5-18, aux processus fiables et signés connus et aux emplacements d'exécutables natifs. Ce filtrage permet d'isoler les comportements potentiellement malveillants des activités légitimes.



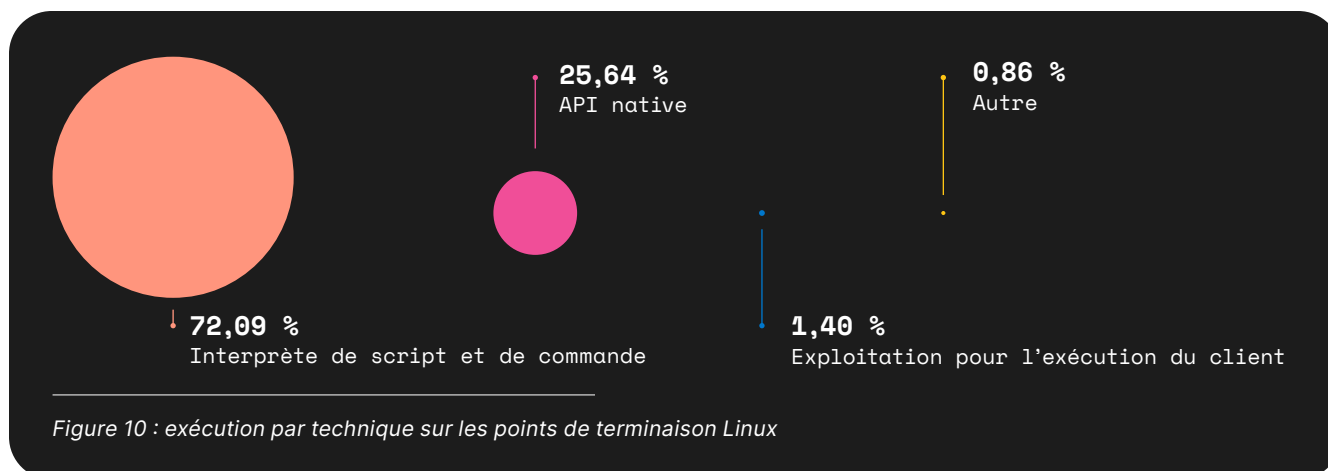
L'utilisation abusive de WMI a augmenté de manière significative, au point qu'elle devrait être à la fois attendue et bien comprise par les équipes de sécurité. Notre analyse des relations entre les processus parent et enfant a révélé que le processus de l'hôte du fournisseur WMI (*WmiPrvSE.exe*) engendre de nombreux processus enfant reconnaissables, tels que PowerShell, CMD, RunDLL32, Tâches planifiées, et bien d'autres, comme le montre la visualisation suivante.

Chacun de ces processus enfant fournit des informations exploitables sur des actions malveillantes spécifiques entreprises via WMI, telles que :

- **Exécution de PowerShell :** des commandes *powershell.exe* ont été observées lors d'actions telles que l'exécution de scripts à partir d'emplacements distants, l'ajout d'exclusions à Windows Defender et l'activation de la communication à distance PowerShell.
- **Exécution de CMD :** les commandes *cmd.exe* observées comprennent l'exécution de scripts PowerShell, le mapping de lecteurs réseau et l'exécution de fichiers en lot.
- **Exécution de RunDLL32 :** *rundll32.exe* a été utilisé pour exécuter des bibliothèques de liens dynamiques, souvent pour charger et exécuter des charges utiles malveillantes, ce qui indique une injection de code et une persistance potentielles.
- **Création de tâches planifiées :** *schtasks.exe* a été utilisé pour créer des tâches planifiées, probablement pour assurer l'exécution récurrente de scripts et/ou de binaires malveillants.
- **Modification des registres :** *regsvr32.exe* a été utilisé pour enregistrer ou annuler l'enregistrement des bibliothèques de liens dynamiques, ce qui peut être exploité pour la persistance.
- **Exécution d'applications HTML :** *mshta.exe* a été utilisé pour exécuter des fichiers HTA, qui peuvent exécuter des scripts dans un framework HTML, souvent exploité pour l'accès initial ou pour exécuter des scripts complexes.
- **Communication réseau :** *curl.exe* et *bitsadmin.exe* ont été utilisés pour télécharger des fichiers ou transférer des données pendant les phases d'exfiltration ou de livraison des charges utiles.

Linux

L'exécution pour Linux est la troisième tactique la plus fréquemment observée et représente près de 14,56 % de l'ensemble des alertes.



Les interprètes de script et de commande représentent 72,09 % de toutes les techniques liées à l'exécution sous Linux, suivis par l'API native à 25,64 %. L'interprète de script et de commande est également la technique la plus utilisée pour l'exécution sous Windows. Cependant, l'API native n'est pas aussi fréquente sous Windows que sur les points de terminaison Linux.

rule_name	Pourcentage
Restricted Shell Breakout via Linux Binary(s)	42,65 %
Interactive Terminal Spawned via Python	20,15 %
Suspicious System Commands Executed by Previously Unknown Executable	9,96 %
Potential Reverse Shell via Suspicious Child Process	7,50 %
Linux Restricted Shell Breakout via Linux Binary(s)	3,92 %

Tableau 7 : alertes de l'interprète de script et de commande par règle sur les points de terminaison Linux

Si l'on analyse les cinq principaux *interprètes de script et de commande* par règle d'alerte, 42,65 % d'entre eux concernent des *tentatives d'intrusion dans des shells restreints via des binaires Linux*, suivies par la *génération de terminaux interactifs via des processus parent Python*. Les intrusions dans des shells restreints se produisent lorsque des utilisateurs malveillants tentent d'utiliser de manière abusive un binaire Linux natif pour

sortir d'un shell ou d'un environnement restreint en générant un shell système interactif. La génération de ces shells à partir d'un binaire n'est généralement pas un comportement courant pour un utilisateur ou un administrateur système et est souvent attribuée à des outils tels que `bash`, `dash`, `ash`, `zsh` et autres, mais peut également être réalisée via `ftp`, `zip`, `tar` et `strace` lorsque les arguments du processus incluent `exec`.

L'utilisation de ce type de binaires "living off the land" (LOLBins) est également utile pour déjouer les détections, en exécutant des commandes par procuration et en modifiant la chaîne d'exécution. Nous avons observé des points de terminaison suspects, tels que `ttty`, générés par Python, souvent attribués à de simples shells inversés et transformés en `ttty` entièrement interactifs après avoir obtenu l'accès *initial* à l'hôte, ce qui souligne l'empressement

à agir de la sorte une fois l'accès obtenu. Ces éléments observables montrent souvent que Python est un processus parent, suivi de processus courants tels que `bash`, `dash`, `ash`, `zsh` et d'autres. Pour ce faire, les utilisateurs malveillants peuvent simplement invoquer l'interprète Python sur le point de terminaison Linux, importer la bibliothèque `pty` et générer un shell interactif à partir de n'importe quel programme shell.

macOS

L'exécution se classe au premier rang avec près de 32,66 % de toutes les tactiques pour macOS.

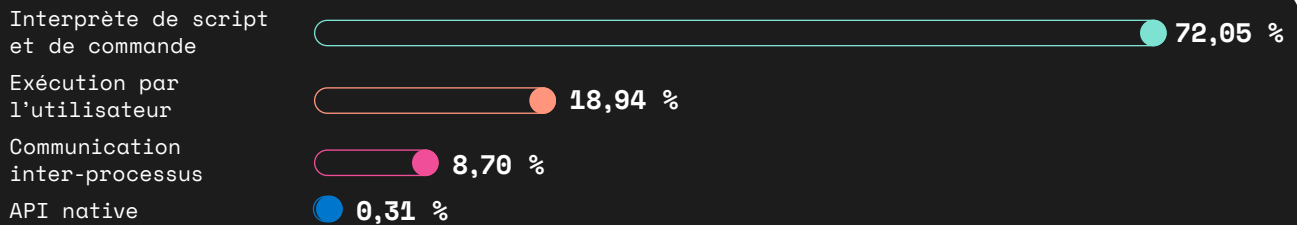


Figure 11 : exécution par technique sur les points de terminaison macOS

Plus précisément, l'interprète de script et de commande représente 72,05 %, suivi de l'exécution par l'utilisateur à 18,94 %. Ensemble, ils représentent près de 91 % de toutes les alertes liées à l'exécution sous macOS.

rule_name	Pourcentage
Suspicious Child Process Execution via Interactive Shell	14,22 %
Suspicious Automator Application Execution	14,22 %
Executable File Extracted to Temporary Directory	7,33 %
Suspicious Nohup Execution	5,60 %
Initial Access via OSA Shell Script Piped to Python Interpreter	5,60 %
Curl Download and Execution of JavaScript Payload	5,17 %
Nohup Execution followed by Outbound Network Connection	4,74 %
User Discovery Command Execution from Volume Mount	3,88 %
PowerShell Outbound Network Connection	3,88 %
PowerShell Encoded Command	3,45 %
Potential Reverse Shell Activity via Terminal	3,45 %

Tableau 8 : interprète de script et de commande par règle sur les points de terminaison macOS

En approfondissant, nous avons observé que *l'exécution suspecte de processus enfant via un shell interactif* était couramment observée, souvent où `bash`, `zsh` et `sh` étaient couramment utilisés comme shell pour ensuite générer des processus `osascript`. Souvent, `osascript` est utilisé de manière abusive par les utilisateurs malveillants pour exécuter du code AppleScript malveillant. De plus, nous avons remarqué un nombre considérable d'*exécutions suspectes d'applications Automator* via XNU Inter-process

Communication (XPC) avec 14,22 % de toutes les alertes de *l'interprète de script et de commande*. Le binaire "Application Stub" sous macOS est associé à Automator, un outil qui permet aux utilisateurs de créer des scripts d'automatisation sans avoir à écrire de code. Les utilisateurs malveillants le ciblent généralement, car il s'agit d'un framework d'automatisation natif sous macOS qui permet non seulement aux utilisateurs malveillants d'exécuter du code malveillant, mais aussi de rester furtifs.

Persistence

Le maintien de l'accès aux environnements des victimes a toujours été une priorité absolue pour les menaces, et ces environnements offrent de nombreuses possibilités grâce aux fonctionnalités propres aux systèmes d'exploitation, aux mauvaises configurations et aux capacités des malwares. Dans cette section, nous décrirons les mécanismes de *persistence* les plus courants que nous avons observés.

Windows

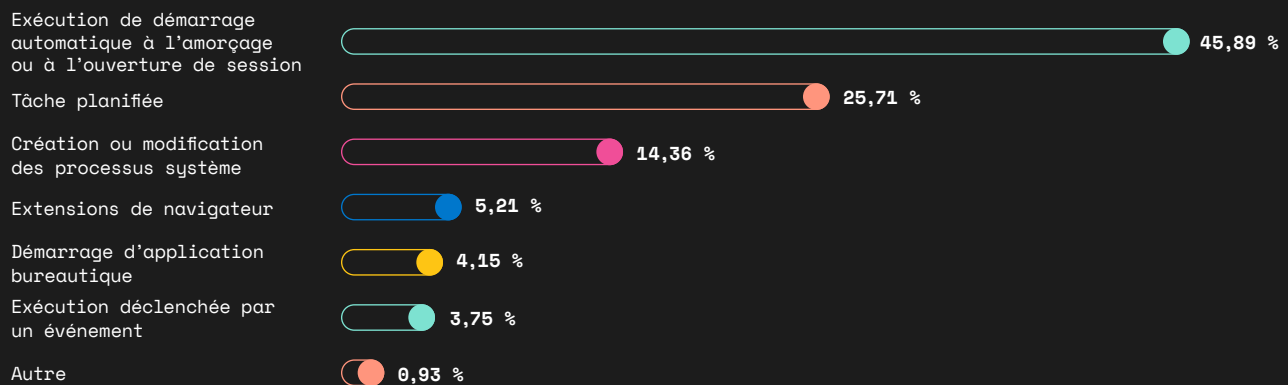


Figure 12 : persistence par technique sur les points de terminaison Windows

Comme la *persistence* reste une priorité absolue, nous continuons à voir des méthodologies de mise en œuvre fortement axées sur *l'exécution de démarrage automatique à l'amorçage* ou à *l'ouverture de session* (avec près de 46 % de

toutes les techniques de *persistence*), suivie des *tâches planifiées* à 26 %, puis de la *modification des processus système* (14 %). Notez que la *persistence*, dans ces cas, dépend fortement des distributions Windows.

Cette année, nous avons également constaté un changement dans la popularité de certaines techniques de *persistance*, avec l'échange des *tâches planifiées* et de l'*exécution de démarrage automatique à l'amorçage ou à l'ouverture de session*. L'*exécution de démarrage automatique à l'amorçage ou à l'ouverture de session* a connu

une augmentation de 29 % de son utilisation, ce qui souligne sa préférence croissante parmi les utilisateurs malveillants. Lorsque nous examinons les détections spécifiques des mécanismes de *persistance* impliquant l'*exécution de démarrage automatique à l'amorçage ou à l'ouverture de session*, nous constatons une grande variété sans qu'il n'y ait de modèle de comportement dominant.

rule_name	Pourcentage
Startup Persistence via Windows Script Interpreter	15,69 %
Unusual File Written or Modified in Startup Folder	12,60 %
Suspicious String Value Written to Registry Run Key	12,07 %
Startup Persistence from a Browser or Compression Utility Descendant	8,83 %
Registry Run Key Modified by Unusual Process	6,18 %
Suspicious Shortcut Modification	6,03 %
Suspicious Launch Service Property List File Creation	5,89 %
Persistence via a Process from a Removable or Mounted ISO Device	5,46 %
Uncommon Persistence via Registry Modification	4,27 %

Tableau 9 : exécution de démarrage automatique à l'amorçage ou à l'ouverture de session par règle pour les points de terminaison Windows

La règle *Startup Persistence via Windows Script Interpreter* (Persistance au démarrage via l'interprète de scripts Windows) représente le pourcentage le plus élevé avec 15,69 %, ce qui indique une utilisation répandue d'interprètes de script tels que PowerShell et *mshta.exe* par des utilisateurs malveillants pour maintenir la *persistance*. De plus, l'utilisation abusive de *reg.exe* a été fréquemment constatée dans ces cas. En règle générale, des types de fichiers de script complexes tels que VBS, LNK, PS, HTA et parfois des fichiers EXE sont identifiés lors de ces détections. Ces scripts deviennent des outils polyvalents permettant aux utilisateurs malveillants d'atteindre la *persistance* avec un minimum d'effort. Une part importante de ces détections impliquait la modification directe des ruches des registres *HKEY_CURRENT_USER* (HKCU) et *HKLM* pour établir la *persistance* avec des scripts. Les utilisateurs

malveillants exploitent ces emplacements de registre pour s'assurer que les charges utiles malveillantes s'exécutent lors de l'amorçage du système ou de l'ouverture de session de l'utilisateur. L'analyse souligne l'importance de monitorer et de sécuriser les emplacements de démarrage et les clés des registres pour empêcher les mécanismes de *persistance* non autorisés. En ce qui concerne la règle *Unusual File Written or Modified in Startup Folder* (Fichier inhabituel écrit ou modifié dans le dossier de démarrage), Elastic Security Labs a observé différents types de fichiers, notamment des bibliothèques de liens dynamiques (DLL), LNK, EXE, TXT, HTA et des scripts PowerShell écrits dans le dossier de démarrage par LOLBins. Cette activité met en évidence la façon dont les utilisateurs malveillants exploitent des outils système légitimes pour établir la *persistance*.

rule_name	Pourcentage
Scheduled Task Creation by an Unusual Process	25,69 %
Suspicious Windows Schedule Child Process	21,51 %
Scheduled Task Creation via Unsigned Parent	20,14 %
Suspicious Scheduled Task Creation	14,63 %
Scheduled Task from a Removable or Mounted ISO Device	5,32 %
Scheduled Task from a Browser or Compression Utility Descendant	3,87 %
Scheduled Task by a Low Reputation Process	3,44 %
Scheduled Task Creation from Suspicious Parent	3,25 %

Tableau 10 : tâche planifiée par règle pour les points de terminaison Windows

Lorsque nous analysons les mécanismes de *persistance* impliquant des tâches planifiées par règle, nous observons une distribution significative entre plusieurs règles. Les règles *Scheduled Task Creation* (Création de tâches planifiées) par un *Unusual Process*, *Suspicious Scheduled Child Process* (Processus inhabituel, processus enfant suspect planifié) et *Scheduled Task Creation via Unsigned Parent* (Création de tâches planifiées via un parent non signé) représentent respectivement 26 %, 22 % et 20 % des détections. Cette distribution indique que la logique de détection se concentre efficacement sur les relations entre les processus parent et enfant ainsi que sur les signatures des processus concernés.

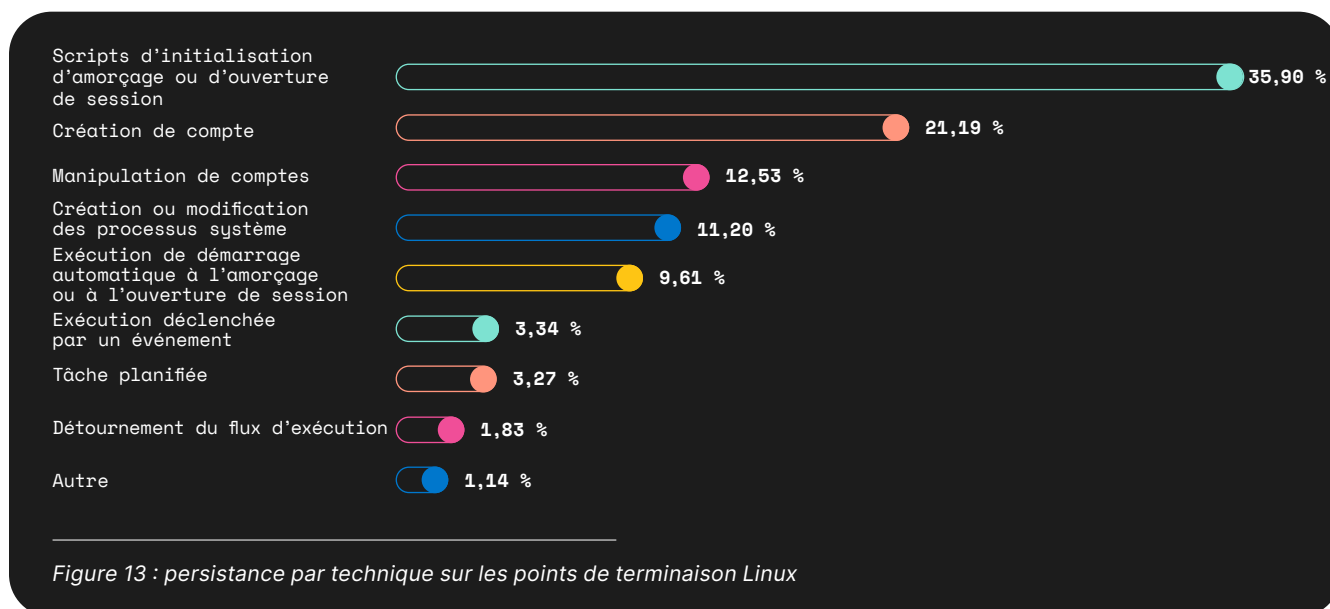
Les utilisateurs malveillants utilisent souvent WScript, MSHTA, RunDLL32, WMIC et CScript pour générer *svchost*. Ces processus parent peuvent être utilisés pour créer ou modifier des tâches planifiées qui dirigent vers des exécutables situés dans des répertoires couramment utilisés de manière abusive comme `%AppData%\Local\Temp`, `%Users%\Public` et `%Windows%\Microsoft.NET`. Ces répertoires

sont fréquemment utilisés par les utilisateurs malveillants, car ils sont souvent négligés et constituent un emplacement pratique pour stocker des charges utiles malveillantes. En créant des tâches planifiées qui dirigent vers ces exécutables, les utilisateurs malveillants s'assurent que leur code malveillant est exécuté à des intervalles spécifiés ou lors d'événements système, maintenant ainsi la *persistance* sur le système compromis. Cette méthode est particulièrement efficace, car elle exploite les fonctionnalités légitimes de Windows pour exécuter un code malveillant, ce qui la rend plus difficile à détecter et à corriger.

La grande fidélité de la logique de détection dans l'identification de relations entre les processus parent-enfant inhabituels et de processus non signés souligne l'importance du suivi des tâches planifiées et de leurs processus associés. Un comportement similaire a été mis en évidence par Elastic Security Labs dans son analyse de [LATRODUCTUS](#). Cette analyse souligne la nécessité de stratégies de suivi et de défense robustes pour identifier et neutraliser efficacement de telles menaces.

Linux

Bien que la *persistance* soit un objectif commun à toutes les campagnes et stratégies des utilisateurs malveillants, il s'agit de la première tactique Linux, avec 24,26 % des alertes.



Nous avons remarqué que *les scripts d'initialisation d'amorçage ou d'ouverture de session, la création de compte et la manipulation de comptes* étaient souvent les techniques les plus utilisées, représentant collectivement plus de 36 % de tous les mécanismes de *persistance*. Ensuite, il existe une distribution presque équivalente pour la modification des processus système et les exécutions déclenchées par des événements.

rule_name	Pourcentage
Suspicious File Creation in /etc for Persistence	54,93 %
Suspicious Process Spawned from MOTD Detected	21,57 %
Chkconfig Service Add	15,47 %
Potential Persistence Through Run Control Detected	2,77 %

Tableau 11 : scripts d'initialisation d'amorçage ou d'ouverture de session par règle sur les points de terminaison Linux

Le répertoire */etc/* est une cible courante des mécanismes de *persistance* de Linux, car il contient des fichiers de configuration et des scripts système stratégiques, tels que :

- */etc/rc.local* pour les commandes de démarrage
- */etc/update-motd.d/* pour les scripts du message du jour

- [/etc/sudoers](#) pour les configurations des utilisateurs privilégiés
- [/etc/profile](#) pour les paramètres d'environnement shell
- [/etc/systemd](#) pour la gestion des services
- [/etc/cron](#) pour les tâches planifiées et la configuration de l'éditeur de liens dynamiques

Tous ces éléments peuvent être manipulés pour maintenir un accès non autorisé ou exécuter un code malveillant au démarrage du système ou lors d'événements spécifiques.

rule_name	SOMME
Linux Group Creation	46,70 %
Linux User Account Creation	46,56 %
Linux User Added to Privileged Group	6,29 %
Autre	0,45 %

Tableau 12 : création de compte sur les points de terminaison Linux

Comme le montre le tableau 13, la création d'utilisateurs et de groupes Linux a souvent été réalisée par des utilisateurs malveillants ayant une distribution similaire, ce qui est normal étant donné que les créations d'utilisateurs et de groupes se font en parallèle.

rule_name	Pourcentage
New Systemd Service Created by Previously Unknown Process	43,15 %
Modification of Standard Authentication Module or Configuration	34,50 %
Potential Execution via XZBackdoor	12,17 %
Modification of OpenSSH Binaries	8,69 %
Systemd Service Created	1,37 %
Autre	0,11 %

Tableau 13 : création ou modification des processus système par règle sur les points de terminaison Linux

La création ou la modification des processus système représentait également près de 11,20 % de l'ensemble des *persistances* sur les points de terminaison Linux. Bien qu'il ne s'agisse pas d'une grande distribution, l'activité spécifique observée est assez importante à l'analyse. Plus précisément, 43,15 % de toutes les créations de processus suspects signalées comme étant liées au service [systemd](#) ont été créées par un processus inconnu. Une grande partie était liée à la création ou

au changement de nom de nouveaux fichiers [systemd](#) dans des emplacements de service communs pour les utilisateurs root et réguliers. C'est souvent le cas des utilisateurs malveillants, car ils peuvent exploiter les fichiers du service [systemd](#) afin d'obtenir la *persistance* en créant ou en modifiant des services pour exécuter des commandes ou des charges utiles malveillantes lors du démarrage du système ou à des intervalles prédéfinis via un minuteur [systemd](#).

rule_name	Pourcentage
Tainted Kernel Module Load	29,02 %
Tainted Out-Of-Tree Kernel Module Load	27,76 %
Kernel Module Load via insmod	20,58 %
Persistence via KDE AutoStart Script or Desktop File Modification	13,96 %

Tableau 14 : démarrage automatique à l'amorçage ou à l'ouverture de session par règle sur les points de terminaison Linux

Le terme "tainted kernel module" (module noyau corrompu) est défini comme un noyau Linux qui est dans un état non pris en charge, car son fonctionnement ne peut pas être garanti, souvent parce que le noyau contient des modules non signés, non standard (out-of-tree) ou d'autres types de modules. Ces modules sont similaires aux bibliothèques de liens dynamiques non signées de Windows, qui sont généralement chargées par l'intermédiaire de l'exécution de proxy binaire du système via des processus natifs, tels que RunDLL32.

