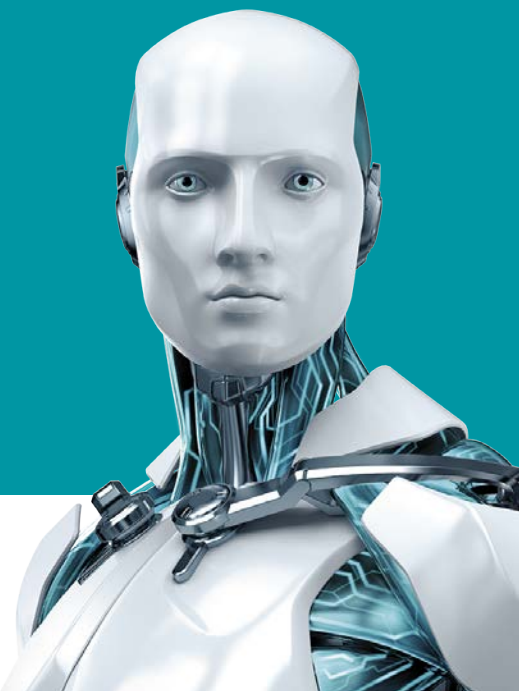
TECHNOLOGIE ESET

L'efficacité d'une approche multicouche

Auteurs :
Jakub Debski, directeur produit
Juraj Malcho, directeur de la technologie
Peter Stančík, responsable de la recherche et de la sensibilisation à la sécurité

Version du document : 1.3



ENJOY SAFER TECHNOLOGY™

TABLE DES MATIÈRES

OBJECTIFS

Dans ce document, nous passons en revue les technologies utilisées par ESET pour offrir une protection multicouche bien plus efficace qu'un simple antivirus, en détaillant le rôle de chacune d'entre elles dans la résolution de problèmes spécifiques, ainsi que les avantages apportés aux utilisateurs.

SOLUTIONS DE SÉCURITÉ NEXT-GEN

Les éditeurs d'antivirus bien établis ont fondé leur réussite sur la volonté d'aider les utilisateurs à combattre les virus ou les malwares, grâce à des technologies adaptées à un éventail de menaces de plus en plus large. Aujourd'hui, les antivirus sont perçus comme un produit de base et la sécurité est un sujet qui trouve de l'écho auprès du plus grand nombre, même ceux qui en ignorent les implications. Récemment, le nombre d'éditeurs soi-disant « next-gen » — ou plutôt de l'« ère post-vérité » selon nous — a explosé. Ces jeunes entreprises possèdent généralement une expérience limitée dans le développement de solutions anti-malware, mais cela ne les empêche pas de vanter le caractère « innovant » de leurs produits, ni de dénigrer les fournisseurs de longue date en les traitant de « dinosaures ». Comme pour la plupart des vendeurs de solutions miracles, bon nombre de leurs allégations sont trompeuses et, paradoxalement, leurs fonctionnalités reposent souvent sur un moteur de détection tiers appartenant à un éditeur reconnu. En effet, parmi les dizaines d'acteurs du marché actuel, rares sont ceux qui disposent de l'expérience ou des compétences nécessaires pour développer leur propre technologie de détection. En ce qui concerne ESET, toutes ses technologies sont exclusives et ont été développées en interne.

Or, la détection simple par signature statique — qui, selon les nouveaux entrants, rend inefficaces les solutions anti-malware des éditeurs bien établis — est aujourd'hui, sinon délaissée, du moins réduite à un rôle mineur au sein de la batterie de technologies déployées par les produits de sécurité contre les menaces actuelles.

UNE PROTECTION MULTICOUCHE CONTRE UNE MULTITUDE DE MENACES

Les éditeurs de logiciels anti-malware toujours en activité à l'heure actuelle ont maintenu leurs parts de marché en s'adaptant aux nouvelles menaces.

Loin d'être statiques, ces menaces n'ont cessé d'évoluer depuis les années 2000, et il est impossible de combattre celles d'aujourd'