Ensemble, les modules noyau corrompus ou chargés de manière suspecte représentent près de 76 % de toutes les alertes observées de démarrage automatique à l'amorçage ou à l'ouverture de session, ce qui est significatif, car les rootkits exploitent souvent ces modules noyau pour la *persistance* et l'*évasion de défense*. Les utilisateurs malveillants accomplissent souvent cela à l'aide de rootkits de modules noyau chargeables (LKM), où les modules sont ajoutés en tant qu'extension pour le noyau, mais ne contiennent pas de signatures valides ou n'appartiennent pas à l'arborescence standard du noyau.

macOS

Les daemons et les agents de lancement sont les mécanismes de *persistance* les plus populaires sous macOS. Comme indiqué ci-dessous, les *scripts d'initialisation d'ouverture de session* représentent 45,45 % de l'ensemble des *persistances* sous macOS, suivis des extensions de navigateur à 22,73 %.

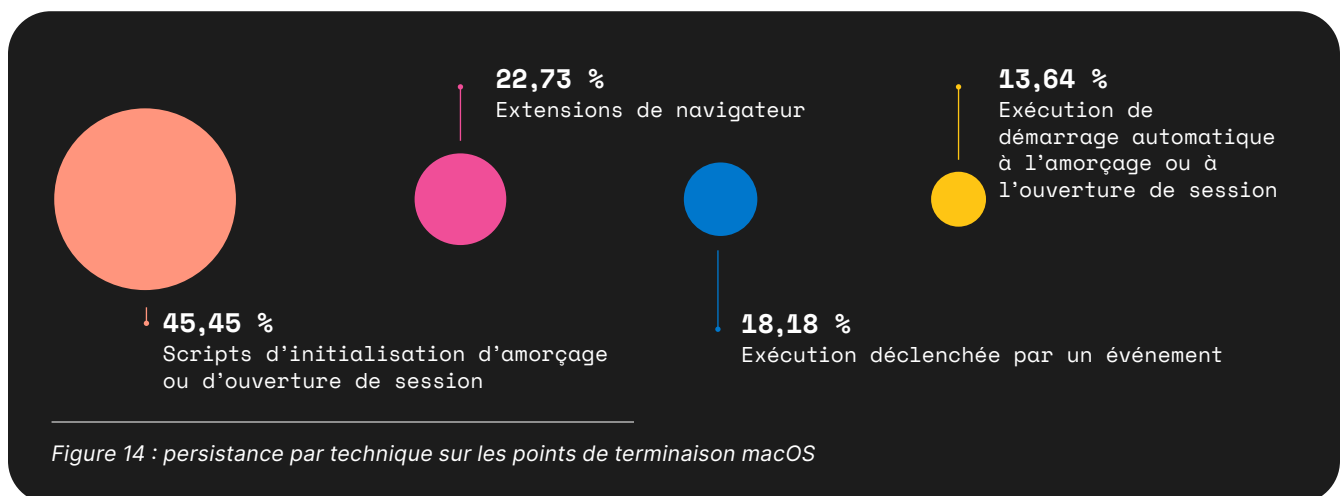


Figure 14 : persistance par technique sur les points de terminaison macOS

Près de 60 % de toutes les alertes liées à la *persistance* sont directement liées à des fichiers suspects de liste de propriétés (plist), qui sont recherchés par [launchd](#). Ceux-ci sont ensuite lancés à la demande à partir de ces fichiers plist.

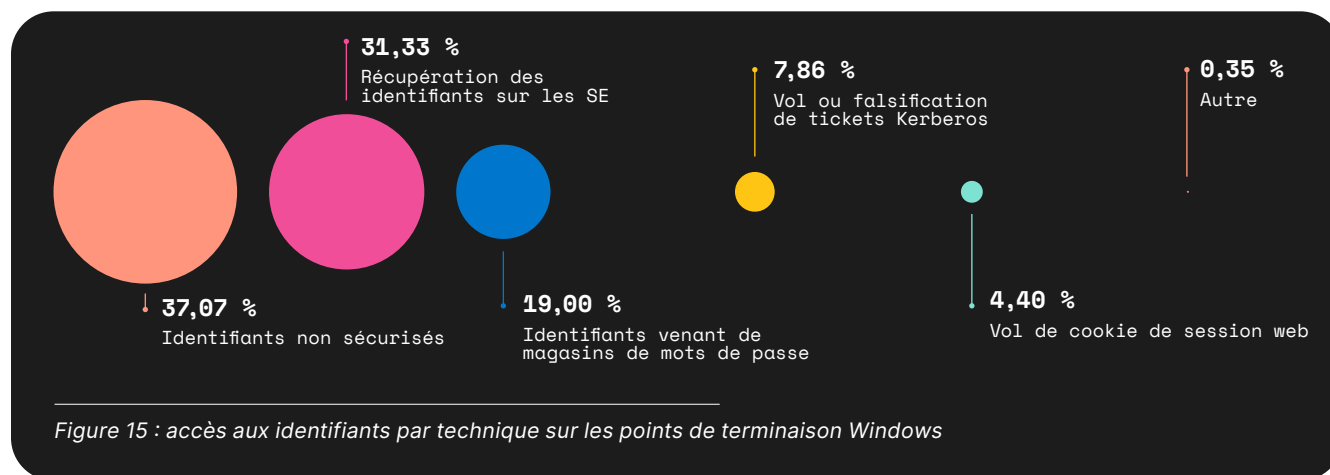
rule_name	Pourcentage
Suspicious StartupItem plist Creation or Modification	45,45 %
Manual Loading of a Suspicious Chromium Extension	22,73 %
Initial Access Staging via Installer Package	9,09 %
Persistence via a Masqueraded plist Filename	6,06 %
Persistence via a Hidden plist Filename	4,55 %
Untrusted or Unsigned Binary Executed via Launch Service	3,03 %
Suspicious File Creation via Pkg Install Script	3,03 %
Suspicious Property List File Creation or Modification	1,52 %
Suspicious Apple Mail Rule plist Creation or Modification	1,52 %
Potential Persistence via Emond	1,52 %

Tableau 15 : alertes de plist par règle sur les points de terminaison macOS

Accès aux identifiants

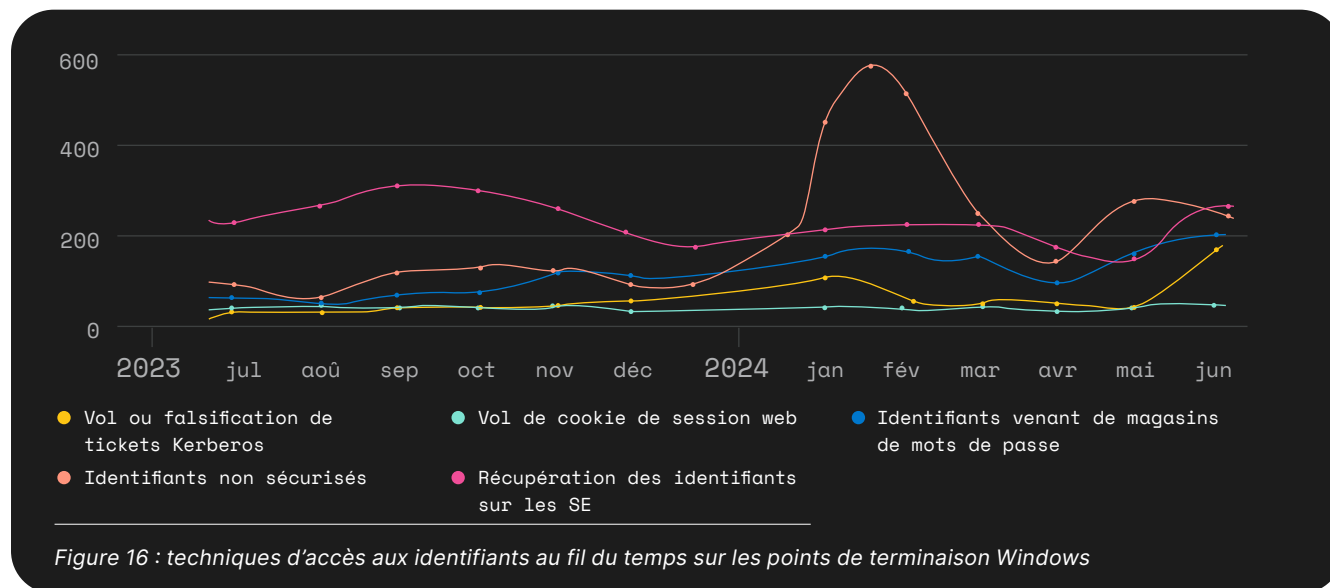
Elastic Security Labs a observé une tendance significative en matière de vol d'informations menant à l'*accès aux identifiants*, les identifiants volés étant souvent vendus ou utilisés par d'autres utilisateurs malveillants dans des campagnes ultérieures.

Windows



Cette activité a contribué à de nombreuses violations publiques récentes, où les attaquants ont utilisé des identifiants volés pour se connecter à des comptes valides, à la fois locaux et basés sur le cloud, afin de poursuivre leur intrusion.

Bien que l'accès aux identifiants ne représente qu'environ 9 % de l'ensemble des détections comportementales, il est essentiel de comprendre les techniques et les méthodologies employées par les utilisateurs malveillants.



Les identifiants non sécurisés représentent près de 37 % de toutes les techniques d'accès aux identifiants, soit une augmentation notable de près de 31 % par rapport à l'année dernière. Cela indique une préférence croissante des utilisateurs malveillants pour l'exploitation des identifiants non sécurisés. La récupération des identifiants sur les SE, généralement associée à l'extraction

des identifiants à partir de régions de mémoire protégées de processus spécifiques sous Windows, a diminué à 35 % de l'accès aux identifiants, mais reste importante. De plus, le ciblage des identifiants venant de magasins de mots de passe a connu une augmentation de 4 % par rapport à l'année dernière, ce qui souligne sa popularité continue parmi les utilisateurs malveillants.

Les lecteurs doivent être conscients de l'existence de vastes réseaux de brokers d'accès, des personnes ou des organisations qui monétisent les identifiants volés et vendus à des écosystèmes criminels et d'espionnage, conduisant à toutes sortes de vols, du vol d'identité au vol de propriété intellectuelle. Cependant, il peut s'avérer extrêmement difficile d'établir un lien concluant entre une activité d'intrusion et des identifiants volés ou exposés.

Alors que les entreprises exploitent de plus en plus les pipelines d'intégration et de livraison continues (CI/CD), les environnements cloud hybrides et les solutions logicielles en tant que service (SaaS), le potentiel d'exploitation des identifiants non sécurisés ne fait que croître.

Il est probable que les utilisateurs malveillants se concentrent sur ces identifiants abondants et souvent mal sécurisés, ce qui souligne la nécessité de mesures de sécurité robustes pour protéger les informations sensibles dans divers environnements.

rule_name	Pourcentage
Access to Browser Credentials from Suspicious Memory	49,43 %
AutoLogons Access Attempt via Registry	16,21 %
Sensitive File Access - SSH Saved Keys	11,63 %
Failed Attempts to Access Sensitive Files	8,62 %
Failed Access Attempt to Web Browser Files	7,00 %
Autre	7,10 %

Tableau 16 : identifiants non sécurisés par règle sur les points de terminaison Windows

Il est important de noter que les utilisateurs malveillants ciblent les identifiants non sécurisés via des outils, des efforts manuels et des malwares. Les identifiants du navigateur en mémoire représentent 49,43 % de toutes les tentatives d'accès aux identifiants non sécurisés. La logique de détection comportementale d'Elastic Security est conçue pour identifier les tentatives d'accès aux identifiants stockés dans le navigateur web à partir de processus présentant des propriétés de mémoire suspectes. En suivant les processus qui accèdent à des fichiers spécifiques tels que les données de connexion,

les bases de données [logins.json](#), [cert.db](#), [key.db](#) et SQLite pour les connexions et les cookies provenant de régions de mémoire inhabituelles, Elastic Security capture le comportement de l'utilisateur malveillant lié aux identifiants non sécurisés qui peuvent échapper aux mécanismes de suivi strictement basés sur les fichiers. Elastic Security Labs a constaté un comportement similaire dans le cadre de ses recherches sur les [voleurs distribués à l'échelle mondiale](#), en particulier avec des familles telles que REDLINE Stealer.

rule_name	Pourcentage
Credential Access via Known Utilities	23,15 %
LSASS Memory Dump via MiniDumpWriteDump	16,73 %
Suspicious Access to LSA Secrets Registry	12,24 %
LSASS Access Attempt from Unbacked Memory	10,61 %
Suspicious Registry Hive Dump	9,50 %
Security Account Manager (SAM) File Access	7,58 %
Security Account Manager (SAM) Registry Access	7,41 %
Potential Credential Access via Mimikatz	4,55 %
LSASS Access Attempt from an Unsigned Executable	3,44 %
Autre	4,78 %

Tableau 17 : récupération des identifiants sur les SE par règle sur les points de terminaison Windows

Credential Access via Known Utilities (Accès aux identifiants via des utilitaires connus) représentait 23 % de l'ensemble des *récupérations des identifiants sur les SE*, principalement pour les systèmes Windows. Cette logique est conçue pour identifier l'exécution d'utilitaires Windows connus fréquemment utilisés par les utilisateurs malveillants pour récupérer la mémoire du service LSASS (Local Security Authority Subsystem Service) ou la base de données Active Directory (*NTDS.dit*). La règle se concentre sur la détection des utilitaires tels que *procdump*, *esentutl.exe*, *diskshadow.exe*, *rundll32.exe* et *reg.exe*, qui sont souvent utilisés dans les activités de récupération d'identifiants. Ces outils, lorsqu'ils sont exécutés avec des arguments spécifiques, peuvent créer des récupérations de mémoire ou exporter des ruches de registres contenant des informations d'identification sensibles, ce qui en fait des cibles de choix pour

les acteurs malveillants cherchant à réaffecter des privilèges ou à pivoter au sein d'un réseau. L'analyse des données d'exécution des processus révèle des schémas et des techniques communs utilisés par les utilisateurs malveillants. Par exemple, *procdump64.exe* est fréquemment observé en train de créer des récupérations du processus *lsass.exe*, qui est une méthode typique pour extraire des hachages de mots de passe et d'autres informations d'identification stockées dans la mémoire. De même, les commandes *reg.exe* sont utilisées pour enregistrer des ruches de registres critiques telles que *HKLM\SAM*, *HKLM\SYSTEM* et *HKLM\SECURITY*, qui peuvent être exploitées pour récupérer les identifiants stockés. L'exécution de *rundll32.exe* avec *comsvcs.dll* pour créer des mini-récupérations et l'utilisation de *esentutl.exe* pour copier le fichier *NTDS.dit* mettent en évidence les diverses stratégies employées par les attaquants pour accéder au stockage des identifiants.

L'outil d'accès aux identifiants le plus couramment observé dans ces détections est *powershell.exe*, qui a été identifié à plusieurs reprises. PowerShell est souvent utilisé à mauvais escient par les attaquants en raison de ses puissantes fonctionnalités de script et de son intégration profonde avec Windows, ce qui en fait un outil idéal pour accéder et manipuler les ressources système, y compris le coffre-fort d'identifiants. D'autres processus tels que *mscorsvw.exe*, *notepad.exe* et *rundll32.exe* ont également été identifiés en train de charger *vaultcli.dll*, ce qui suggère que les utilisateurs malveillants exploitent ces processus pour effectuer le vol d'identifiants. En utilisant ces processus, les attaquants peuvent combiner leurs activités malveillantes avec des opérations système légitimes, réduisant ainsi la probabilité de détection.

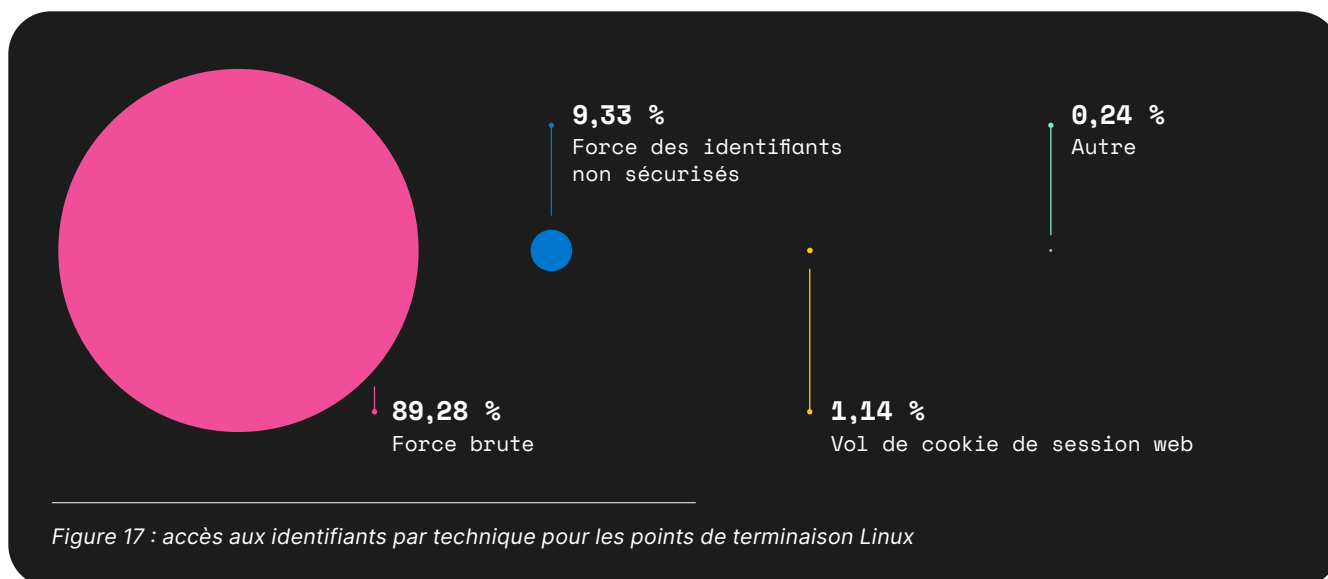
Les processus ciblés accèdent généralement à *vaultcli.dll* à partir d'emplacements inhabituels ou avec des arguments inattendus, ce qui indique un comportement suspect. Par exemple, l'utilisation de *rundll32.exe* avec des arguments spécifiques ciblant les répertoires AppData de l'utilisateur, ou de *powershell.exe* avec des commandes chiffrées, suggère des tentatives de dissimuler des intentions malveillantes et d'échapper aux contrôles de sécurité. En outre, l'inclusion d'autres processus tels que *mshta.exe*, *cvtres.exe* et divers exécutables *.NET* indique une stratégie plus large consistant à utiliser un ensemble varié d'outils pour atteindre leurs objectifs.

Les utilisateurs malveillants exploitent ces méthodes pour extraire des identifiants du gestionnaire d'informations d'identification de Windows, ce qui leur permet de réaffecter des privilèges, de se déplacer latéralement sur le réseau et d'obtenir un accès non autorisé à des systèmes et à des données sensibles. En suivant ces activités de processus inhabituelles et le chargement de *vaultcli.dll*, les solutions de sécurité peuvent identifier et déjouer ces tentatives, protégeant ainsi l'intégrité des informations d'identification des utilisateurs et maintenant la sécurité de l'environnement dans son ensemble.

Linux

Lors de l'analyse de l'accès aux identifiants pour Linux, il est important de se rappeler que le stockage des identifiants est différent d'une plateforme à l'autre. Souvent, les organisations dont les utilisateurs se trouvent derrière des points de terminaison s'appuient sur des solutions IAM (gestion de l'accès aux identités)

ou des fournisseurs d'identité de services tiers tels qu'Okta et Entra ID pour gérer l'authentification ainsi que le stockage et la récupération des mots de passe. Cependant, sous Linux, l'authentification avec les utilisateurs et les groupes s'étend à des services tels que SSH où l'authentification est basée sur des clés privées et publiques.



89,28 % de tous les signaux d'accès aux identifiants sont liés à la force brute, avec seulement une petite quantité liée aux identifiants non sécurisés, avec 9,33 % respectivement.

rule_name	Pourcentage
Potential Internal Linux SSH Brute Force Detected	50,03 %
Potential Linux SSH Brute Force Detected	20,90 %
Potential External Linux SSH Brute Force Detected	18,24 %
Potential Successful SSH Brute Force Attack	4,44 %
Potential SSH Password Guessing	4,10 %
Potential Linux Local Account Brute Force Detected	2,29 %

Tableau 18 : force brute par règle pour les points de terminaison Linux

La force brute, bien qu'il ne s'agisse pas de l'attaque la plus complexe, s'appuie souvent sur différentes sous-techniques, telles que la pulvérisation de mots de passe et le bourrage d'identifiants, qui sont plus répandues que jamais pour les utilisateurs malveillants au moment de la rédaction de ce rapport. Dans près de 97 % de toutes les alertes de force brute, le principal

coupable était des échecs de connexion consécutifs ciblant des comptes d'utilisateurs à partir de la même adresse source externe dans des internes de courte durée. Cela suggère également que ces points de terminaison Linux étaient également destinés au public, alors que les connexions capturées étaient généralement basées sur SSH.

macOS

Les chercheurs ont identifié que *les identifiants venant de magasins de mots de passe, les identifiants non sécurisés, le vol de cookies de session web et la capture d'entrées* étaient les techniques les plus courantes, avec 31,35 %, 30,33 %, 22,13 % et 13,93 % respectivement. Par rapport à d'autres systèmes d'exploitation, la capture d'entrées est une anomalie et est

unique à macOS en raison de l'utilisation abusive d'osascript par des utilisateurs malveillants. Il convient également de noter que, quelle que soit la technique ou la règle, les cibles les plus courantes des utilisateurs malveillants sont souvent les trousseaux d'accès, les portefeuilles de cryptomonnaies, les navigateurs web et la capture d'entrées des utilisateurs.

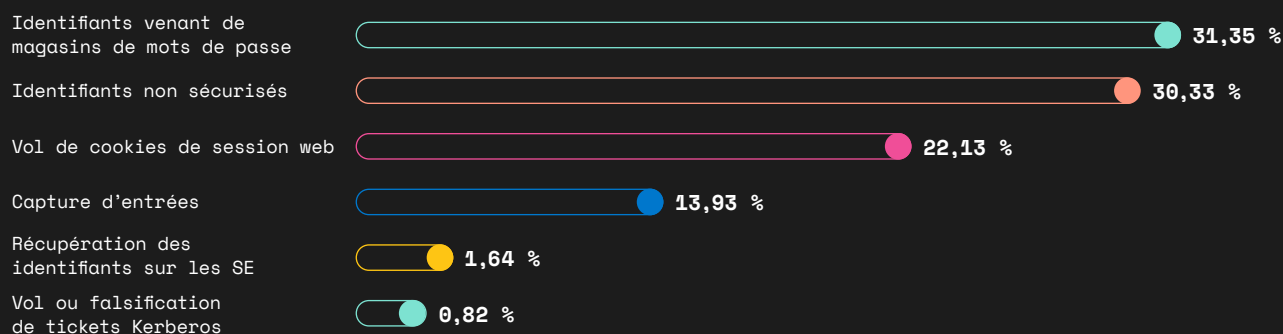


Figure 18 : accès aux identifiants par technique pour les points de terminaison macOS

Plus que jamais, les voleurs d'informations sont devenus un outil populaire dans l'arsenal d'un utilisateur malveillant lorsqu'il s'agit de cibler des points de terminaison macOS potentiels, en particulier pour les tentatives d'accès aux *identifiants* contre les plateformes SaaS et autres applications hébergées dans le cloud.

Sécurité du cloud

Peu d'organisations opèrent totalement en dehors des environnements hébergés dans le cloud, étendant ainsi leur surface d'attaque des ressources autogérées à "l'ordinateur de quelqu'un d'autre" dans le cloud. Les clients d'Elastic ont volontairement fourni la télémétrie des alertes utilisée dans cette section, aidant les chercheurs à découvrir de nouvelles menaces et des fonctions d'ingénierie pour améliorer les fonctionnalités de sécurité. Ces alertes sont générées sur la base de règles de détection prêtes à l'emploi, qui utilisent les données des intégrations Elastic spécifiques à chaque fournisseur de services cloud.

Il est important de noter que la nature de la détection d'activités potentiellement malveillantes au sein des fournisseurs de services cloud, en particulier lorsqu'il s'agit de comptes valides et

d'activités légitimes, fait que ces alertes sont souvent moins fidèles que celles provenant des systèmes EDR. Nous traitons ces alertes davantage comme des signaux potentiels d'activité malveillante que comme des preuves confirmées de menaces, et nous soulignons cette distinction pour les lecteurs qui pourraient être enclins à tirer des conclusions plus définitives. Cette année, Elastic Security Labs a regroupé Microsoft 365 avec les données de Microsoft Azure et Google Workspace avec les données de Google Cloud plutôt que de les séparer dans une catégorie SaaS. Comme les entités et les services sont étroitement liés, utilisant souvent les mêmes API et ressources, nous pensons que cela offre une meilleure vision globale de chaque fournisseur.

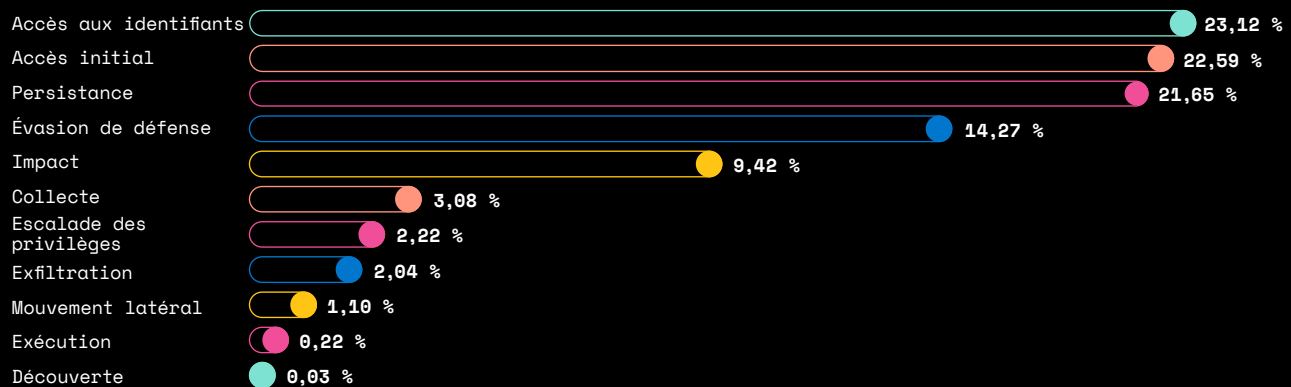
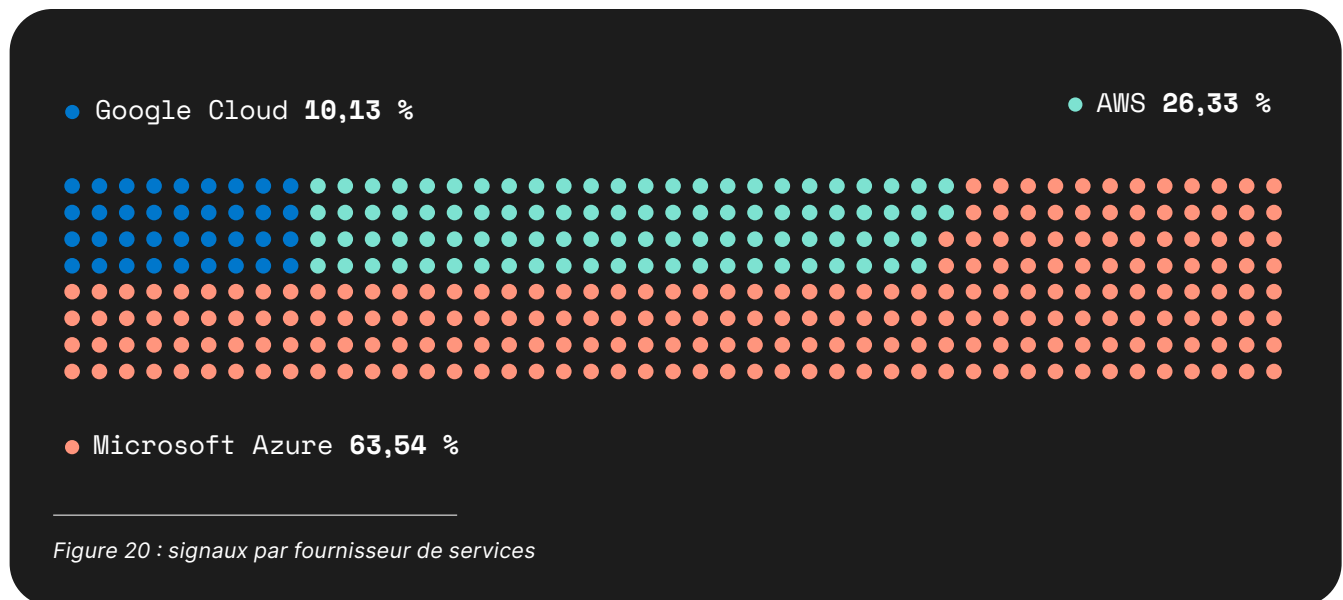


Figure 19 : tactiques MITRE ATT&CK observées dans les environnements cloud

Dans l'ensemble, l'accès aux identifiants représente un peu plus de 23 % de toutes les activités, suivi de l'accès initial, de l'impact et de l'évasion de défense, qui représentent respectivement 22 %, 21 % et 14 %. Au cœur

de la sécurité du cloud se trouve IAM, la technologie qui façonne les tentatives d'accès aux identifiants. Nous nous attendons à ce que les techniques de cette catégorie représentent la plus grande proportion des comportements que nous observons et qui ciblent les plateformes cloud.

Distribution par fournisseur de services cloud



Dans notre analyse de la distribution des signaux par fournisseur de services cloud, nous avons constaté que Microsoft Azure était l'environnement le plus courant pour les signaux anormaux, représentant 64 % du total. Cela marque un changement par rapport aux années précédentes, où AWS comptait le plus grand nombre de signaux. La combinaison des données de Microsoft 365, qui comprennent les tentatives d'accès aux identifiants et de *phishing*, avec celles de Microsoft Azure est à l'origine de ce changement. Nous déconseillons aux lecteurs de conclure que cela reflète une quelconque préférence en matière de ciblage ou une tendance en matière de menaces. Notamment, Microsoft Azure inclut Entra ID, la solution IAM par défaut de Microsoft. Bien qu'AWS

détienne la [plus grande part de marché](#) parmi les fournisseurs de services cloud, les sources de données de Microsoft ont fourni le plus grand nombre d'événements. Avec la popularité des déploiements hybrides, l'adoption d'Entra ID par rapport aux fournisseurs d'identité tiers devient de plus en plus courante. Google Cloud, ainsi que Google Workspace, ne représentent qu'environ 10 % de tous les signaux émis par les fournisseurs de services cloud.

Dans les sous-sections suivantes, nous fournirons des détails par fournisseur de services cloud pour les plateformes Microsoft, Amazon et Google. La dernière section comprendra un aperçu de la posture du cloud basée sur les références du [Center for Internet Security \(CIS\)](#).

Microsoft Azure

Microsoft Azure a évolué au-delà de l'infrastructure en tant que service (IaaS) Windows pour inclure de solides capacités de plateforme en tant que service (PaaS), l'hébergement web et une variété de fonctionnalités de gestion des identités. Entra ID est la capacité intégrée de gestion des identités de Microsoft. Les comptes Microsoft Azure présentent

souvent un grand intérêt pour les utilisateurs malveillants qui peuvent vouloir se déplacer latéralement vers des points de terminaison physiques ou des messageries d'employés dans Office 365 pour poursuivre leurs intrusions ou réaliser des actions en vue de leurs objectifs.

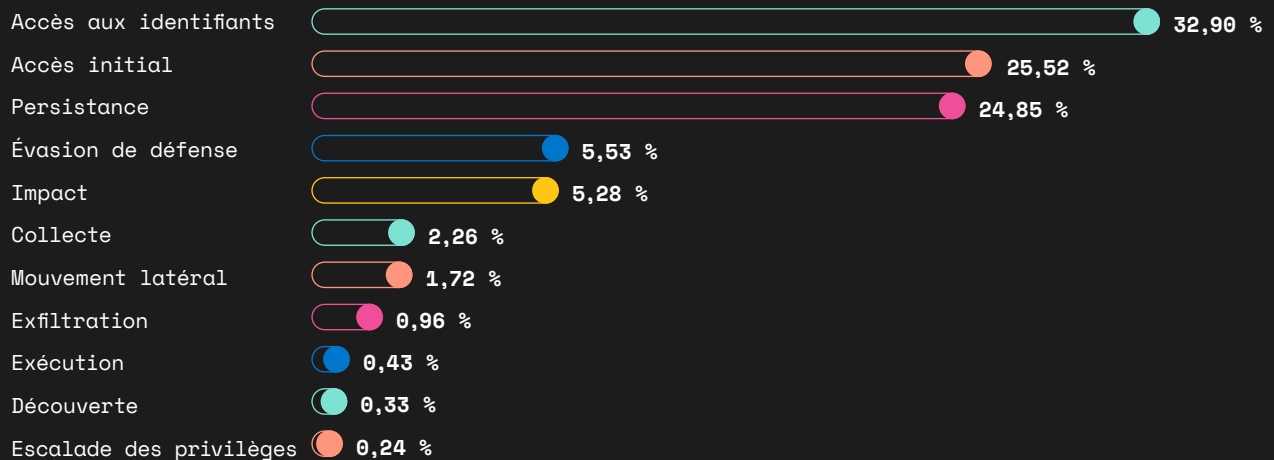


Figure 21 : signaux de Microsoft Azure par tactique

Accès aux identifiants

L'accès aux identifiants représente environ 32,90 % des signaux de Microsoft Azure, soit une augmentation de plus de 26 % par rapport à l'année dernière, et est souvent réalisé par des malwares de vol d'informations et des portails frauduleux qui se font passer pour des sites légitimes. De vastes économies existent pour monétiser les identifiants volés en menaces de toutes sortes, ce qui permet à des acteurs malveillants de faible maturité de réussir dans des environnements pourtant renforcés. Les brokers d'accès, des individus et des groupes qui vendent des identifiants volés et des systèmes précédemment infectés, sont des innovateurs

actifs qui combinent généralement l'ingénierie sociale, les vulnérabilités non corrigées et les environnements permissifs pour réussir. Nous avons attribué 98 % des tentatives d'accès aux identifiants pour Microsoft Azure aux techniques de *force brute*, comme le montre le tableau 20. Il s'agit souvent d'une combinaison de techniques telles que la supposition de mots de passe, le craquage de mots de passe hachés, la pulvérisation de mots de passe et le bourrage d'identifiants. Les entreprises doivent anticiper les risques liés à la force brute et en tenir compte lors du déploiement d'une infrastructure destinée au public.

Les tentatives de force brute représentaient auparavant environ 86 % des signaux d'accès aux identifiants dans Microsoft Azure. Ce chiffre a augmenté de 12 %.

technique_name	Pourcentage
Force brute	97,74 %
Identifiants non sécurisés	2,05 %
Vol de tokens d'accès à l'application	0,17 %
Network Sniffing	0,04 %

Tableau 19 : accès aux identifiants par technique dans Microsoft Azure

Accès initial

L'accès initial, 25,52 % des signaux de Microsoft Azure, décrit les techniques utilisées pour s'implanter. Nous constatons que deux techniques principales sont employées : l'utilisation abusive d'identifiants de *comptes valides* et le *phishing* d'utilisateurs. Les *comptes valides* représentent près de 57 % de toutes les méthodes d'accès initial dans Microsoft Azure, ce qui montre bien que l'écosystème des brokers d'accès est en plein essor. Le *phishing* représente 43 % des signaux, une augmentation significative par rapport à l'année dernière qui s'explique en grande partie par la façon dont les données ont été combinées pour le rapport de cette année. Une analyse détaillée de nos règles de détection a révélé que 62 % des incidents de *phishing* observés impliquaient des e-mails Microsoft 365 signalés comme des malwares ou du phishing par les utilisateurs. Les 38 % restants étaient liés à des attaques par consentement via des applications enregistrées sur Microsoft Azure. Ces attaques exploitent les autorisations OAuth 2.0 en incitant les utilisateurs à accorder leur consentement à des applications malveillantes, obtenant ainsi un accès non autorisé à leurs données.

Persistance

Les techniques de cette catégorie fournissent aux utilisateurs malveillants un accès persistant ou à la demande aux environnements, systèmes ou données des victimes. Dans notre analyse de la *persistance*, qui représentait 25 % de tous les signaux anormaux liés à Microsoft Azure, nous avons observé que presque tous les signaux étaient directement liés à la *manipulation de comptes* d'une manière ou d'une autre. Contrairement aux points de terminaison, sur lesquels la *persistance* est obtenue via des applications, des paramètres, le système de fichiers, le registre ou une mauvaise configuration, la *persistance* dans l'environnement cloud (à l'exclusion des instances de calcul) est fréquemment liée à un compte IAM.

technique_name	Pourcentage
Manipulation de comptes	98,02 %
Comptes valides	1,03 %
Création d'une instance cloud	0,83 %
Création ou modification d'un compte cloud	0,07 %
Modification du processus d'authentification	0,06 %

Tableau 20 : persistance par technique dans Microsoft Azure

Une fois qu'un compte valide est compromis et que les identifiants restent inchangés, les utilisateurs malveillants peuvent se connecter et établir la *persistance* en modifiant les politiques principales existantes, en altérant les workflows d'authentification et en exploitant les autorisations et les privilèges inutiles.

Notre analyse a révélé que les autorisations de messagerie de Microsoft 365 Exchange sont des cibles courantes. Comme les applications enregistrées et les comptes valides compromis ajoutent fréquemment des autorisations telles que Accès complet, Envoyer en tant que ou Envoi par procuration, les utilisateurs malveillants dissimulent leurs signaux dans le bruit. À partir d'une entité Microsoft Azure de confiance, les menaces peuvent plus facilement hameçonner d'autres victimes.

Amazon Web Services

Selon [Statista](#), AWS est le fournisseur de services cloud le plus largement adopté cette année en termes de parts de marché, bien que seulement 26 % des signaux cloud proviennent d'AWS. Cela peut s'expliquer par notre décision de combiner les événements Microsoft Azure et Microsoft 365 cette année.

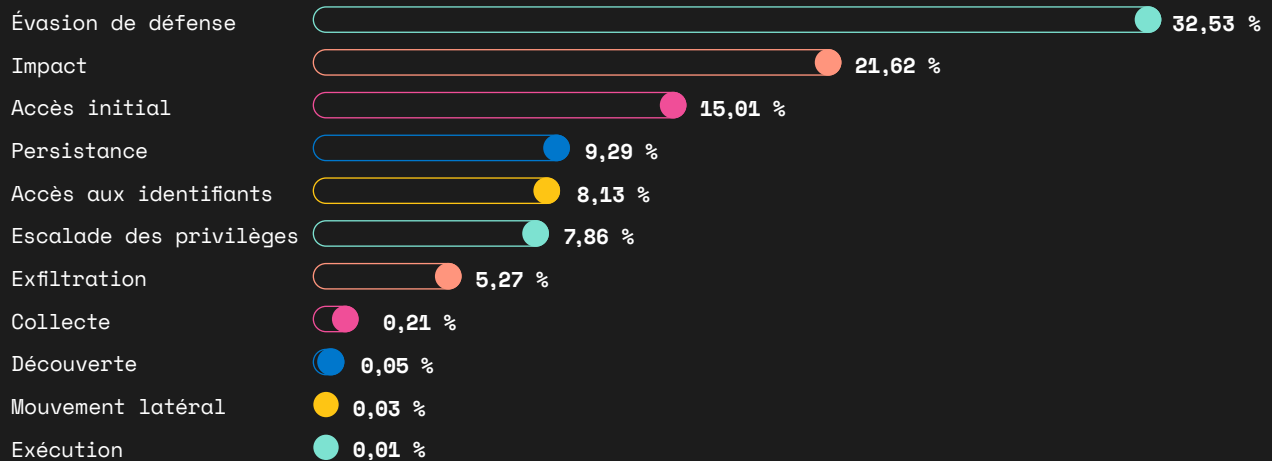


Figure 22 : signaux d'AWS par tactique

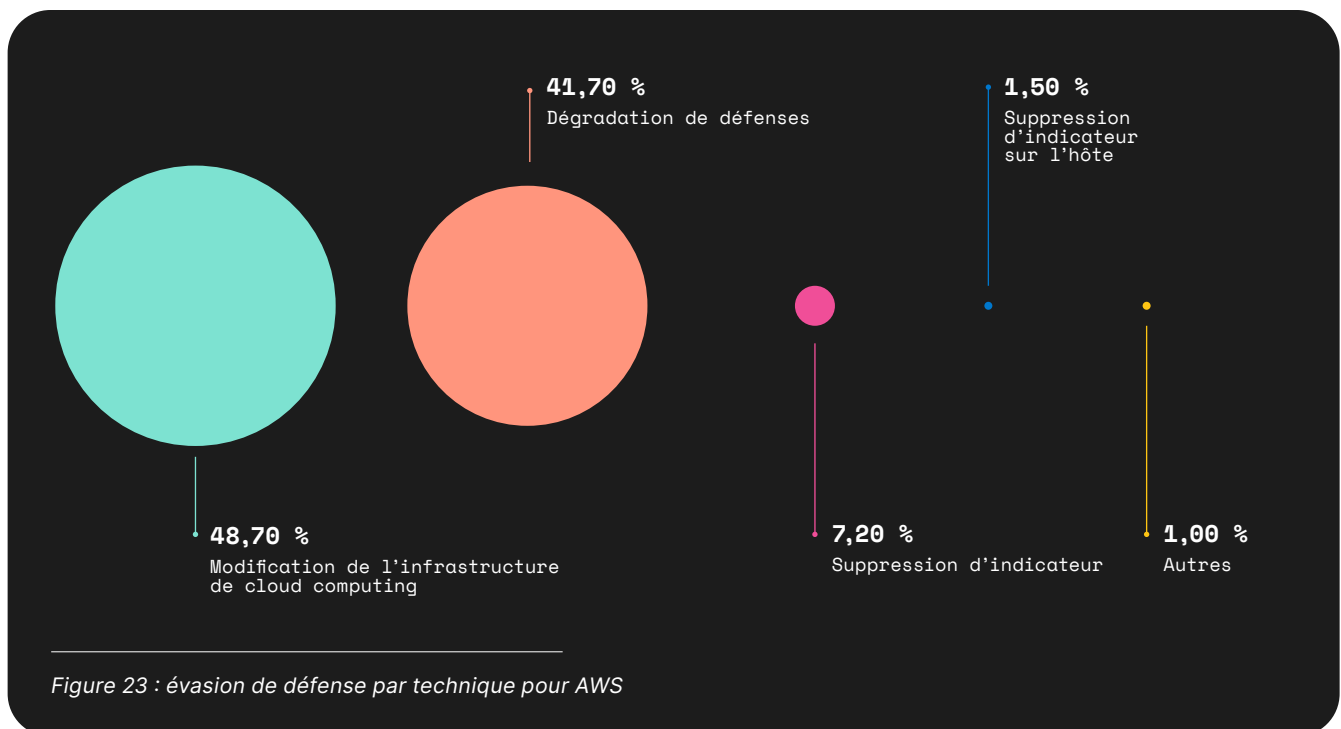
Au cours de notre analyse, 32,53 % de tous les signaux anormaux dans AWS ont été directement mis en correspondance avec des techniques potentielles d'évasion de défense. L'année dernière, cette valeur était de 38 %, soit une légère baisse. Les techniques d'impact ont connu l'une des augmentations les plus significatives,

avec un volume en hausse de plus de 20 %. L'accès initial a également augmenté, passant de moins d'un dixième de pourcentage l'année dernière à plus de 15 %, et les méthodes de persistance ont été observées de manière significative, passant de moins de 1 % l'année dernière à plus de 9 % en 2024.

Évasion de défense

Les techniques d'évasion de défense ont été l'observation la plus importante dans les données d'AWS, et nous estimons qu'elles continueront d'être importantes pour les entreprises afin de maintenir une certaine visibilité. Les événements les plus courants concernaient la modification de l'infrastructure de cloud computing, qui représentait 48,70 % des signaux. L'année dernière, les signaux liés à cet événement ont été observés moins de 1 % du temps. Les efforts de dégradation de défenses, qui représentaient la

majorité des signaux d'AWS l'année dernière avec 37 %, ont légèrement augmenté pour atteindre 41,70 %. La suppression d'indicateur est passée de 1 % l'année dernière à plus de 7 %. Les techniques les plus fréquemment observées pour tenter de *modifier l'infrastructure de cloud computing* ont identifié des modifications potentielles dans les configurations des groupes de sécurité et la restauration des snapshots RDS, avec respectivement 83,47 % et 13,90 %.



La forte distribution des signaux liés à la modification de l'infrastructure cloud peut être attribuée à la grande dépendance aux services d'AWS pour le déploiement et la gestion de l'infrastructure, en particulier pour les applications, les pipelines CI/CD et d'autres fonctions critiques. Dans un environnement de développement Agile, des ajustements fréquents et dynamiques de

l'infrastructure sont courants. Ce flux constant rend difficile pour les analystes de la sécurité de faire la distinction entre les activités bénignes et malveillantes. Les attaquants profitent donc de cette complexité pour masquer leurs actions, faisant de la modification de l'infrastructure cloud une tactique de premier plan pour échapper à la détection.

Dégradation de défenses

On peut supposer que les utilisateurs malveillants sont conscients de la visibilité et des capacités en matière de sécurité et qu'ils élaborent des stratégies pour s'assurer qu'elles n'interfèrent pas avec leurs objectifs. Les techniques et procédures de cette catégorie ont été développées dans ce but précis.

kibana_alert_rule_name	Pourcentage
AWS CloudWatch Alarm Deletion	42,16 %
AWS Config Resource Deletion	25,72 %
AWS EC2 Network Access Control List Deletion	10,79 %
AWS VPC Flow Logs Deletion	5,54 %
AWS WAF Access Control List Deletion	4,76 %
AWS CloudTrail Log Deleted	3,80 %
AWS WAF Rule or Rule Group Deletion	3,18 %
Autre	4,04 %







Tableau 21 : dégradation de défenses par nom d'alerte dans AWS

Les utilisateurs malveillants peuvent employer différentes approches pour désactiver ou falsifier les outils de sécurité :





- En supprimant les alarmes d'AWS CloudWatch (42,16 %) et les ressources d'AWS Config (25,72 %), les attaquants peuvent désactiver des systèmes de suivi et d'alerte essentiels.
- La suppression des listes de contrôle d'accès réseau (10,79 %) et des logs de flux VPC (cloud privé virtuel) (5,54 %) masque encore plus leurs activités en supprimant la visibilité sur les schémas de trafic réseau et les tentatives d'accès.
- La falsification directe des logs CloudTrail, que ce soit par suppression (3,80 %) ou suspension (1,13 %), peut interférer avec les fonctions de détection et de réponse.

Les techniques de cette catégorie sont conçues pour créer ou étendre des angles morts, et le suivi de leurs preuves devrait être une priorité. La méthode la plus courante pour la suppression d'indicateur consistait à supprimer les configurations du compartiment S3 (Simple Storage Service) à 98,48 %, qui pouvaient alerter les administrateurs en cas de modifications non autorisées ou de vols de données. En supprimant ou en modifiant ces indicateurs, les attaquants peuvent éviter d'être détectés. Les sources de données d'AWS contiennent une mine d'informations, comme le montre la représentation suivante, qui indique la fréquence d'apparition de chaque élément dans les données de télémétrie, en fonction des catégories de tactiques de MITRE ATT&CK. *L'évasion de défense*, qui est le phénomène le plus fréquemment observé, dépend fortement des événements d'Elastic Compute Cloud (EC2).



Évasion de défense

ec2.amazonaws.com	16,38 %	
monitoring.amazonaws.com	5,74 %	
config.amazonaws.com	3,65 %	
s3.amazonaws.com	2,36 %	
rds.amazonaws.com	2,21 %	
Autre	2,26 %	




Impact

ras.amazonaws.com	9,89 %	
logs.amazonaws.com	6,58 %	
kms.amazonaws.com	2,07 %	
Autre	2,97 %	

Accès initial

ssm.amazonaws.com	12,99 %	
signin.amazonaws.com	2,05 %	




Escalade des privilèges

sts.amazonaws.com	3,98 %	
iam.amazonaws.com	3,32 %	
Autre	0,57 %	

Exfiltration

ec2.amazonaws.com	3,87 %	
Autre	1,41 %	

Persistance

rds.amazonaws.com	4,05 %	
iam.amazonaws.com	2,65 %	
Autre	2,59 %	

Accès aux identifiants



secretsmanager.amazonaws.com	8,04 %	
ssm.amazonaws.com	0,05 %	

Figure 24 : sources de données d’AWS mises en correspondance avec les tactiques MITRE ATT&CK

Google Cloud

Google Cloud est un autre fournisseur de services cloud largement adopté, populaire pour des raisons similaires à celles de Microsoft Azure et AWS, notamment ses offres de services robustes, son infrastructure mondiale et ses fonctionnalités d’analyses avancées. Les organisations choisissent souvent Google Cloud, en particulier lorsqu’elles utilisent déjà Google Workspace, en raison de l’intégration fluide d’IAM, des services et des

outils de Google. Cette intégration étroite fait également de Google Cloud une cible de choix pour les utilisateurs malveillants. L’utilisation intensive de Google Workspace au sein des entreprises signifie que la compromission d’un seul ensemble d’identifiants peut potentiellement permettre aux attaquants d’accéder à un large éventail de services et de données.

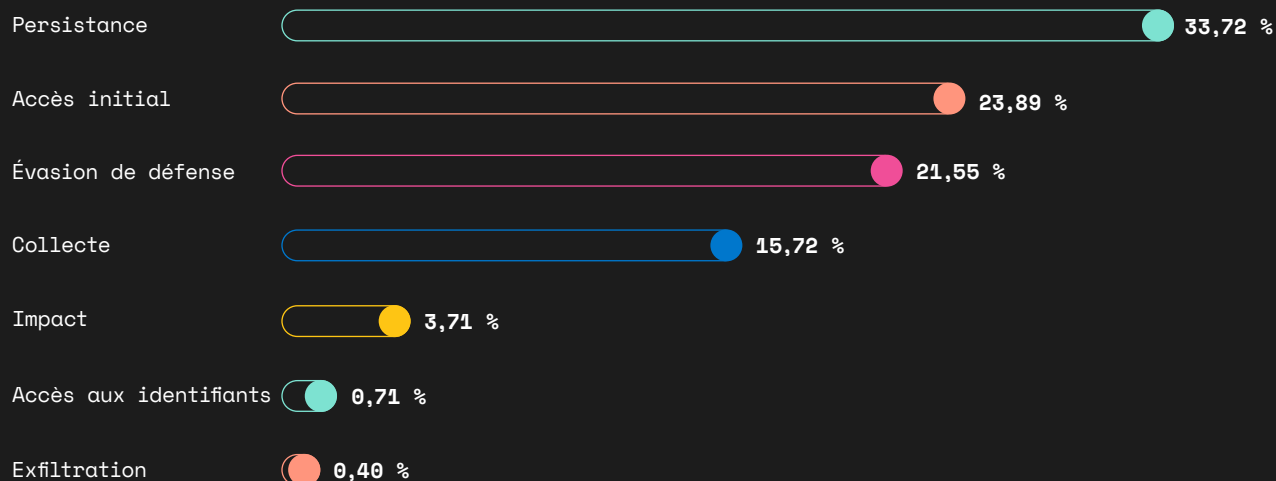


Figure 25 : signaux de Google Cloud par tactique

La *persistance* a augmenté de manière significative, passant de 1,5 % des signaux l'année dernière à 33,72 %, les méthodes d'*accès initial* ont été observées près de 24 % du temps par rapport à une valeur statistiquement insignifiante l'année dernière, et les événements d'*évasion de défense* ont diminué d'environ 85 % à 21,55 % cette année. La *collecte*, qui était la deuxième tactique la plus courante l'année dernière avec 10,74 %, a légèrement augmenté pour atteindre 15,72 %.

Persistence

En décomposant la *persistance* par technique, nous notons que 65,88 % de toutes les techniques de *persistance* dans Google Cloud sont liées à la *manipulation de comptes*, comme dans la partie Microsoft Azure de cette section. Cependant, dans Google Cloud, IAM inclut souvent les comptes d'utilisateurs et de service qui sont des cibles de grande valeur pour les utilisateurs malveillants.

À l'instar de Microsoft Azure et d'AWS, la *persistance*, l'*accès initial* et l'*évasion de défense* se classent en tête des signaux anormaux sur Google Cloud, mais l'*accès aux identifiants* est considérablement inférieur. À cet égard, les données constituent l'une des principales différences entre les fournisseurs de services cloud, le facteur le plus important pour détecter les menaces dans les environnements cloud. Bien que nous soupçonnions que les tentatives de connexion par force brute sont très courantes pour Google Cloud, les données n'étaient pas suffisantes pour conclure à cet impact.

Les identifiants compromis pour les comptes valides permettent aux utilisateurs malveillants de se connecter et de manipuler l'authentification du compte, les autorisations, etc. Les organisations doivent monitorer les événements d'authentification réussis et échoués, et s'efforcer d'identifier les anomalies comportementales.

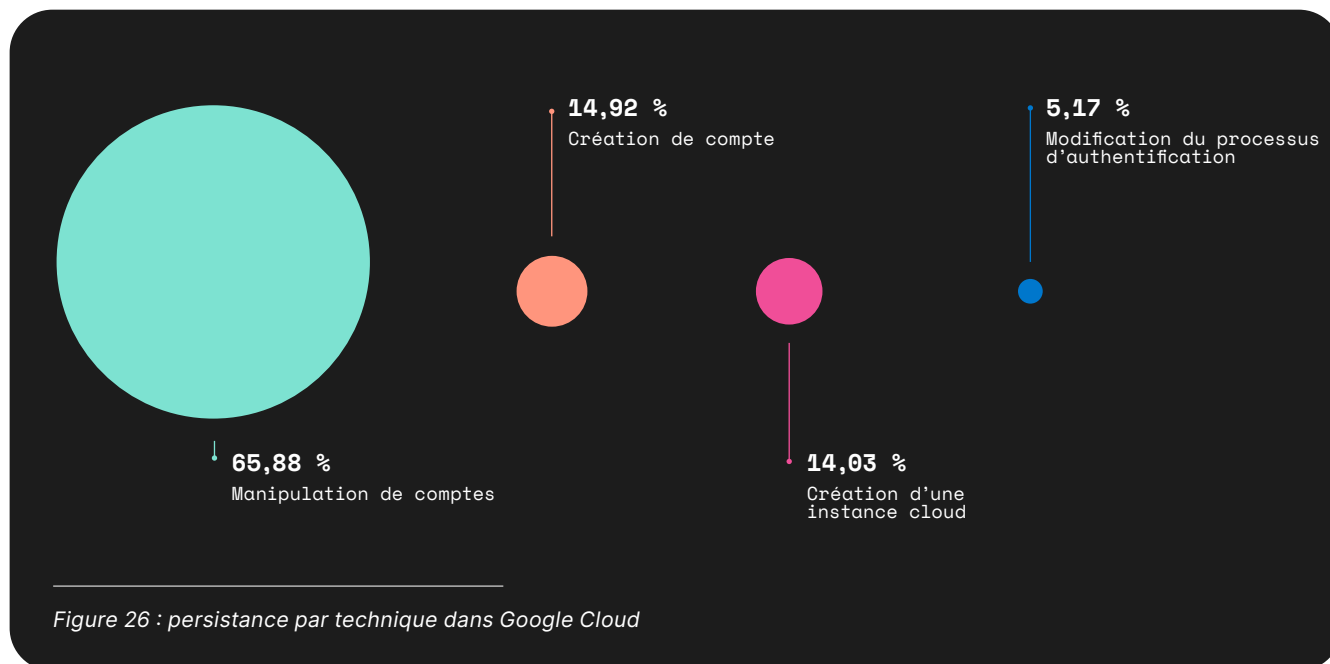


Figure 26 : persistance par technique dans Google Cloud

Les menaces disposant du niveau d'accès approprié créent couramment des comptes, éventuellement après une *escalade des privilèges* ou la compromission d'un compte d'administrateur. Les utilisateurs malveillants peuvent utiliser des comptes frauduleux pour un accès à la demande,

en utilisant des outils de productivité par ailleurs bénins pour effectuer des recherches et des exfiltrations rapides. L'audit d'IAM et les données contextuelles sur les connexions devraient révéler des preuves de changements de comptes, de nouveaux comptes et de nouvelles entités.

kibana_alert_rule_name	Pourcentage
Google Workspace API Access Granted via Domain-Wide Delegation of Authority	31,58 %
Google Workspace Admin Role Assigned to a User	24,21 %
Google Cloud Service Account Key Creation	20,87 %
Google Cloud IAM Service Account Key Deletion	9,28 %
Google Workspace Custom Admin Role Created	7,46 %
Google Workspace Role Modified	5,12 %
Google Workspace Password Policy Modified	0,95 %
Suspended User Made Active	0,52 %

Tableau 22 : manipulation de comptes par nom de règle dans Google Cloud

La *manipulation de comptes* reste une technique de *persistance* prédominante dans les environnements Google Cloud, une grande partie de ces activités étant centrée sur l'utilisation abusive des privilèges administratifs et des comptes de service. 31,58 % des signaux anormaux liés à la *manipulation de comptes* étaient dus à l'accès à l'API Google Workspace accordé via une *délégation d'autorité à l'échelle du domaine*. Cette délégation d'autorité peut être utilisée à mauvais escient par des utilisateurs malveillants pour maintenir un accès permanent

à des données et services sensibles, en contournant les mécanismes d'authentification normaux que les équipes de sécurité seraient plus enclines à monitorer.

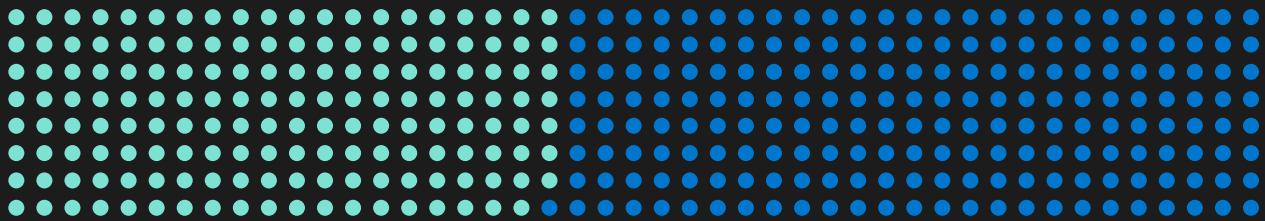
L'attribution des rôles d'administrateur de Google Workspace aux utilisateurs représente 24,21 % des signaux de *manipulation de comptes*. De même, la création et la suppression de clés des comptes de service IAM de Google Cloud, qui représentent respectivement 20,87 % et 9,28 % des alertes, mettent en évidence des événements de sécurité critiques.

Parmi les autres activités notables de *manipulation de comptes* figurent la création de rôles d'administrateur personnalisés (7,46 %) et la modification de rôles existants (5,12 %) au sein de Google Workspace. Les rôles d'administrateur personnalisés peuvent être adaptés pour accorder des privilèges spécifiques qui facilitent les activités malveillantes en cours tout en échappant à la détection. En outre, même des actions moins fréquentes, telles que la modification des politiques de mots de passe (0,95 %) ou la réactivation d'utilisateurs suspendus (0,52 %), peuvent avoir un impact significatif sur la sécurité en affaiblissant les contrôles d'authentification ou en rétablissant l'accès à des comptes précédemment compromis.

Accès initial

Dans l'analyse des techniques d'accès *initial* dans les environnements Google Cloud, les *comptes valides* et le *phishing* apparaissent comme les principales méthodes utilisées par les utilisateurs malveillants pour accéder aux systèmes. Ces deux méthodes seront très familières à de nombreuses équipes de sécurité.

● Phishing 43,80 %



● Comptes valides 56,20 %

Figure 27 : accès initial par technique

Les comptes valides représentent 56,20 % des signaux d'accès initial, ce qui rend difficile la détection d'actions malveillantes par les équipes de sécurité. La forte prévalence de l'utilisation de comptes valides souligne le besoin essentiel de politiques de mots de passe strictes, d'authentification multi-facteurs et de suivi continu

des schémas et comportements de connexion inhabituels. Le *phishing*, responsable de 43,80 % des signaux d'accès initial, reste un vecteur de menace important dans les environnements Google Cloud. Une fois obtenus, les identifiants détournés peuvent être utilisés pour accéder aux données et services sensibles de Google Cloud.

kibana_alert_rule_name	Pourcentage
Google Workspace Object Copied from External Drive and Access Granted to Custom Application	41,44 %
User Reported Phishing	29,52 %
User Reported Spam Spike	14,98 %
Gmail Potential Employee Spoofing	6,63 %
Phishing Reclassification	6,09 %
User Suspended (Spam)	1,33 %

Tableau 23 : alertes de phishing par nom de règle dans Google Cloud

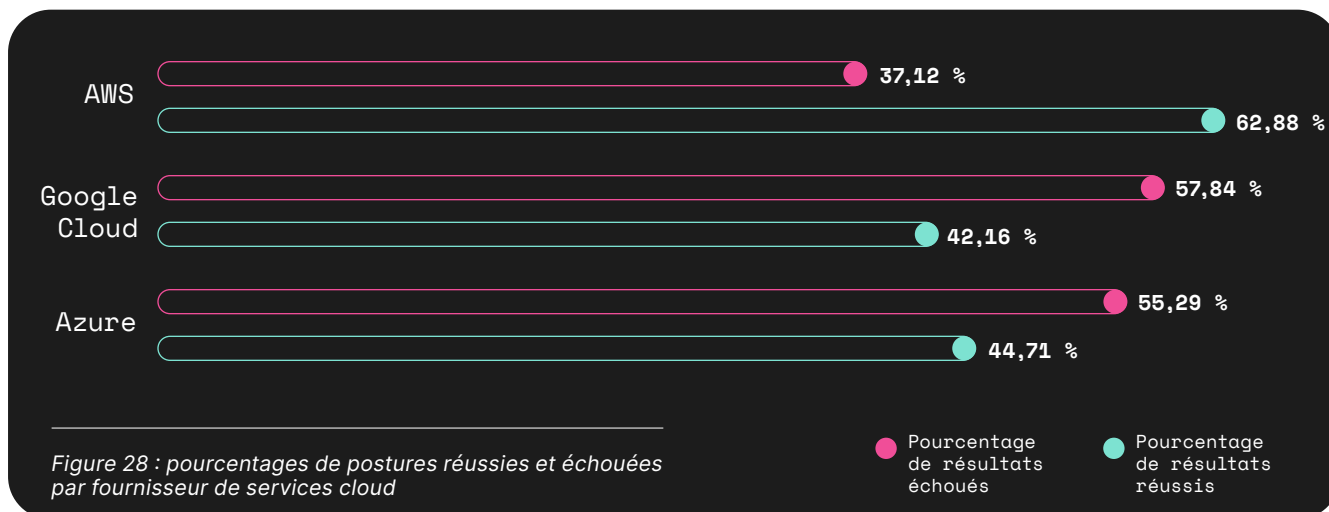
La technique de *phishing* la plus courante consiste à copier des objets Google Workspace à partir de lecteurs externes et à accorder l'accès à des applications personnalisées, ce qui représente 41,44 % des signaux. Le phishing signalé par les utilisateurs représente 29,52 % des signaux de *phishing*, ce qui indique que les utilisateurs finaux

constituent une ligne de défense essentielle pour identifier et signaler les activités suspectes. Les spams signalés par les utilisateurs, distincts des tentatives de phishing, représentent 14,98 % des signaux.

Évaluation comparative de la posture de sécurité du cloud

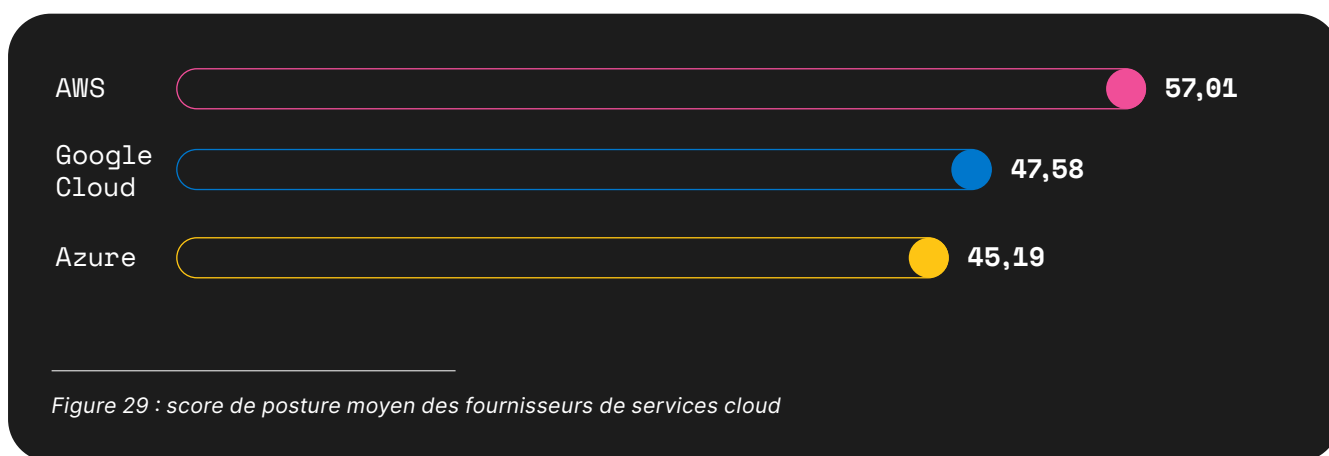
Nouveauté cette année, le rapport d'Elastic sur les menaces mondiales inclut une analyse des résultats générés par la capacité de [gestion de la posture de sécurité du cloud](#) (CSPM) d'Elastic Security. Cette dernière découvre et évalue les instances des services cloud, tels que le stockage, le cloud computing, IAM, et plus encore, par rapport aux directives de configuration

sécurisée définies par le [CIS](#). Cette évaluation aide les organisations à identifier les risques liés à la configuration. Ces mauvaises configurations sont décrites comme des résultats, et la figure 27 montre les proportions de résultats (réussites et échecs) recueillis à partir de la télémétrie pour chaque fournisseur de services cloud.



Les lecteurs doivent noter qu'en fin de compte, les entreprises sont responsables de la sécurisation de leur infrastructure hébergée par le fournisseur de services cloud, et que ces statistiques ne reflètent pas la sécurité du fournisseur, mais plutôt la sécurité générale des différentes populations d'utilisateurs.

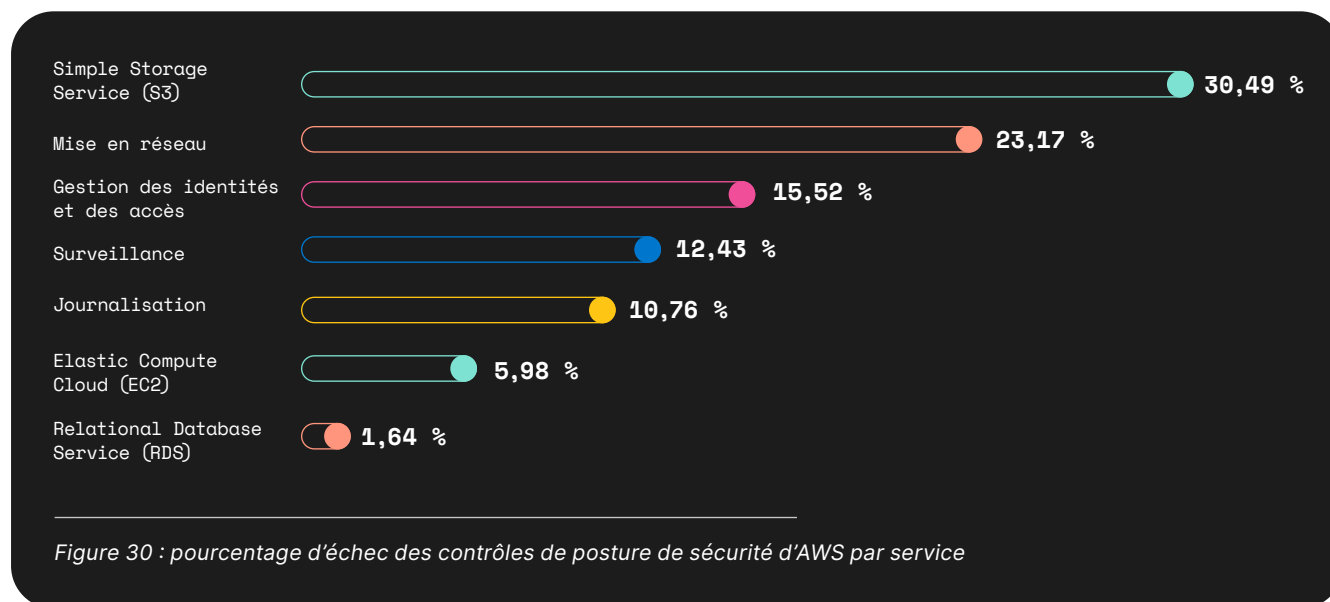
Le score de référence du CIS de chaque fournisseur de services cloud, appelé score de posture sur la figure 28, est noté sur 100 et mesure la conformité aux directives de configuration sécurisée décrites dans les références du CIS. En moyenne, AWS a un score de posture de 57 avec Google Cloud et Microsoft Azure à 48 et 45 respectivement.



Le score de posture du CIS est une abstraction intentionnelle. Pour rendre ces résultats exploitables, nous devons décomposer les résultats des fournisseurs de services cloud spécifiques. Nous explorerons les détails de chaque fournisseur de services cloud dans les sous-sections suivantes.

Amazon Web Services

En décomposant les échecs des contrôles de posture par AWS, nous avons observé que 30 % de tous les échecs des contrôles de posture concernent S3. S3 est un service de stockage d'objets d'AWS qui permet aux utilisateurs de stocker et de récupérer des données. Souvent, ce service est utilisé par les organisations pour stocker des données sensibles et non sensibles, c'est pourquoi AWS propose plusieurs [fonctionnalités de sécurité](#) critiques natives de S3.



Les résultats de la mise en réseau, d'IAM et de la surveillance d'AWS révèlent un pourcentage moyen d'échec des contrôles de 23,17 %, 15,52 % et 12,43 % respectivement. Pour aller plus loin, nous avons analysé les échecs des contrôles de posture pour AWS en les croisant avec les noms des règles de référence du CIS. Près de 53 % de tous les échecs des contrôles de posture étaient liés à l'activation des autorisations de suppression de l'authentification multi-facteurs dans les

compartiments S3. L'autorisation de suppression de l'authentification multi-facteurs permet aux personnes ayant accès aux compartiments S3 de supprimer la version d'un objet ou l'état de version de ce compartiment. En outre, 24 % des compartiments S3 n'étaient pas configurés pour bloquer l'accès public, ce qui les exposait, ainsi que leurs objets potentiellement sensibles, à des clients non autorisés.

rule_name	Pourcentage de résultats échoués
Ensure MFA Delete is enabled on S3 buckets	53,23 %
Ensure that S3 Buckets are configured with 'Block public access (bucket settings)'	24,00 %
Ensure S3 Bucket Policy is set to deny HTTP requests	22,77 %

Tableau 24 : pourcentage d'échec des contrôles de posture du S3 (Simple Storage Service) par règle

En recoupant ces données avec les signaux anormaux de gestion des informations et des événements de sécurité (SIEM) analysés précédemment dans ce rapport, nous avons observé qu'une part importante de ces signaux était liée à des changements de configuration du compartiment S3, à la suppression d'objets et à des tentatives d'accès à des objets à partir de sources inconnues. Cette corrélation souligne l'importance cruciale de la mise en place de l'authentification multi-facteurs sur les compartiments S3 et les objets. Nous recommandons aux personnes qui cherchent à améliorer leur posture de sécurité de consulter les [bonnes pratiques de sécurité](#) d'AWS pour S3.

Le tableau 26 développe les résultats de la posture de sécurité du réseau par règle. Les problèmes de mise en réseau représentent le deuxième plus grand nombre de défaillances de la posture de sécurité pour AWS, avec 23 % de tous les contrôles. Après un examen plus approfondi, nous avons constaté que 33 % de ces échecs des contrôles étaient liés à l'accès aux réseaux hébergés dans AWS. Plus précisément, les politiques liées aux ressources autorisent le trafic en provenance de n'importe quelle adresse IP ou de n'importe quel port, qu'il soit administratif ou non. Cette mauvaise configuration rend de nombreux réseaux VPC et potentiellement des instances EC2 vulnérables à l'accès de n'importe qui, y compris des menaces.

Benchmark_rule	Pourcentage de résultats échoués
Ensure no Network ACLs allow ingress from 0.0.0.0/0 to remote server administration ports	33,19 %
Ensure no security groups allow ingress from 0.0.0.0/0 to remote server administration ports	32,56 %
Ensure the default security group of every VPC restricts all traffic	30,62 %
Ensure no security groups allow ingress from ::/0 to remote server administration ports	3,63 %

Tableau 25 : pourcentage d'échec des contrôles de posture de sécurité du réseau par règle

Le fait d'autoriser l'accès de n'importe où et à n'importe quel moment permet aux acteurs malveillants de procéder à des analyses de vulnérabilité, de relever les empreintes digitales

des serveurs web et de tenter d'accéder à distance à l'aide de protocoles tels que RDP et SSH. Une telle posture permissive nuit aux contrôles disponibles au niveau du périmètre du réseau.

Augmentation du score du CIS pour AWS

La correction de ces erreurs de configuration des règles des groupes de sécurité et des listes de contrôle d'accès réseau pour restreindre le trafic entrant aux seules adresses IP fiables et aux ports nécessaires constitue une étape fondamentale afin d'améliorer la posture de sécurité et d'augmenter les scores de référence du CIS. N'autorisez pas le trafic en provenance de n'importe quelle adresse IP, appliquez le principe du moindre privilège en n'accordant que l'accès nécessaire au bon fonctionnement des services et des utilisateurs. De plus, isolez les ressources et services critiques à l'aide de segments de réseau. (suite)

Des audits réguliers des configurations du réseau et un suivi continu de tout changement ou anomalie sont des pratiques essentielles. Des outils automatisés et des services gérés comme [AWS Config](#) sur le [tableau de bord CSPM d'Elastic Security](#) peuvent aider à maintenir la conformité avec les bonnes pratiques de sécurité. L'amélioration du logging et des alertes pour les tentatives d'accès inhabituelles ou non autorisées, et l'utilisation de services tels que CloudTrail et les logs de flux VPC, offrent une visibilité sur le trafic réseau et les schémas d'accès.

Microsoft Azure

Les références de Microsoft Azure mettent notamment l'accent sur les services IAM et de collaboration via Microsoft 365. L'analyse de la posture de sécurité de Microsoft Azure soulève d'importantes préoccupations concernant les comptes de stockage, qui représentent 46,68 % de tous les échecs des contrôles de sécurité.

Cela correspond à des configurations erronées dans les comptes de service de stockage de Microsoft Azure. Dans le cadre d'un exercice de simulation du pire des cas, la question suivante pourrait se poser : que se passe-t-il si un affilié de ransomware utilisant des identifiants volés achetés auprès d'un broker d'accès décide de supprimer le contenu du stockage de Microsoft Azure ?

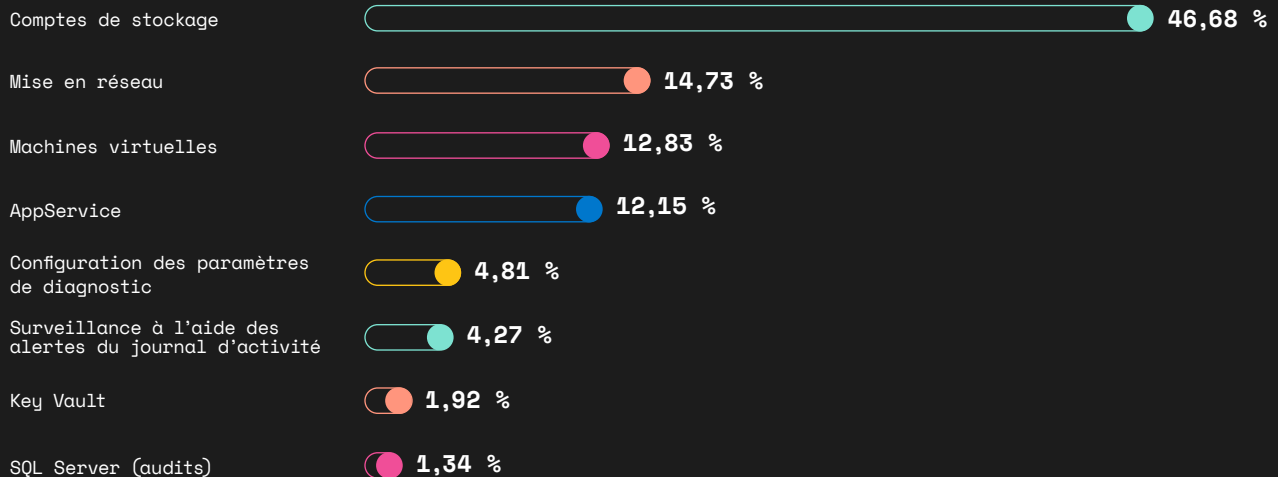


Figure 31 : pourcentage d'échec des contrôles de posture de sécurité de Microsoft Azure par service

La mise en réseau, les machines virtuelles et les AppService constituent d'autres sujets de préoccupation, avec des pourcentages d'échec des contrôles de 14,73 %, 12,83 % et 12,15 %,

respectivement. Les erreurs de configuration de la mise réseau peuvent exposer les ressources internes à des menaces externes, tandis que les vulnérabilités des machines virtuelles et

des AppService peuvent fournir aux utilisateurs malveillants des points d'appui pour lancer d'autres attaques. Il est essentiel de garantir des configurations de sécurité robustes et un suivi continu de ces services pour atténuer les risques et protéger l'ensemble de l'infrastructure cloud. Les comptes de stockage Microsoft Azure sont

des composants essentiels dans de nombreux environnements cloud, fournissant des solutions de stockage évolutives et sécurisées pour un large éventail de données. Cependant, une analyse plus approfondie révèle plusieurs erreurs de configuration courantes qui ont un impact sur la posture de sécurité.

Benchmark_rule	Pourcentage de résultats échoués
Ensure that 'Enable Infrastructure Encryption' for Each Storage Account in Microsoft Azure Storage is Set to 'enabled'	15,89 %
Ensure Private Endpoints are used to access Storage Accounts	15,52 %
Ensure Default Network Access Rule for Storage Accounts is Set to Deny	14,26 %
Ensure 'Allow Microsoft Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access	14,26 %
Ensure Storage Logging is Enabled for Queue Service for 'Read', 'Write', and 'Delete' requests	7,67 %
Ensure Storage Logging is Enabled for Table Service for 'Read', 'Write', and 'Delete' Requests	7,62 %
Ensure Storage logging is Enabled for Blob Service for 'Read', 'Write', and 'Delete' requests	7,57 %
Ensure the "Minimum TLS version" for storage accounts is set to "Version 1.2"	6,56 %
Ensure Soft Delete is Enabled for Microsoft Azure Containers and Blob Storage	5,14 %
Ensure that 'Public access level' is disabled for storage accounts with blob containers	4,00 %
Ensure that 'Secure transfer required' is set to 'Enabled'	1,50 %

Tableau 26 : pourcentage d'échec des contrôles de posture de sécurité du compte de stockage Microsoft Azure par règle

15,89 % des échecs des contrôles étaient dus à l'absence de chiffrement de l'infrastructure ("Enable Infrastructure Encryption" [Activer le chiffrement de l'infrastructure] n'était pas défini sur "Enabled" [Activé]). Le [chiffrement de l'infrastructure](#) ajoute une couche de sécurité supplémentaire en chiffrant les données au repos à l'aide d'une deuxième couche de chiffrement afin de protéger les informations sensibles contre d'éventuelles violations. Cette dernière ligne de

défense contre les intrusions et les vols devient de plus en plus vulnérable à mesure que d'autres formes de sécurité sont désactivées ou altérées. Les points de terminaison privés résident dans les réseaux virtuels de Microsoft Azure et sont utilisés pour interagir avec les comptes de stockage de Microsoft Azure, un mécanisme d'abstraction clé qui a entraîné environ 16 % des échecs. L'utilisation d'un point de terminaison privé limite l'exposition des identifiants et des données des comptes.

Plusieurs contrôles des services étaient fréquemment mal configurés, ce qui permettait d'accéder facilement aux comptes de stockage pour monitorer les schémas d'accès afin de détecter les activités suspectes :

- Autorisation des services Microsoft Azure figurant sur la liste des services fiables à accéder aux comptes de stockage : 14,26 %

- Définition de la règle d'accès au réseau par défaut comme étant un refus : 14,26 %
- Activation du logging de stockage pour les services Blob, Queue et Table : 22,86 % combinés

L'activation du logging pour les demandes de lecture, d'écriture et de suppression est particulièrement importante à des fins d'analyse judiciaire et d'audit.

L'authentification multi-facteurs n'était pas activé pour tous les utilisateurs d'IAM disposant d'un mot de passe de console dans 7 % des cas. L'authentification multi-facteurs fournit une couche de sécurité supplémentaire au-delà du simple mot de passe, ce qui rend l'accès non autorisé beaucoup plus difficile pour les attaquants. L'activation de l'authentification multi-facteurs est une mesure de sécurité cruciale, en particulier pour les comptes dotés de privilèges élevés. Ce chiffre devrait être de 0 %. L'importance de l'authentification multi-facteurs ne peut être surestimée lorsqu'il est question des contrôles de sécurité d'IAM.

Google Cloud

Google Cloud met fortement l'accent sur ses capacités sophistiquées d'analyse de données et de Machine Learning, ce qui élargit le paysage des menaces. Cela nécessite de solides mesures de sécurité pour se protéger contre les accès non autorisés et les éventuelles violations, ce qui souligne l'importance de maintenir une posture sécurisée dans les environnements Google Cloud.

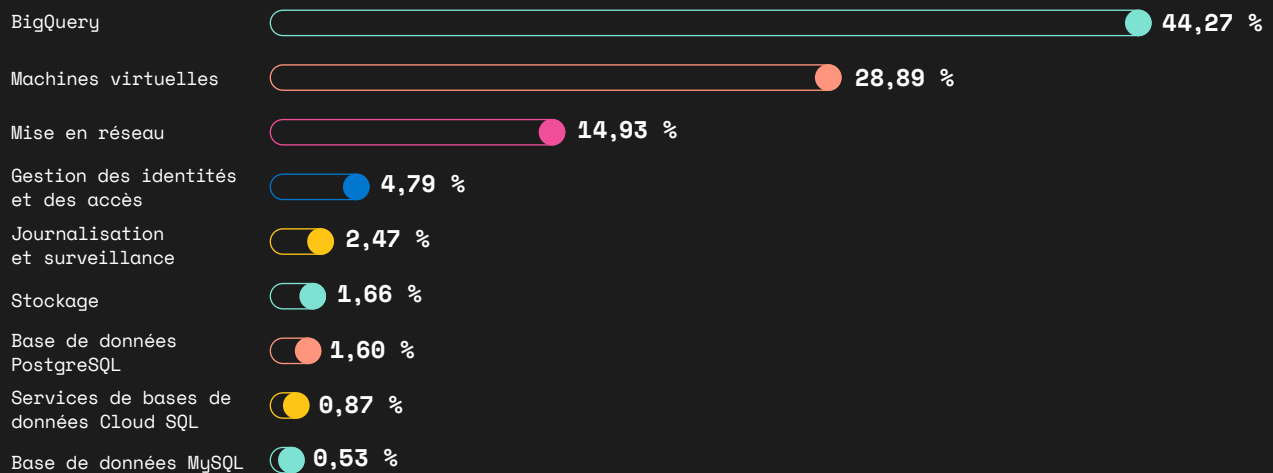


Figure 32 : pourcentage d'échec des contrôles de posture de sécurité de Google Cloud par service

Selon nos données, BigQuery de Google Cloud est le service qui enregistre le pourcentage le plus élevé d'échec des contrôles de posture de sécurité, soit près de 44 % du total. BigQuery est une puissante solution d'entrepôt de données utilisée pour analyser de grands ensembles de données, et son utilisation intensive dans de nombreuses organisations en fait une cible de choix pour les erreurs de configuration et les failles de sécurité. Les problèmes de mise en réseau représentent 15 % des échecs des contrôles, ce qui met en

évidence un autre domaine critique dans lequel les pratiques de sécurité doivent être améliorées. Des paramètres réseau mal configurés, tels que des règles de pare-feu trop permissives ou une segmentation inappropriée, peuvent exposer les ressources cloud à des menaces externes et à des accès non autorisés.

L'analyse de la posture de sécurité du service BigQuery de Google Cloud a permis de mettre en évidence la prévalence écrasante des erreurs de configuration liées au chiffrement.

rule_name	Pourcentage de résultats échoués
Ensure that All BigQuery Tables Are Encrypted with Customer-Managed Encryption Key (CMEK)	95,75 %
Ensure that a Default Customer-Managed Encryption Key (CMEK) Is Specified for All BigQuery Data Sets	4,25 %

Tableau 27 : pourcentage d'échec des contrôles de posture de sécurité de BigQuery de Google Cloud par règle

Étonnamment, 96 % des échecs des contrôles étaient dus à des utilisateurs utilisant des tables BigQuery sans les chiffrer avec CMEK. CMEK offre un niveau de contrôle et de sécurité supérieur sur le chiffrement des données en permettant aux organisations de gérer leurs clés de chiffrement. Certaines des charges de travail les plus critiques de toute organisation peuvent être traitées via BigQuery. Les utilisateurs doivent s'assurer que toutes les tables BigQuery sont chiffrées avec CME.

4,25 % des échecs des contrôles concernent l'absence d'un CMEK par défaut défini par l'utilisateur et spécifié pour tous les ensembles de données BigQuery. Cette configuration garantit que toutes les nouvelles tables créées dans un ensemble de données héritent de la politique de chiffrement spécifiée, ce qui simplifie la gestion de la sécurité et réduit le risque de données non chiffrées. Aucun échec de contrôle n'a été enregistré pour des ensembles de données BigQuery anonymes ou publics, ce qui suggère que les organisations sont vigilantes quant aux politiques de contrôle d'accès. Le thème récurrent des erreurs de

configuration liées au chiffrement chez différents fournisseurs de services cloud, notamment AWS et Microsoft Azure, montre que les entreprises doivent adopter des politiques de chiffrement plus strictes et procéder à des audits réguliers pour protéger leurs données dans le cloud.

Les machines virtuelles dans Google Cloud posent également des problèmes de sécurité importants, représentant 29 % des échecs des contrôles. Une mauvaise configuration des paramètres des machines virtuelles peut exposer les charges de travail critiques à des menaces, les rendant vulnérables à des attaques telles que des accès

non autorisés, des infections par malwares et des violations de données. Afin de sécuriser correctement les machines virtuelles, il convient de mettre en œuvre des contrôles d'accès stricts, de veiller à ce que les correctifs et les mises à jour soient à jour et d'utiliser des fonctionnalités

de sécurité avancées telles que les machines virtuelles blindées et le chiffrement des disques. L'analyse de la posture de sécurité des machines virtuelles de Google Cloud révèle d'importantes vulnérabilités liées au chiffrement et à la gestion des clés SSH.

Benchmark_rule	Pourcentage de résultats échoués
Ensure VM Disks for Critical VMs Are Encrypted with Customer-Supplied Encryption Keys (CSEK)	51,24 %
Ensure "Block Project-Wide SSH Keys" Is Enabled for VM Instances	20,06 %
Ensure Oslogin Is Enabled for a Project	11,10 %
Ensure that Compute Instances Have Confidential Computing Enabled	6,71 %
Ensure that Compute Instances Do Not Have Public IP Addresses	4,19 %
Ensure that Instances Are Not Configured to Use the Default Service Account	3,49 %
Ensure that IP Forwarding Is Not Enabled on Instances	1,24 %
Ensure Compute Instances Are Launched with Shielded VM Enabled	0,90 %
Ensure that Instances Are Not Configured to Use the Default Service Account with Full Access to All Cloud APIs	0,85 %
Ensure 'Enable Connecting to Serial Ports' Is Not Enabled for VM Instance	0,23 %

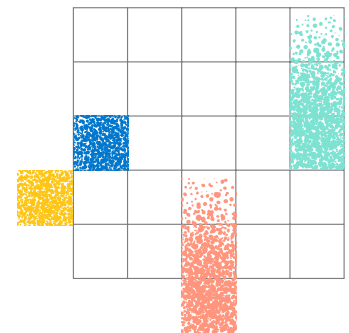
Tableau 28 : pourcentage d'échec des contrôles de posture de sécurité des machines virtuelles de Google Cloud par règle

Plus de 51 % des échecs des contrôles étaient dus à l'absence de CSEK pour les disques des machines virtuelles, ce qui est essentiel pour garantir que les entreprises gardent le contrôle de leurs clés de chiffrement et, par conséquent, de la sécurité de leurs données.

Autre résultat remarquable : 20,06 % des échecs des contrôles étaient dus à l'absence de blocage des clés SSH à l'échelle du projet. Lorsque "Block Project-Wide SSH Keys" (Bloquer les clés SSH à

l'échelle du projet) n'est pas activé, cela permet d'utiliser les clés SSH ajoutées au niveau du projet sur toutes les instances de machines virtuelles de ce projet, ce qui peut entraîner un accès non autorisé si l'une de ces clés est compromise. L'activation de ce paramètre garantit que seules les clés SSH spécifiques aux instances sont autorisées, ce qui réduit la surface d'attaque et empêche l'accès non autorisé aux instances de machines virtuelles via SSH.

Aucun fournisseur de services cloud n'est capable de vous protéger contre vous-même, et nous estimons que les résultats les plus courants sont dus à l'affaiblissement de la sécurité par les utilisateurs ou les administrateurs, et non à des failles ou à des faiblesses inhérentes. Les lecteurs devraient réfléchir à leur propre utilisation de ces fournisseurs de services cloud et se demander dans quelle mesure ils peuvent se rapprocher d'une référence du CIS parfaite en acceptant le moins de risques possible.



Profils des menaces

Au cours de cette année, Elastic Security Labs a suivi des dizaines de menaces observées dans la télémétrie d'Elastic. Des chercheurs et des ingénieurs spécialisés dans l'analyse du renseignement, la rétro-ingénierie des malwares et la détection analysent ces menaces afin de découvrir les méthodes les plus efficaces pour les atténuer. Pour le rapport sur les menaces mondiales, nous avons décrit cinq grands profils de menaces élaborés au cours de l'année écoulée dans le cadre de l'engagement d'Elastic Security Labs à démocratiser l'accès au paysage des menaces. Ces profils ont été choisis en fonction des menaces existantes observées grâce à notre télémétrie unique et qui mettent en évidence des approches nouvelles ou inédites que les équipes de sécurité n'ont peut-être pas détectées. Les groupes d'activités étudiés dans le rapport sur les menaces mondiales de cette année sont les suivants :

- **REF5961** : trois familles de malwares inédites qui ciblent un ministère des Affaires étrangères de l'Association des nations d'Asie du Sud-Est (ASEAN) ;
- **GHOSTPULSE** : un malware inédit qui utilise les packages d'applications du programme d'installation de Microsoft pour Windows 10 (MSIX) afin d'obtenir un accès *initial* ;
- **GHOSTENGINE** : une porte dérobée non documentée utilisée pour établir la *persistance* et exécuter un mineur de cryptomonnaie ;
- **KANDYKORN** : une intrusion inédite qui cible les ingénieurs blockchain d'une plateforme d'échange de cryptomonnaies, une opération utilisée par un État isolé pour échapper aux sanctions imposées par la communauté internationale ;
- **WARMCOKIE** : une porte dérobée inédite utilisée à des fins d'espionnage.

Dénomination des menaces

Elastic Security Labs utilise un système de suivi des références qui rassemble les groupes d'activités, les schémas d'attaque et les ensembles d'intrusions. Ces éléments sont mis en corrélation avec des malwares, une logique d'attaque et des techniques spécifiques, et parfois, avec les victimes ciblées. Un numéro à quatre chiffres avec le préfixe "REF" (exemple : REF1234) leur est attribué. Les lecteurs ne doivent pas les confondre avec des cryptonymes, qu'Elastic Security Labs ne divulgue pas.

Lorsque la découverte concerne une famille de malwares non documentée auparavant, comme EAGERBEE, ou une technique d'intrusion comme GrimResource, nous utilisons des conventions de dénomination distinctes pour éviter toute confusion : les noms des malwares sont tout en majuscules et les noms des techniques portent une majuscule à la première lettre de chaque mot.

Le modèle en diamant

Chaque profil de menace contient un diagramme conventionnel appelé modèle en diamant pour chaque groupe répertorié avec un identifiant REF. Afin d'en faciliter la lecture, nous avons omis les points communs avec les groupes nommés surveillés par d'autres fournisseurs. Attention toutefois : cela ne signifie pas que nous validons ou infirmons les éléments identifiés par ces fournisseurs.

Le modèle en diamant nous permet de décrire les relations générales qui existent entre les utilisateurs malveillants, les capacités, l'infrastructure et les victimes des intrusions, en mettant l'accent sur l'axe technique exploitable (capacités:infrastructure). Généralement, c'est l'intrusion qui se trouve au centre de ce modèle, mais ici, nous plaçons les utilisateurs malveillants comme point de mire pour mettre en avant les observations réalisées sur de nombreux incidents.

Terminologie

Nous utilisons un sous-ensemble de termes propres au secteur pour décrire les activités malveillantes et les résultats connexes, dont beaucoup sont imbriqués ou dérivés les uns des autres. Un groupe d'activités peut se composer d'un ou de plusieurs schémas d'attaque et être résumé en un ou plusieurs ensembles d'intrusions. Les éléments suivants sont classés par degré d'information, du plus grand au plus petit :

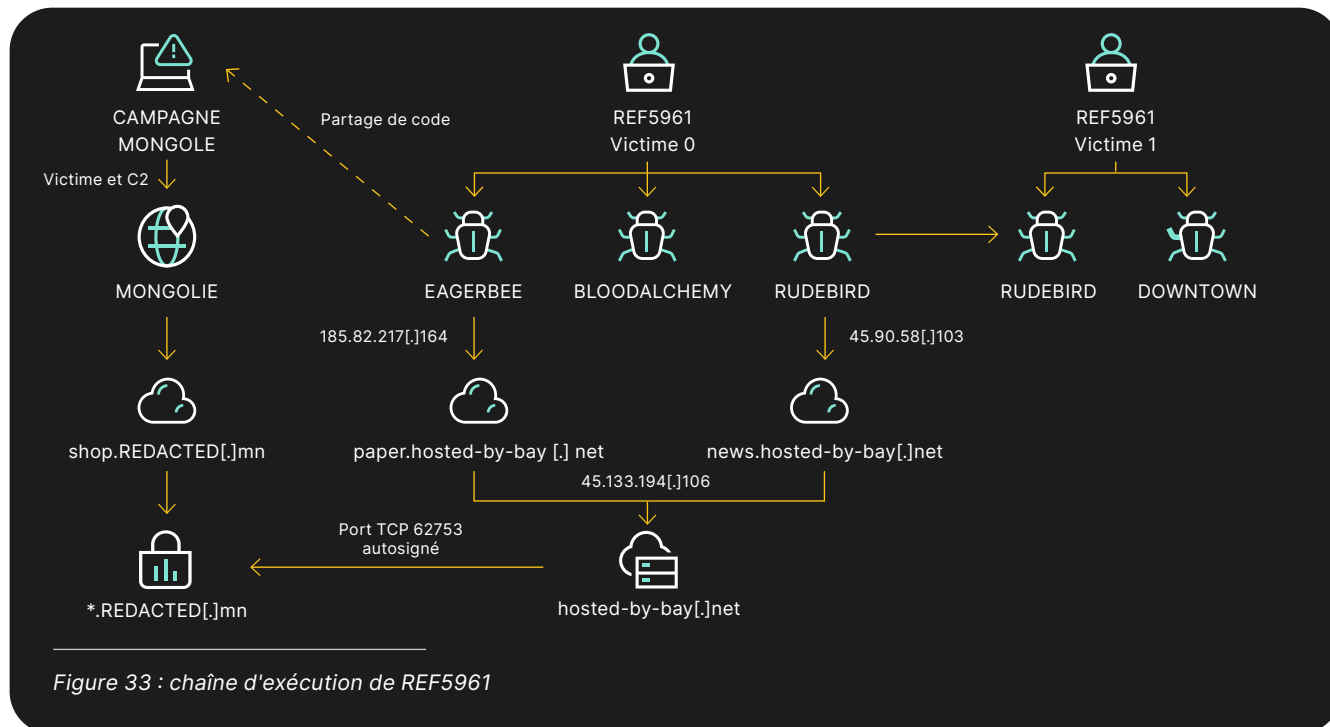
- **Groupe d'activités** : un ensemble d'activités attribuées à des personnes ou à des organisations dont on pense qu'elles agissent avec une intention malveillante
- **Schéma d'attaque** : une description détaillée de la façon dont les utilisateurs malveillants ont tenté de compromettre des cibles spécifiques (plus communément appelé les tactiques, techniques et procédures)
- **Ensemble d'intrusions** : un résumé des comportements et des ressources des utilisateurs malveillants ayant des propriétés communes et dont on pense qu'ils sont orchestrés par une seule organisation sur de nombreux incidents

REF5961

BLOODALCHEMY, RUDEBIRD, EAGERBEE, DOWNTOWN

REF5961 est un ensemble d'intrusions qui comprend trois familles de malwares inédites découvertes et analysées par Elastic Security Labs. Ces familles de malwares cohabitaient avec des familles découvertes dans l'ensemble

d'intrusions REF2924 et ciblaient un membre du ministère des Affaires étrangères de l'ASEAN. La figure 31 décrit comment REF5961 a déployé les différents malwares, l'infrastructure associée et les mouvements latéraux.



En quoi consiste la menace ?

L'ensemble d'intrusions REF5961 est une activité qui correspond aux comportements des acteurs malveillants parrainés par l'État et/ou motivés par l'espionnage. En outre, la corrélation des flux d'exécution, des outils, de l'infrastructure et des victimes ciblées entre les multiples campagnes que nous suivons, ainsi que le consensus avec les services de renseignement tiers, confirment l'hypothèse qu'il s'agit d'un acteur lié à la Chine. EAGERBEE est une porte dérobée récemment identifiée qui charge des fonctionnalités supplémentaires à l'aide de fichiers exécutables portables téléchargés à distance et hébergés sur une infrastructure contrôlée par des utilisateurs malveillants. Cependant, sa mise en œuvre et ses pratiques de codage s'appuient sur des techniques conventionnelles simples. Lors de notre analyse d'EAGERBEE, nous avons également observé deux échantillons (auparavant non nommés) impliqués dans une campagne ciblée visant le gouvernement

mongol. Ces exemples ont été regroupés avec d'autres fichiers partagés et des métadonnées de codage.

RUDEBIRD est une porte dérobée Windows légère qui communique via HTTPS et qui permet d'effectuer des opérations de reconnaissance et d'exécution de code.

DOWNTOWN est un implant modulaire qui partage une architecture de plug-ins, présente des similitudes de code et s'aligne sur les victimes ciblées décrites en relation avec le malware SMANAGER/PHANTOMNET, qui a fait l'objet d'un rapport public.

BLOODALCHEMY est une porte dérobée x86 rédigée en C et trouvée comme shellcode injecté dans un processus bénin signé. Elle est toujours en cours de développement et comprend plusieurs modes d'exécution, mécanismes de *persistance* et options de communication.

Quelles sont les répercussions ?

Le statut d'agence diplomatique gouvernementale de la victime du REF5961 en ferait un point de départ idéal pour d'autres cibles à l'intérieur et à l'extérieur des frontières nationales de

l'agence. En outre, de multiples entités au sein de l'infrastructure de renseignement national étranger aux pouvoirs régionaux auraient des exigences de collecte qui pourraient être satisfaites directement par cette victime.

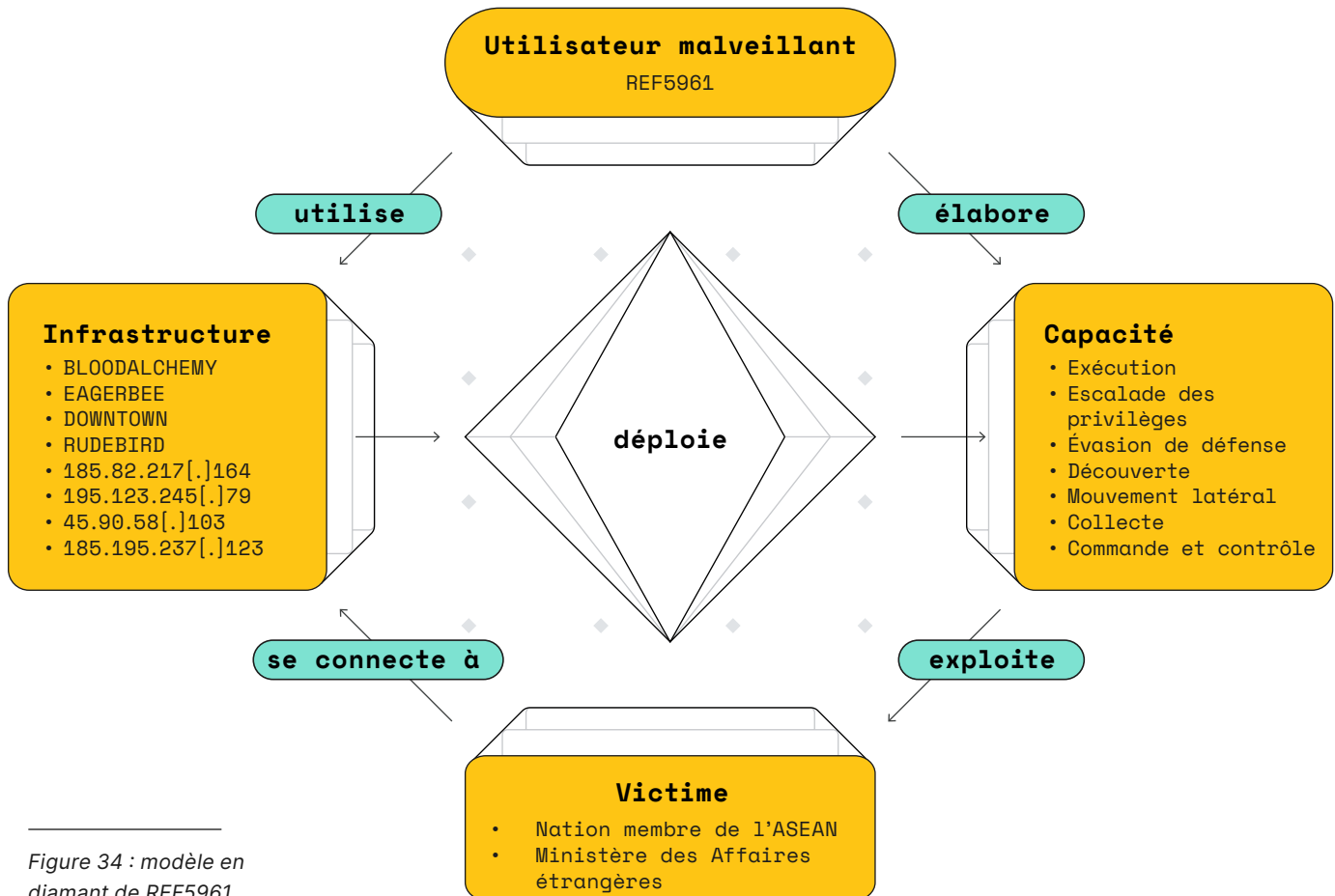


Figure 34 : modèle en diamant de REF5961

Quelle a été la réponse d'Elastic ?

Elastic fournit des détections et des préventions prêtes à l'emploi contre REF5961 dans la solution Elastic Security. De plus, Elastic a publié des règles YARA, ainsi qu'une analyse détaillée de la

campagne et du malware. Les rapports du secteur en la matière, dont la recherche publiée par Elastic, aident à atténuer cette menace. Voici un exemple de la règle YARA publiée spécifiquement pour RUDEBIRD :

```

RUDEBIRD
rule Windows_Trojan_RudeBird {
  meta:
    author = "Elastic Security"
    creation_date = "2023-05-09"
    last_modified = "2023-06-13"
    threat_name = "Windows.Trojan.RudeBird"
    license = "Elastic License v2"
    os = "windows"

  strings:
    $a1 = { 40 53 48 83 EC 20 48 8B D9 B9 D8 00 00 00 E8 FD C1 FF FF 48 8B C8 33 C0 48 85
C9 74 05 E8 3A F2 }

  condition:
    all of them
}

```

En savoir plus



Articles d'Elastic Security Labs :

- [Introducing the REF5961 intrusion set](#)
- [Disclosing the BLOODALCHEMY backdoor](#)
- [SiestaGraph: New implant uncovered in ASEAN member foreign ministry](#)
- [Update to the REF2924 intrusion set and related campaigns](#)

Entrées Malpedia :

- [BLOODALCHEMY](#)
- [EAGERBEE](#)

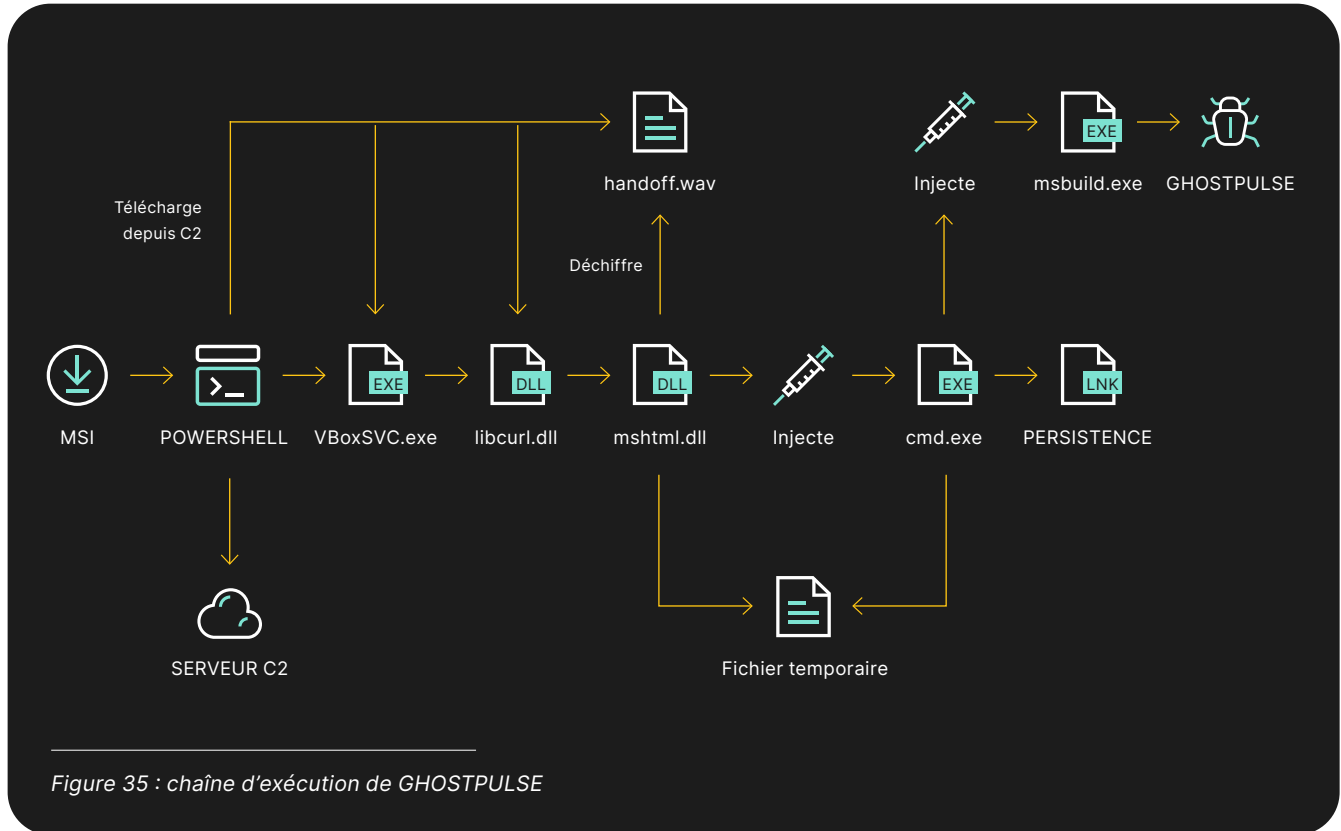
REF8207

GHOSTPULSE

En octobre 2023, Elastic Security Labs a observé une campagne visant à compromettre les utilisateurs avec des packages d'applications MSIX signés. La campagne s'est appuyée sur un programme de chargement récemment découvert que nous avons nommé GHOSTPULSE, qui déchiffre et injecte sa charge utile finale afin d'échapper à la détection.

MSIX est un format de package d'applications Windows que les développeurs peuvent utiliser

pour emballer, distribuer et installer leurs applications aux utilisateurs de Windows. Avec App Installer, les packages MSIX peuvent être installés d'un double-clic. Cela en fait une cible potentielle pour les utilisateurs malveillants qui cherchent à compromettre des victimes qui ne se doutent de rien. Cependant, MSIX nécessite l'accès à des certificats de signature de code achetés ou volés, ce qui les rend viables pour les groupes qui peuvent obtenir ces ressources.



En quoi consiste la menace ?

GHOSTPULSE est un implant malveillant en plusieurs étapes utilisé pour s'implanter, établir la *persistance*, collecter des informations sur l'hôte, puis déployer d'autres malwares. Dans un scénario d'attaque courant, les utilisateurs sont dirigés vers le téléchargement de packages MSIX malveillants par le biais de sites web compromis, de techniques d'optimisation des moteurs de recherche (SEO) ou de publicité

malveillante. Les thèmes camouflés que nous avons observés incluent des programmes d'installation pour Chrome, Brave, Edge, Grammarly et WebEx. Du point de vue de l'utilisateur, le bouton "Install" (Installer) fonctionne comme prévu. Aucune fenêtre contextuelle ni aucun avertissement ne s'affiche. Cependant, un script PowerShell est utilisé secrètement pour télécharger, déchiffrer et exécuter GHOSTPULSE sur le système.

Quelles sont les répercussions ?

Une fois que GHOSTPULSE avait terminé son flux d'exécution, des voleurs d'informations tels que SECTOPRAT, RHADAMANTHYS, VIDAR, LUMMA et NETSUPPORT ont été observés en train de charger.

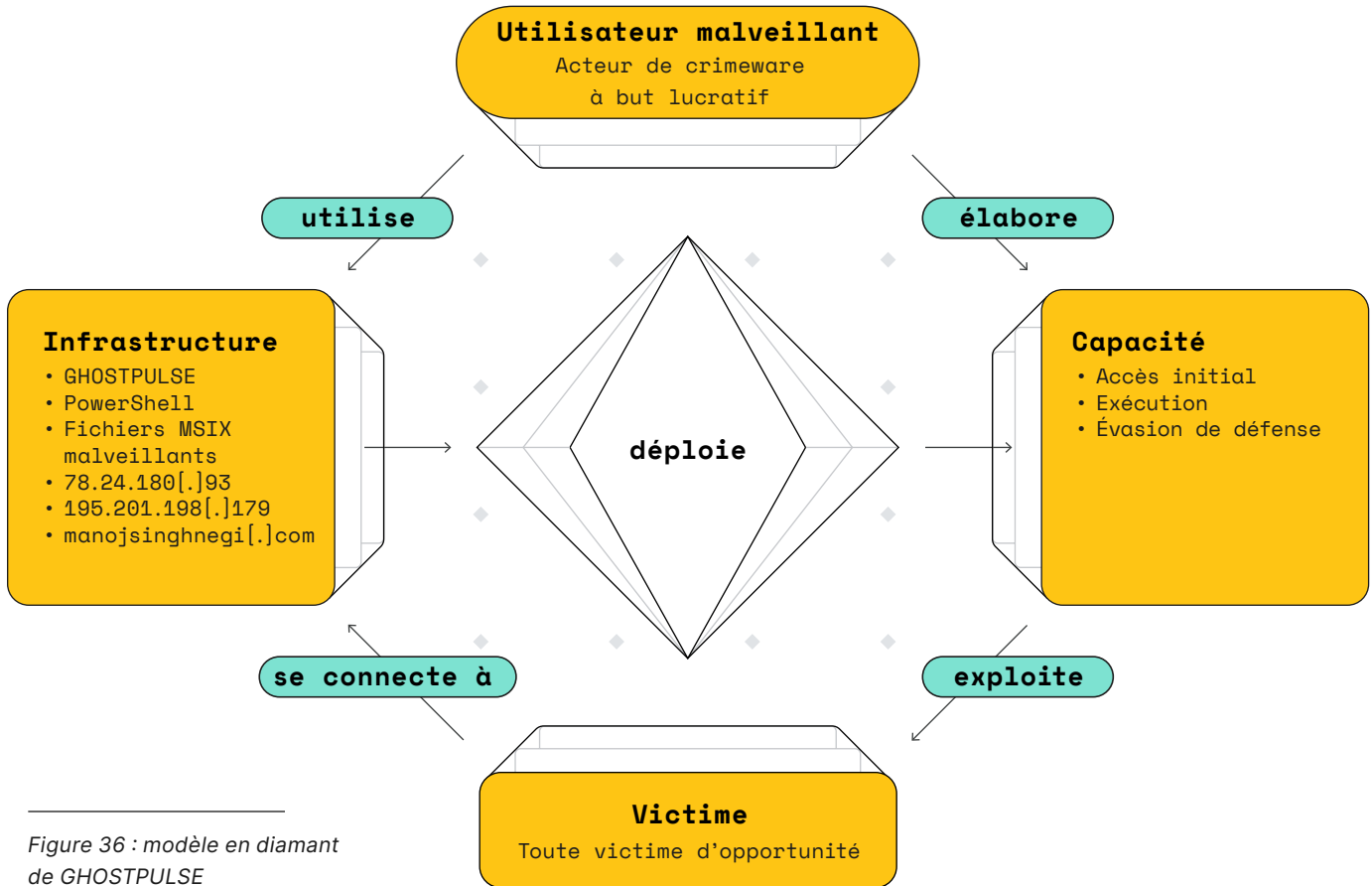


Figure 36 : modèle en diamant de GHOSTPULSE

Quelle a été la réponse d'Elastic ?

L'équipe d'Elastic Security Labs a détaillé l'architecture et l'exécution du malware, ses phases, ainsi que les tactiques et techniques observées. Pour minimiser encore l'impact, les

capacités de détection et de prévention ont été publiées et les outils d'extraction de configuration ont été partagés, ainsi que les indicateurs de compromission (IOC) des fichiers et du réseau.

En savoir plus



Article d'Elastic Security Labs :

- [GHOSTPULSE haunts victims using defense evasion bag o' tricks](#)

Entrée Malpedia :

- [GHOSTPULSE](#)

REF4578 GHOSTENGINE

En mai 2024, Elastic Security Labs a identifié REF4578, un ensemble d'intrusions décrivant plusieurs modules malveillants et exploitant des pilotes vulnérables pour désactiver des solutions de sécurité connues (EDR) pour le cryptomining.

Dans cette recherche, nous avons partagé des détails sur GHOSTENGINE, une porte dérobée précédemment non documentée utilisée pour établir la *persistance* et exécuter un mineur de cryptomonnaie.

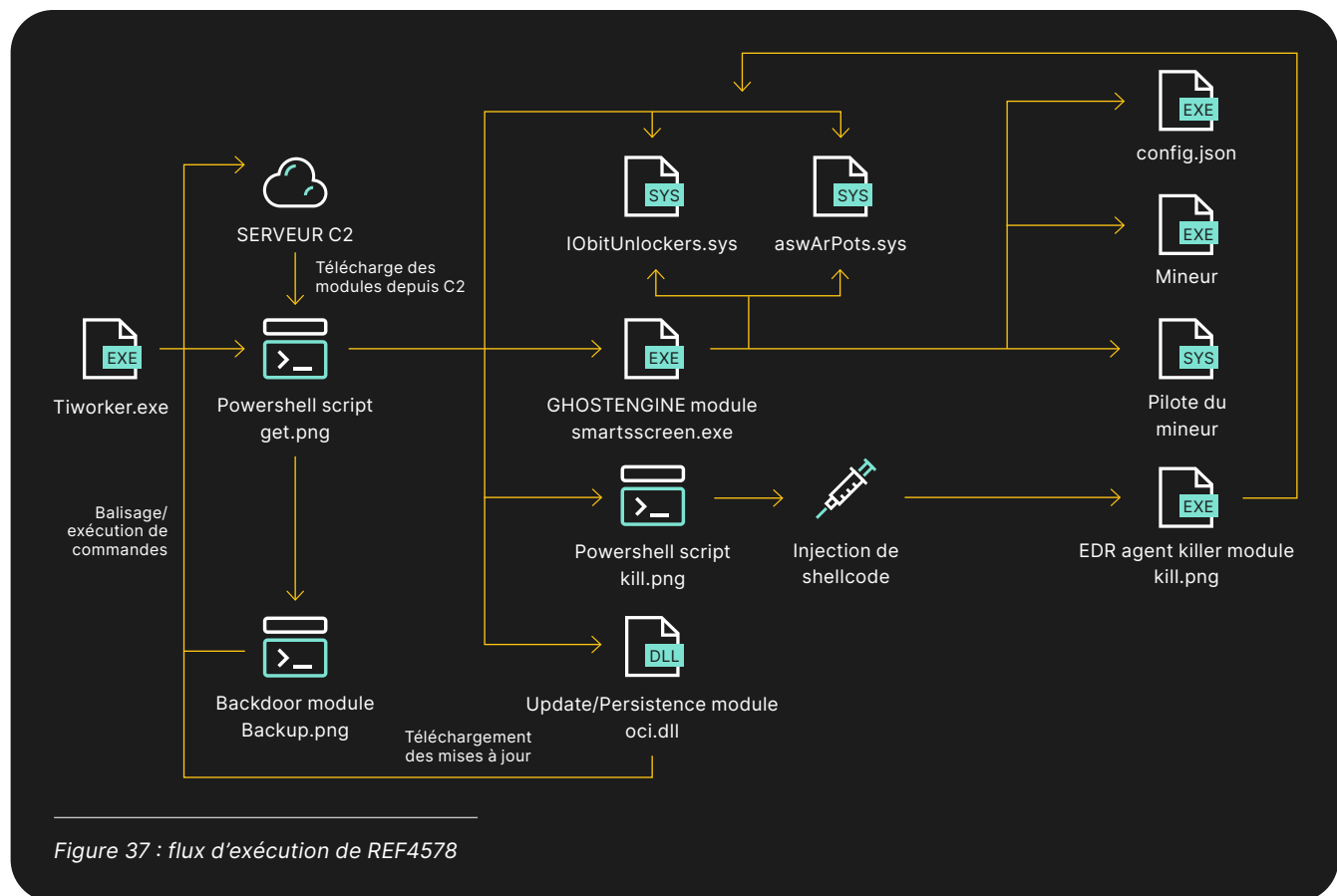


Figure 37 : flux d'exécution de REF4578

En quoi consiste la menace ?

REF4578 est un ensemble d'intrusions qui décrit une nouvelle porte dérobée nommée GHOSTENGINE. Les responsables de la campagne ont intégré de nombreux mécanismes d'urgence et de sauvegarde, ont exploité des pilotes vulnérables

(BYOVD) pour neutraliser et supprimer des agents EDR connus, et ont exécuté la campagne avec une complexité peu commune. Ces éléments suggèrent une intention de la part d'un opérateur qui privilégie les mineurs fiables.

Quelles sont les répercussions ?

L'acteur malveillant a pu désactiver tous les agents EDR actifs, charger des mineurs de cryptomonnaie (le programme de minage client XMRig a été observé) et maintenir la *persistance*

et le *logiciel d'accès à distance* en utilisant le service de transactions distribuées de Microsoft pour charger une bibliothèque de liens dynamiques fantôme afin d'exécuter un script PowerShell.

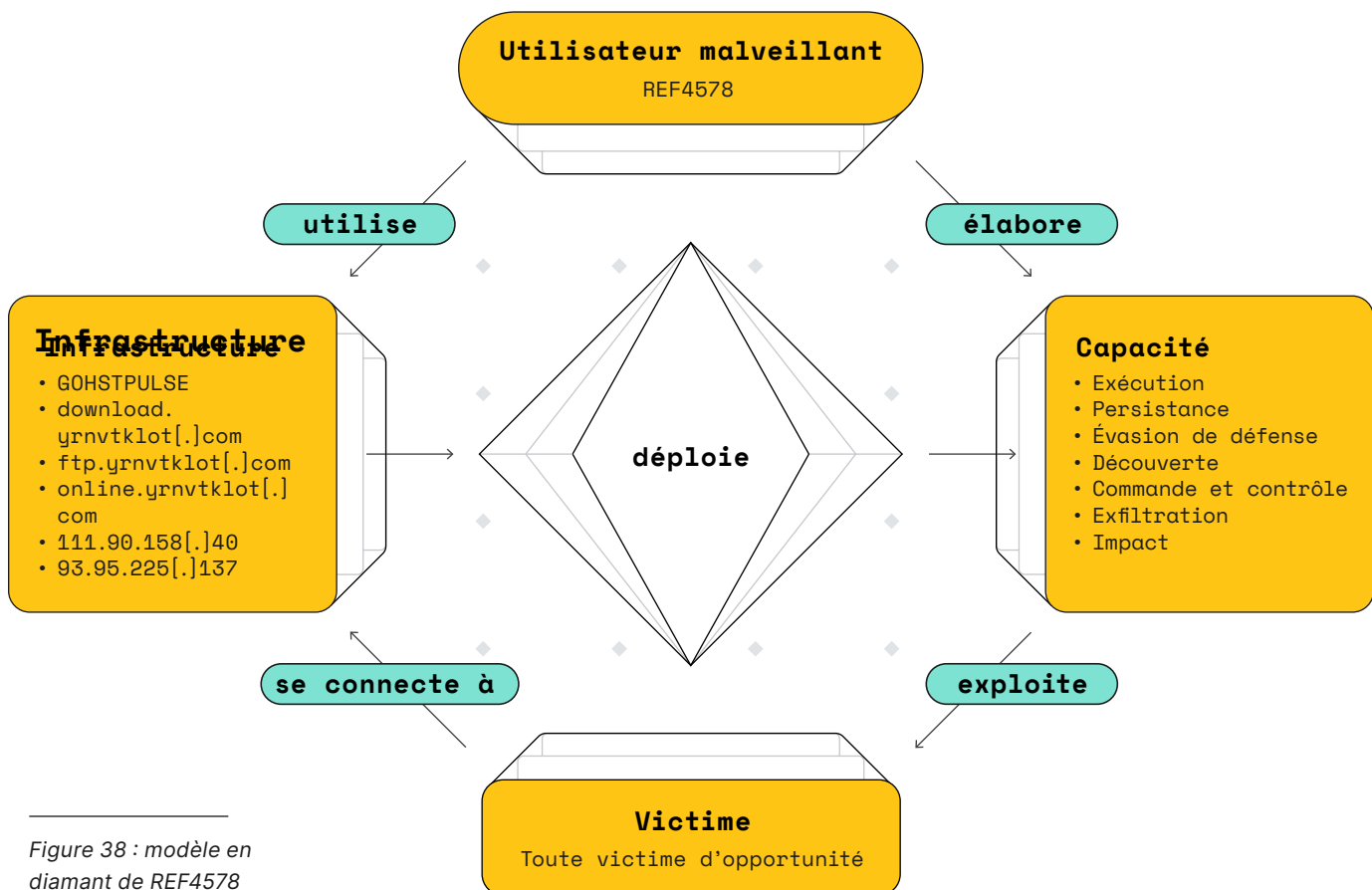


Figure 38 : modèle en diamant de REF4578

Quelle a été la réponse d'Elastic ?

Elastic Security Labs a publié un produit d'analyse mettant en évidence le flux d'exécution de REF4578 et le contrôleur EDR, la *persistance* et les mécanismes d'*accès à distance* exploités par l'ensemble d'intrusions de REF4578 et mettant en correspondance ces observations avec le framework MITRE ATT&CK.

Pour comprendre l'ampleur de la campagne, la configuration de XMRig, les identifiants des portefeuilles Monero et le solde des portefeuilles ont été partagés. Les règles YARA pour les malwares observés dans l'ensemble d'intrusions ont également été publiées, à savoir les règles de prévention des points de terminaison et les indicateurs atomiques de l'hôte et du réseau.

```

rule Windows_Trojan_GhostEngine {
  meta:
    author = "Elastic Security"
    creation_date = "2024-05-07"
    last_modified = "2024-05-13"
    threat_name = "Windows.Trojan.GhostEngine"
    license = "Elastic License v2"
    os = "windows"

  strings:
    $str0 = "\\.\IOBitUnlockerDevice"
    $str1 = "C:\\Windows\\Fonts\\taskhostw.exe"
    $str2 = "C:\\Windows\\Fonts\\config.json"
    $str3 = "/drives/kill.png"
    $str4 = "C:\\Windows\\Fonts\\WinRing0x64.sys"
    $str5 = "C:\\Windows\\Fonts\\smartsscreen.exe"
    $binary0 = { 89 C2 C1 E8 1F C1 E0 1F 85 C0 0F 84 74 01 00 00 D1 E2 89 CB C1 E9 1F 09 D1
D1 E3 C1 EB 1F 89 CA D1 E1 09 D9 89 CB 81 C1 80 7F B1 D7 C1 EA 1F 81 C3 80 7F B1 D7 83 D2 0D 81
C1 00 09 6E 88 89 4C 24 20 83 D2 F1 89 54 24 24 }
    $binary1 = { 83 F9 06 0F ?? ?? ?? ?? ?? 8B 10 81 FA 78 38 36 5F 0F 85 ?? ?? ?? ?? 0F B7
50 04 66 81 FA 36 34 74 ?? E9 ?? ?? 00 00 C7 04 24 00 E4 0B 54 C7 44 24 04 02 00 00 00 }

  condition:
    3 of ($str*) or 1 of ($binary*)
}

```

En savoir plus



Article d'Elastic Security Labs :

- [Recherche initiale exposant JOKERSPY](#)

Entrée Malpedia :

- [JOKERSPY](#)

REF7001

KANDYKORN

En octobre 2023, Elastic Security Labs a révélé une intrusion inédite ciblant les ingénieurs blockchain d'une plateforme d'échange de cryptomonnaies. L'intrusion s'est appuyée sur des fonctionnalités personnalisées et open source pour l'accès *initial* et la post-exploitation.

L'intrusion a été découverte lors de l'analyse des tentatives de chargement réflexif d'un binaire en mémoire sur un point de terminaison macOS. L'intrusion a été attribuée à une application Python se faisant passer pour un robot d'arbitrage de

cryptomonnaies diffusé par message direct sur un serveur Discord public basé sur la blockchain. Nous attribuons cette activité à la République

populaire démocratique de Corée (RPDC) et reconnaissons des chevauchements avec les rapports publics.

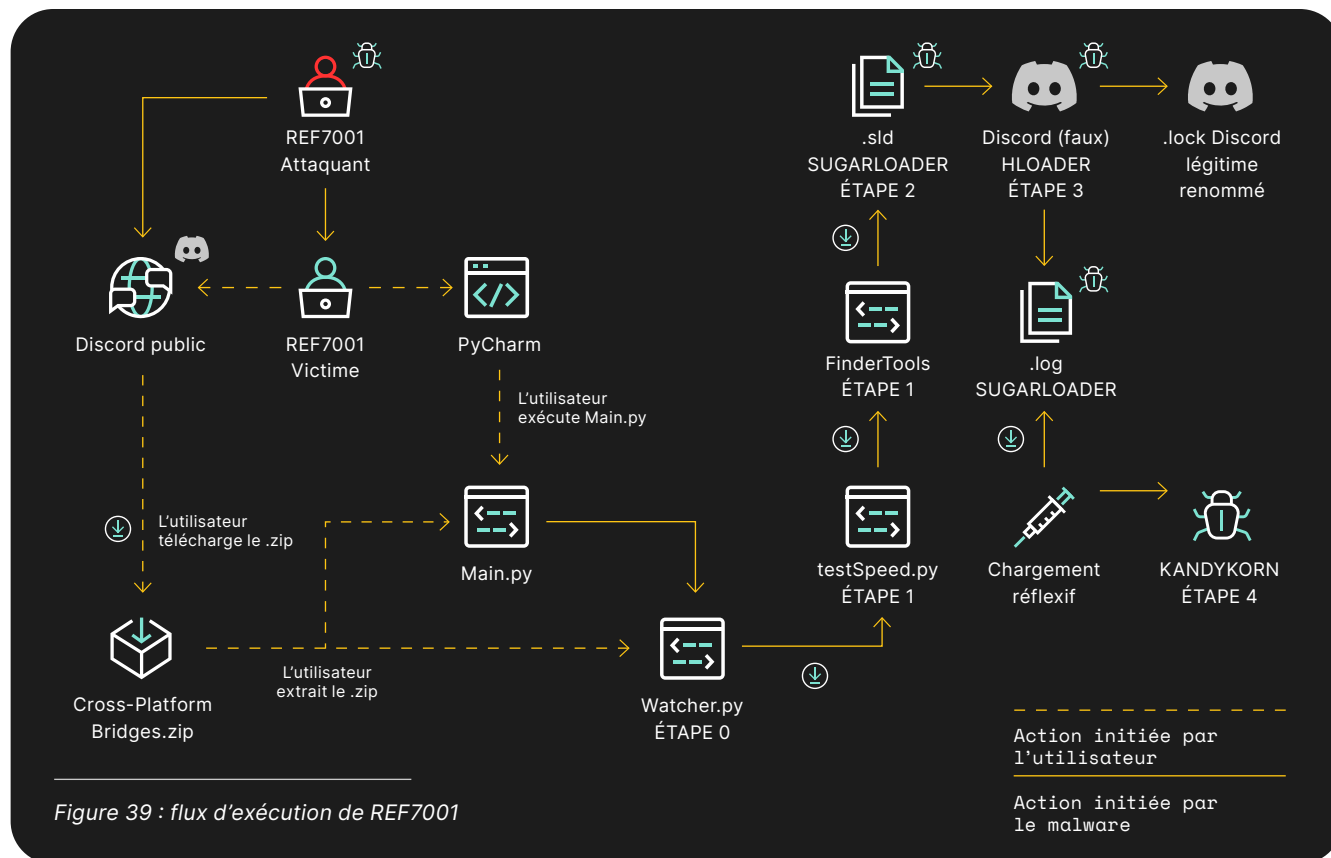


Figure 39 : flux d'exécution de REF7001

En quoi consiste la menace ?

Les acteurs malveillants ont attiré les ingénieurs blockchain avec une application Python pour obtenir un accès initial à l'environnement. Cette intrusion comportait plusieurs étapes complexes qui utilisaient chacune des contre-mesures délibérées d'évasion de défense. L'ensemble

d'intrusions a été observé sur un système macOS, sur lequel un utilisateur malveillant a tenté de charger des binaires en mémoire, ce qui est atypique des intrusions macOS. L'étape finale consistait à charger KANDYKORN, un outil complet d'accès à distance et d'exfiltration.

Quelles sont les répercussions ?

REF7001 a exposé une technique opérationnelle et tactique d'ingénierie sociale et de chargement de binaires directement en mémoire sur les

systèmes macOS. La RPDC utilise couramment l'ingénierie sociale, ciblant les ressources humaines et maintenant les ingénieurs, pour obtenir un

accès initial dans un environnement contesté. En associant cette technique à un malware macOS inédit, les acteurs malveillants ont pu accéder à des hôtes d'ingénieurs susceptibles de leur donner accès à des données sensibles sur les échanges de cryptomonnaies, à la propriété intellectuelle ou

à des chaînes d'approvisionnement. La RPDC a démontré des solutions créatives pour faire face aux sanctions, notamment le vol de cryptomonnaies, les escroqueries de travailleurs informatiques et la fraude aux transactions de la Society for Worldwide Interbank Financial Telecommunication (SWIFT).

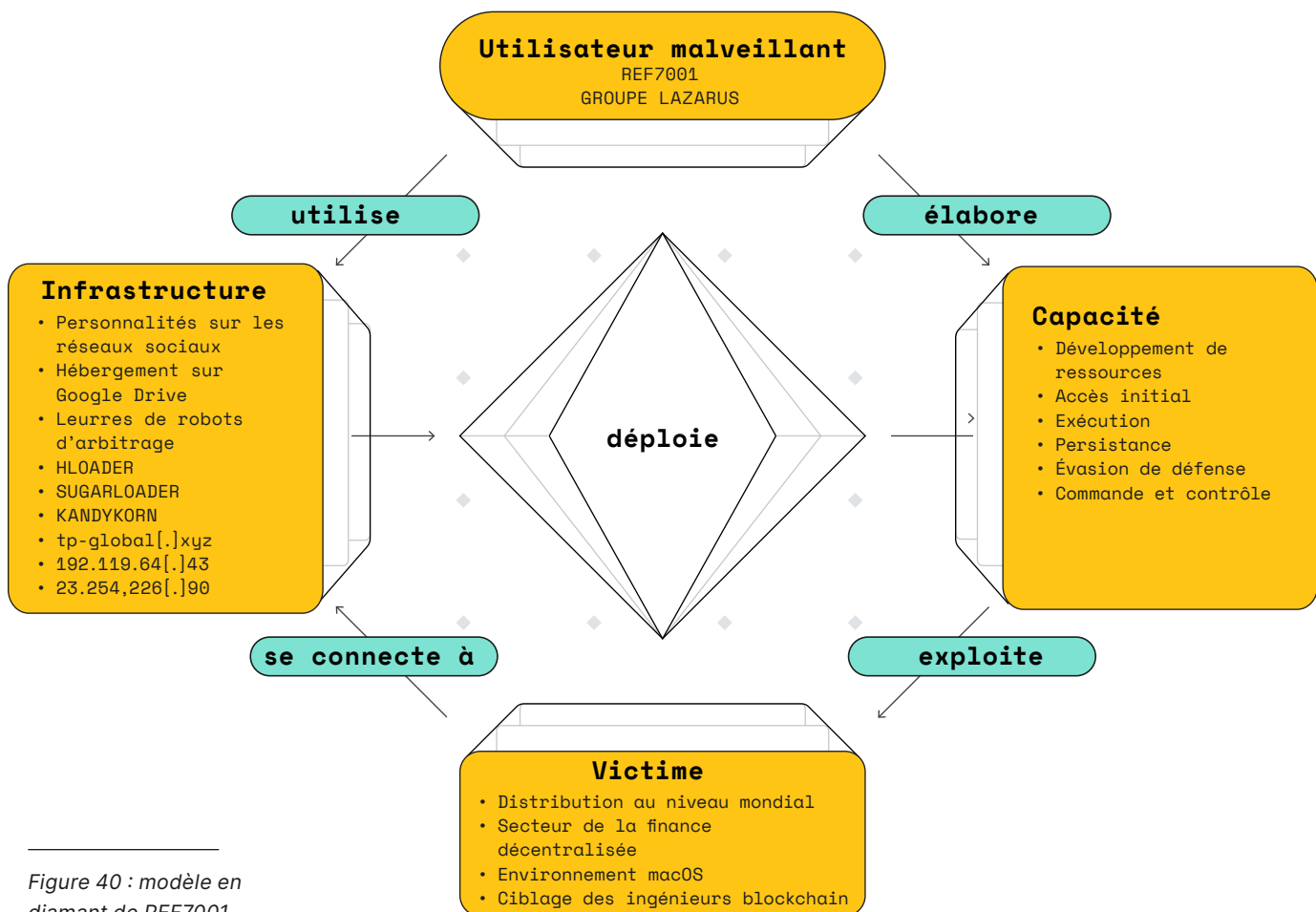


Figure 40 : modèle en diamant de REF7001

Quelle a été la réponse d'Elastic ?

Elastic a publié une analyse détaillée de la campagne et des malwares, des signatures YARA et des protections aux points de terminaison permettant de détecter et de prévenir les malwares de cet ensemble d'intrusions. En outre, nous avons publié tous les indicateurs atomiques observés dans cet ensemble.

Nos recherches sur REF7001 ont abouti à trois règles YARA axées sur l'identification des différents malwares observés dans cet ensemble d'intrusions, ainsi qu'à huit requêtes de détection en [langage de requête d'événement](#) (EQL) qui identifient les éléments comportementaux et techniques de cette campagne.

Ci-dessous se trouve un exemple de requête EQL créée pour KANDYKORN. Plus précisément, elle peut être utilisée pour identifier le moment où un exécutable masqué crée puis supprime immédiatement un fichier dans un répertoire temporaire :

```
sequence by process.entity_id, file.path with maxspan=30s
[file where event.action != "deletion" and process.name : "*" and
file.path : ("/private/tmp/*", "/tmp/*", "/var/tmp/*")]
[file where event.action == "deletion" and process.name: "*" and
file.path : ("/private/tmp/*", "/tmp/*", "/var/tmp/*")]
```

En savoir plus



Article d'Elastic Security Labs :

- [Elastic catches DPRK passing out KANDYKORN](#)

Entrées Malpedia :

- [KANDYKORN](#)
- [HLOADER](#)
- [SUGARLOADER](#)

REF6127

WARMCOOKIE

En juin 2024, Elastic Security Labs a observé une vague de campagnes par e-mail sur le thème du recrutement ciblant les environnements en déployant une nouvelle porte dérobée que nous avons nommée WARMCOOKIE. Bien que certaines fonctionnalités soient similaires aux variantes

précédemment signalées, comme la mise en œuvre du brouillage de chaînes, WARMCOOKIE contient des fonctionnalités différentes. Notre équipe a vu cette menace se propager quotidiennement avec l'utilisation des thèmes du recrutement et de l'emploi ciblant des individus.

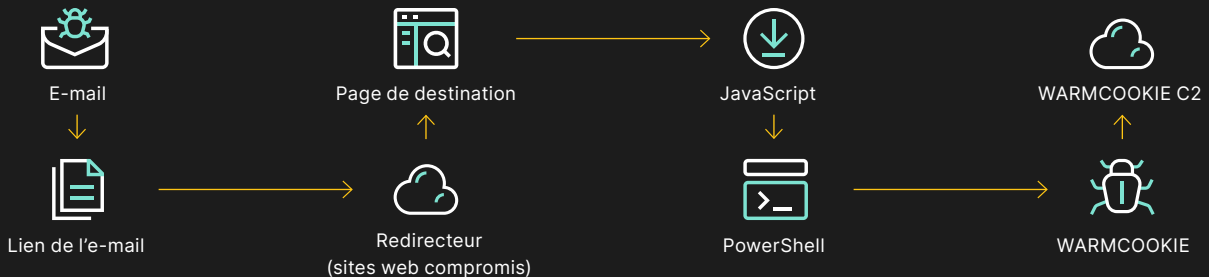


Figure 41 : flux d'exécution de REF6127

En quoi consiste la menace ?

WARMCOOKIE est un premier outil de porte dérobée utilisé pour identifier les réseaux des victimes et déployer des charges utiles supplémentaires. Chaque échantillon est compilé avec une adresse IP C2 codée en dur et une clé RC4.

Quelles sont les répercussions ?

WARMCOOKIE propose sept gestionnaires de commandes permettant aux acteurs malveillants d'invoquer différentes fonctions, notamment la récupération d'informations sur les victimes, l'enregistrement de captures d'écran, le lancement

de charges utiles supplémentaires, etc. Les fonctionnalités proposées sont relativement simples, permettant aux groupes de menaces qui ont besoin d'une porte dérobée légère de monitorer les victimes et de déployer d'autres charges utiles nuisibles telles que des ransomwares.

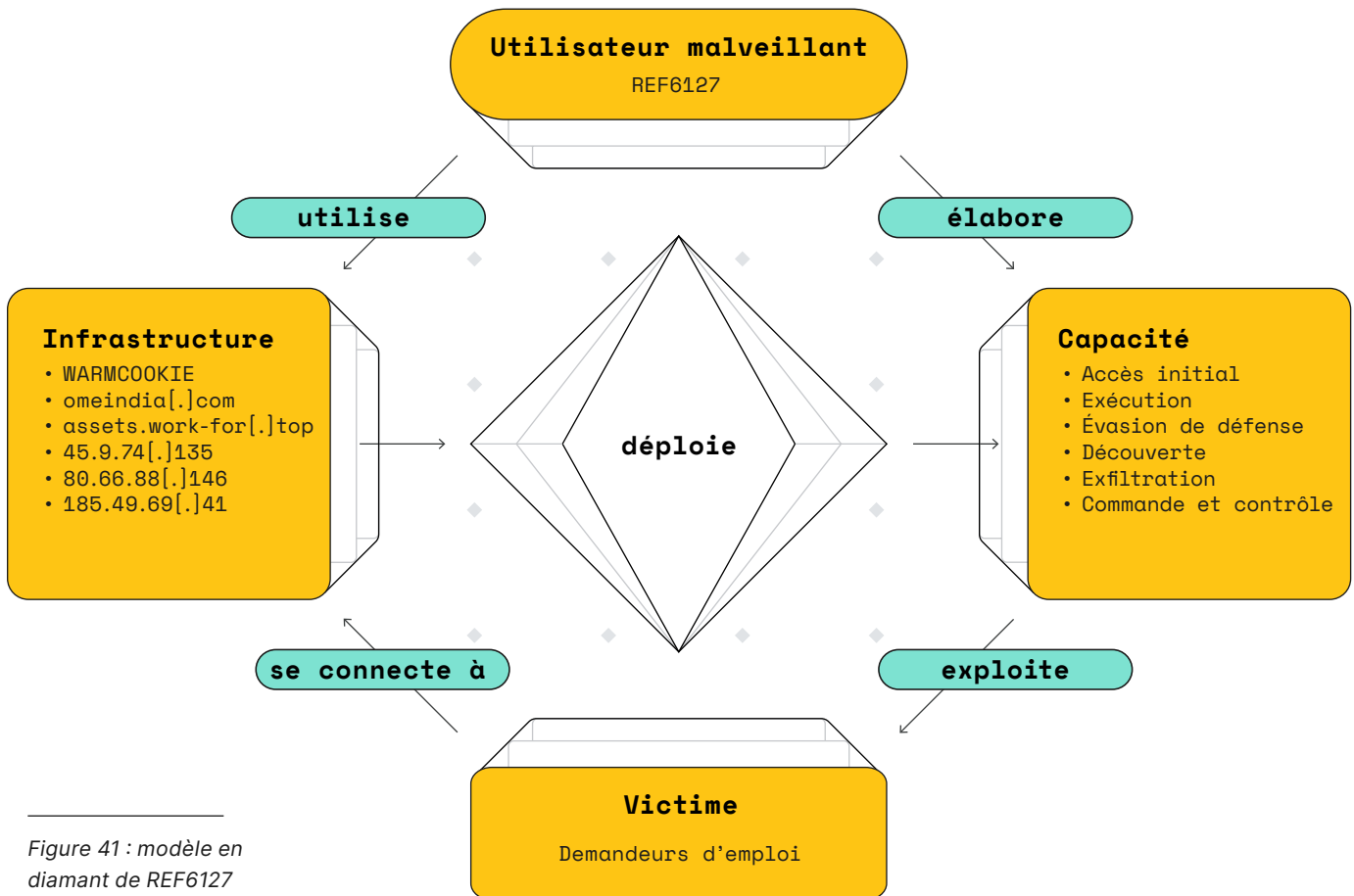


Figure 41 : modèle en diamant de REF6127

Quelle a été la réponse d'Elastic ?

Elastic Security Labs a publié une analyse détaillée de la campagne et des malwares, une signature

YARA et des protections aux points de terminaison permettant de détecter et de prévenir les malwares

de cet ensemble d'intrusions. Nous avons mis en correspondance cet ensemble d'intrusions avec le framework MITRE ATT&CK et publié tous

les indicateurs atomiques observés dans cet ensemble. Ci-dessous se trouve la signature YARA pour détecter WARMCOOKIE :

```
rule Windows_Trojan_WarmCookie_7d32fa90 {
  meta:
    author = "Elastic Security"
    creation_date = "2024-04-29"
    last_modified = "2024-05-08"
    os = "Windows"
    arch = "x86"
    threat_name = "Windows.Trojan.WarmCookie"
    license = "Elastic License v2"

  strings:
    $seq_checksum = { 45 8D 5D ?? 45 33 C0 41 83 E3 ?? 49 8D 4E ?? 44 03 DB 41 8D 53 ?? }
    $seq_string_decrypt = { 8B 69 04 48 8D 79 08 8B 31 89 6C 24 ?? 48 8D 4E ?? E8 }
    $seq_filesearch = { 48 81 EC 58 02 00 00 48 8B 05 82 0A 02 00 48 33 C4 48 89 84 24 40 02
00 00 45 33 C9 48 8D 44 24 30 45 33 C0 48 89 44 24 20 33 C9 41 8D 51 1A FF 15 83 4D 01 00 85 C0
78 22 48 8D 4C 24 30 E8 1D }
    $seq_registry = { 48 81 EC 80 02 00 00 48 8B 05 F7 09 02 00 48 33 C4 48 89 84 24 70 02
00 00 4C 89 B4 24 98 02 00 00 48 8D 0D 4D CA 01 00 45 33 F6 41 8B FE E8 02 4F 00 00 48 8B E8 41
B9 08 01 00 00 48 8D 44 24 }
    $plain_str1 = "release.dll" ascii fullword
    $plain_str2 = "\"Main Invoked.\"" ascii fullword
    $plain_str3 = "\"Main Returned.\"" ascii fullword
    $decrypt_str1 = "ERROR: Cannot write file" wide fullword
    $decrypt_str2 = "OK (No output data)" wide fullword
    $decrypt_str3 = "OK (See 'Files' tab)" wide fullword
    $decrypt_str4 = "cmd.exe /c %ls" wide fullword
    $decrypt_str5 = "Cookie:" wide fullword
    $decrypt_str6 = "%ls\\*.*" wide fullword

  condition:
    (3 of ($plain*)) or (2 of ($seq*)) or 4 of ($decrypt*)
}
```

En savoir plus



Article d'Elastic Security Labs :

- [Dipping into Danger: The WARMCOOKIE backdoor](#)

Entrée Malpedia :

- [WARMCOOKIE](#)

Réponses aux prévisions de 2023

Chaque année, Elastic Security Labs propose plusieurs prévisions pour l'année à venir, en fonction des tendances, des corrélations et de notre visibilité sur le paysage dynamique des menaces mondiales. Conformément à l'engagement plus large d'Elastic en faveur de la transparence, nous aimerions prendre le temps de réfléchir aux prévisions de l'année dernière.

Prévision 1

L'évasion de défense va rester l'investissement principal, tandis que la falsification va supplanter le camouflage

Verdict : **nous avions raison.**

Notre analyse des données de cette année a révélé que la catégorie de tactique numéro un pour le point de terminaison était l'*évasion de défense*, et que la *falsification* battait le *camouflage* d'environ 1 %. L'*évasion de défense* a également joué un rôle important pour les fournisseurs de services cloud, bien qu'à un moindre degré. Nous avons également noté que les capacités d'*évasion de défense* sont de plus en plus courantes dans les malwares ciblés et non ciblés, et qu'elles constituent une priorité évidente pour les chercheurs en sécurité offensive. Plus largement, les entreprises devraient reconnaître deux phénomènes :

- Les utilisateurs malveillants sont à la fois plus conscients et plus susceptibles de recourir à l'*évasion de défense*, y compris la falsification.

- Les outils de sécurité, en particulier les capteurs capables d'atténuer les comportements, sont suffisamment efficaces pour que les *évasions* ne soient plus facultatives mais nécessaires.

Les articles suivants d'Elastic Security Labs décrivent des *évasions de défense* identifiées :

- [GHOSTPULSE haunts victims with defense evasion bag 'o tricks](#)
- [GrimResource - Console de gestion Microsoft pour l'accès initial et l'évasion](#)
- [Démantèlement du contrôle intelligent des applications](#)

Prévision 2

Le modèle malware-as-a-service (MaaS) va gagner en popularité.

Verdict : nous avons en grande partie raison.

En particulier, l'évolution de l'écosystème de la cybercriminalité a incité les groupes de menaces à s'abstraire des intrusions et de l'intérêt qu'elles suscitent auprès des pouvoirs publics. En conséquence, on assiste à une explosion des menaces non ou peu expérimentées qui utilisent des outils et des stratégies en tant que proxys. Cela réduit dans une certaine mesure la barrière à l'entrée, bien que les entreprises doivent tenir compte du fait que les proxys qui n'ont pas les compétences et l'adaptabilité des menaces matures peuvent être plus faciles à influencer

que ceux qu'ils représentent. Cependant, il convient également de noter que cela interfère considérablement avec l'attribution et le fait de concentrer les pouvoirs en place sur les coalitions qui luttent contre la criminalité.

Les articles suivants d'Elastic Security Labs décrivent les familles de malwares utilisées dans un contexte MaaS :

- [PIKABOT, je vous choisis !](#)
- [Globally Distributed Stealers](#)

Prévision 3

Les utilisateurs malveillants se reposeront de plus en plus sur les communautés open source pour les implants, les outils et les infrastructures

Verdict : nous avons raison.

Dans presque toutes les intrusions observées par Elastic Security Labs cette année, les outils et fonctionnalités open source ont joué un rôle central. Tunnelers et proxys réseau, outils de collecte d'identifiants, capacités d'escalade des privilèges, scripts, webshells : il s'agit d'un pari très sûr pour l'avenir, et nous ne nous attendons pas à ce que cela change. Cependant, il n'est pas non plus pratique pour les entreprises de trop se concentrer sur le suivi des référentiels publics pour de nouveaux types d'outils ou de malwares. Pour la plupart des organisations touchées par ces intrusions, la prise de conscience et le contrôle de l'environnement auraient fait la plus grande différence : segmentation des réseaux, suivi des

processus exécutant du code non sauvegardé, réglementation de l'accès aux systèmes sensibles et suivi des nouveaux mécanismes de *persistance*.

Les articles suivants d'Elastic Security Labs font état des fonctionnalités open source utilisées lors d'intrusions :

- [Unmasking a Financial Services Intrusion: REF0657](#)
- [Elastic catches the DPRK passing out KANDYKORN](#)

Prévision 4

L'exposition des identifiants du cloud deviendra une source principale des incidents exposant des données

Verdict : nous avions raison.

Pour chaque fournisseur de services cloud dont nous avons reçu des données, l'accès aux identifiants était la catégorie de tactique numéro un. Comme indiqué précédemment, il s'agit d'une fatalité, car l'accès aux identifiants est la passerelle vers tous les accès non anonymes des fournisseurs de services cloud. Avec des identifiants valides volés, les utilisateurs malveillants peuvent facilement accéder à des services tels que la messagerie électronique et

le stockage hébergé dans le cloud. Nous avons observé cette activité régulièrement et identifié quelques recommandations de posture clés pour l'année prochaine.

L'article suivant d'Elastic Security Labs décrit plusieurs façons dont des identifiants volés peuvent être obtenus pour compromettre les fournisseurs de services cloud :

- [Protecting your devices from information theft](#)

Prévision 5

Les pods Kubernetes ayant des privilèges trop élevés vont aggraver les dommages dus aux vulnérabilités des conteneurs

Verdict : nous avions tort.

Nous nous attendions à une relation beaucoup plus claire entre Kubernetes, les privilèges trop élevés et les vulnérabilités non corrigées existantes. En raison de l'utilisation d'identifiants valides, l'exploitation était un phénomène beaucoup moins courant. Il était également beaucoup plus difficile de faire la distinction, étant donné

que l'espace de traitement pour de nombreux conteneurs est constant pendant toute la durée de vie du conteneur, tandis que les groupes d'accès utilisateur peuvent changer tous les mois, voire toutes les semaines. Les problèmes d'accès aux identifiants sont susceptibles de perdurer.

Prévisions et recommandations

Les chercheurs ont examiné les données de télémétrie mondiale d'Elastic pour tenter de prévoir ce que nous pourrions observer au cours de l'année à venir. Dans chaque cas, nous essayons d'associer une recommandation spécifique et réalisable afin que les organisations qui partagent nos évaluations puissent prendre des décisions.

Prévision 1

Les utilisateurs malveillants vont redoubler d'efforts en matière d'évasion de défense, en particulier en ce qui concerne les techniques qui entravent la visibilité des capteurs

Les signaux d'évasion de défense les plus courants ont été observés sur les systèmes Windows, impliquant généralement un trio de techniques : l'injection de processus, l'exécution de proxy binaire du système et la dégradation de défenses. Collectivement, ces techniques peuvent être utilisées pour s'implanter avec des privilèges suffisants afin de falsifier ou d'aveugler les outils avant que les données ne puissent être envoyées à des back-ends de type SIEM.

Recommandation :

Il n'existe pas de solution unique pour cette méthodologie complexe, mais plusieurs d'entre elles se sont révélées efficaces :

- monitorer le code non sauvegardé injecté dans les processus privilégiés ;
- monitorer et limiter l'utilisation des proxys binaires intégrés (mshta, RunDLL, etc.) ;

- monitorer les changements dans la visibilité des points de terminaison (les règles de diagnostic sont une option).

Il est important de noter qu'aucun de ces objectifs ne peut être atteint de manière satisfaisante sans le déploiement d'agents de points de terminaison interactifs avant la découverte d'une activité malveillante, qui ne seront pas efficaces s'ils sont mal configurés. Les chercheurs ont fréquemment observé des entreprises au sein desquelles les administrateurs n'ont pas activé les mesures d'atténuation sous licence, ce qui a entraîné des résultats indésirables.

Prévision 2

La suppression des logs constituera toujours une méthode simple pour interférer avec la visibilité de l'infrastructure des conteneurs et des serveurs

De nombreuses entreprises s'appuient encore sur des approches centrées sur la visibilité pour détecter les menaces, plutôt que sur les fonctionnalités interactives recommandées précédemment. Pour ces organisations, la perte de logs peut s'avérer un obstacle difficile à surmonter. Nous avons régulièrement observé la suppression de logs dans des environnements de conteneurs et de serveurs dans lesquels il s'agissait de la principale ou de l'unique source de données sur les menaces. En raison des délais nécessaires à la collecte, à l'analyse et à la réponse à cette dynamique, les organisations n'ont pas été en mesure de contrôler efficacement l'environnement.

Cette prévision a été observée de manière cohérente sur l'ensemble des systèmes des entreprises, sans se limiter aux postes de travail, aux serveurs, aux conteneurs ou aux systèmes de stockage.

Recommandation :

Dans l'idéal, les organisations empêcheront les personnes non autorisées d'accéder aux systèmes en leur laissant la possibilité de supprimer ces logs nécessaires. Les entreprises doivent savoir que chaque système d'exploitation propose des fonctionnalités différentes à cet égard, et que certains sont peut-être plus robustes que d'autres.

Prévision 3

Les identifiants exposés entraîneront de plus en plus d'expositions de données ou d'accès non autorisés, en grande partie à cause des brokers d'accès et de l'écosystème des voleurs d'informations

Au cours de plusieurs intrusions de grande envergure cette année, les chercheurs ont observé que les utilisateurs malveillants apportaient des identifiants volés provenant de l'environnement. Dans la majorité de ces cas, l'environnement contenait également des preuves de voleurs d'informations antérieurs ou d'éléments de portes dérobées. Il peut être très difficile de déterminer quels identifiants ont été compromis après un certain temps, mais en règle générale, il convient de changer les identifiants de tous les utilisateurs du système lorsqu'un système a été compromis.

Recommandation :

Changez les identifiants des comptes exposés et investissez dans des workflows rapides qui soutiennent les objectifs de réponse aux violations, comme la réinitialisation des comptes. L'analyse du comportement des utilisateurs et des entités (UEBA) est une catégorie de technologies qui peut aider à identifier les comptes compromis, et le suivi des comptes utilisés dans les attaques par *force brute* (très courantes pour cibler les fournisseurs de services cloud) peut aider dans les cas où les preuves ont été modifiées ou supprimées.

Prévision 4

La posture permissive des ressources des fournisseurs de services cloud contribuera à l'exposition ou à l'altération des données à l'avenir

Nous avons observé que ces paramètres de posture étaient systématiquement mal configurés chez tous les fournisseurs, de sorte qu'il est difficile de déterminer une cause première unique. D'une manière ou d'une autre, les utilisateurs ont mal configuré les mêmes fonctionnalités de tous les fournisseurs de services cloud :

- les politiques d'accès permissives autorisaient les connexions de n'importe où ;
- les politiques de stockage permissives autorisaient les opérations sur les fichiers à partir de comptes de toutes sortes ;
- les politiques de traitement des données ou les exigences en matière de chiffrement étaient peu strictes.

Les entreprises qui cherchent à trouver un équilibre entre la facilité d'utilisation et les frais généraux liés à la sécurisation des ressources critiques peuvent avoir du mal à donner la priorité à une posture agressive, ou à le faire de manière cohérente.

Dans de nombreux cas, les audits et les conseils sont bien compris et largement disponibles sans frais. Pour cette raison, il semble plus probable qu'il s'agisse d'un problème culturel ou de perception que d'un problème technique spécifique.

Recommandation :

Envisagez d'utiliser le processus de référence du CIS pour identifier les paramètres qui nécessitent plus d'attention dans votre environnement. Une fois que le score de posture du CIS aura atteint 100, assurez-vous que votre équipe connaît bien les techniques d'intrusion basées sur le cloud les plus courantes. Le suivi à partir de cet état de base devrait permettre d'améliorer la vitesse de détection des menaces tout en renforçant l'environnement contre les menaces futures.

Prévision 5

L'adoption et l'innovation de l'intelligence artificielle générative entraîneront de nouvelles formes de collecte de données télémétriques et permettront d'identifier de nouvelles menaces existantes

De l'authentification des reproductions d'œuvres d'art à l'analyse des propriétés malveillantes d'une archive ZIP, les technologies d'IA générative sont susceptibles d'avoir un impact durable sur le fonctionnement des entreprises. Cependant, les vulnérabilités liées à la mise en œuvre de ces modèles peuvent entraîner l'exposition des données, l'exploitation du système ou l'empoisonnement, en particulier d'une manière

qui peut être difficile à découvrir. Les utilisateurs malveillants peuvent découvrir un nouveau moyen d'extraire des informations médicales confidentielles à partir d'un message relatif à la santé, ou demander à un modèle hébergé de prendre des mesures perturbatrices, et sont probablement en train de rechercher des méthodes pour y parvenir.

Nous ne savons pas exactement quelles seront ces nouvelles menaces, mais nous savons qu'il sera plus facile de les identifier avec plus de données. C'est l'une des raisons pour lesquelles Elastic continue d'investir dans les outils de télémétrie pour ces modèles.

Prévision 6

Les fournisseurs de services cloud amélioreront les paramètres de sécurité par défaut

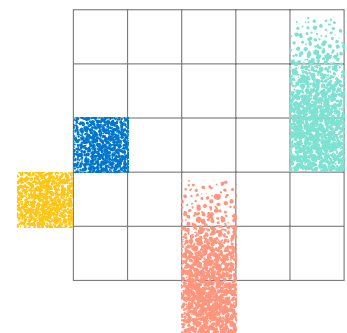
L'adoption généralisée de l'évaluation comparative du cloud basée sur des normes de sécurité a mis en évidence un domaine à risque : les contrôles de sécurité par défaut non sécurisés mis en œuvre par les fournisseurs cloud. Lorsque l'on examine les menaces les plus courantes pour les plateformes hébergées dans le cloud, ces paramètres par défaut non sécurisés constituent un facteur important de réduction des risques. Imposer l'authentification multi-facteurs pour neutraliser le risque de vol d'identifiants en est un exemple. Une autre approche consisterait à segmenter l'accès au stockage, en le limitant à des comptes sur lesquels l'authentification multi-facteurs est activée au sein de groupes spécifiques, ce qui limiterait encore l'impact potentiel de ces menaces. Nous prévoyons que les fournisseurs cloud répondront à ces risques en mettant en œuvre de meilleurs contrôles standard pour les utilisateurs à mesure qu'ils adoptent de nouvelles fonctionnalités.

Recommandation :

Les modèles de risques basés sur FAIR sont un moyen pour les entreprises de déterminer si une fonctionnalité d'IA générative augmente ou diminue le risque organisationnel. Des frameworks tels que le [top 10 des LLM de l'OWASP](#) peuvent également aider les organisations à avoir des conversations éclairées basées sur les risques avec les fournisseurs de LLM.

Recommandation :

Veillez à ce que l'évaluation comparative et l'évaluation des risques fassent partie d'une stratégie plus large de renforcement et de minimisation pour les environnements cloud gérés. Mettez en œuvre des frameworks d'évaluation comparative, tels que ceux fournis par le CIS, en mettant l'accent sur l'application du moindre privilège. Les utilisateurs doivent préconiser des paramètres par défaut plus sécurisés pour l'authentification, l'accès aux données et les changements de configuration. En outre, veillez à ce que les bonnes pratiques soient respectées pour chaque environnement de fournisseur de services cloud géré, et veillez à ce que les mises à jour des politiques et des normes par défaut soient effectuées.



Conclusion

Bien qu'on n'en ait pas toujours l'impression, les efforts déployés en matière de sécurité font la différence. L'attention considérable accordée aux menaces prouve à elle seule que les utilisateurs malveillants sont confrontés à des défis de plus en plus importants, et ce n'est pas une coïncidence. Toutefois, les acteurs malveillants parvenus à maturité apprennent à surmonter les obstacles, par exemple en exploitant les vulnérabilités inhérentes aux pilotes de périphériques privilégiés pour Windows afin de désactiver les capteurs EDR, en s'injectant dans des processus privilégiés afin de supprimer les logs de sécurité critiques ou en déchargeant les composants de sécurité afin d'empêcher toute ingestion de sécurité. Malgré tous nos progrès, nous avons encore une marge d'amélioration. Cette année, nous avons vu des utilisateurs malveillants de toutes sortes tirer parti d'identifiants volés pour obtenir un accès *initial*, facilité par une marketplace massive de brokers de données volées. Les entreprises doivent redoubler d'efforts pour limiter les systèmes publics, mettre en place l'authentification multi-facteurs, minimiser leur surface d'attaque et protéger les données nécessaires à la détection des menaces. Pour les entreprises qui paient déjà pour des mesures d'atténuation puissantes, l'étape la plus importante consiste à les activer. Une approche axée uniquement sur la détection ne fonctionne pas, vous devez prévenir ce que vous pouvez prévenir. En outre, n'oublions pas le sujet qui devrait faire une grande différence cette année : l'IA. Les capacités de l'intelligence artificielle n'ont pas

transformé le paysage pour le meilleur ou pour le pire, elles n'ont pas conduit à une explosion de nouvelles menaces et elles n'ont pas créé un avantage tel que toutes les menaces ont été éliminées. Nous pensons que les répercussions de cette technologie ne se sont pas encore fait sentir. Il n'existe aucune garantie en matière de sécurité, c'est pourquoi la recherche sur la sécurité reste un élément essentiel pour naviguer dans le paysage des menaces. Les attaquants comme les défenseurs repoussent les limites du possible au quotidien. La mission d'Elastic Security Labs est de comprendre ces dynamiques. Pour supprimer le statut "occulte" des actions des attaquants, il convient d'exposer, de contextualiser et d'atténuer. Nous espérons que vous nous rejoindrez dans cette mission. Bien qu'écrasant, le paysage des menaces n'est pas insurmontable. Chaque action fait pencher la balance de notre côté, et nous espérons que nos efforts sont visibles dans notre engagement à démocratiser la connaissance, à publier des outils puissants et à partager l'incroyable visibilité d'Elastic.

Vous pouvez le faire. Et nous sommes là pour vous accompagner.

Pour en savoir plus sur [Elastic Security](#) et sur la façon de vous protéger contre les menaces abordées dans ce rapport (et d'autres vulnérabilités), rendez-vous sur [Elastic Security Labs](#). Vous pouvez aussi [nous suivre sur X](#) pour savoir dès que nous publions une nouvelle recherche sur les menaces.

Le rapport 2024 d'Elastic sur les menaces mondiales présente des informations et une expertise provenant de l'ensemble de l'organisation Elastic. Nous tenons à remercier les Elasticiens suivants pour leur contribution :

- ♦ Mika Ayenson
- ♦ Samir Bousseaden
- ♦ Terrance DeJesus
- ♦ Chris Donaher
- ♦ Tinsae Erkailo
- ♦ Ayoub Faouzi
- ♦ Eric Forte
- ♦ Ruben Groenewoud
- ♦ Justin Ibarra
- ♦ Devon Kerr
- ♦ Jake King
- ♦ Shashank Suryanarayana
- ♦ Mark Mager
- ♦ Asuka Nakajima
- ♦ Andrew Pease
- ♦ John Uhlmann
- ♦ Alyssa VanNice
- ♦ Colson Wilhoit

Rapport sur les menaces mondiales

—
2024



© 2024. Elasticsearch B.V. Tous droits réservés.

Elastic, Elasticsearch et les autres marques associées sont des marques commerciales, des logos ou des marques déposées d'Elasticsearch B.V. aux États-Unis et dans d'autres pays. Microsoft, Azure, Windows et les autres marques associées sont des marques commerciales du groupe Microsoft. Amazon Web Services, AWS, et les autres marques associées sont des marques commerciales d'Amazon.com, Inc. ou de ses sociétés affiliées. Tous les autres noms de marque, noms de produit ou marques commerciales appartiennent à leurs propriétaires respectifs.

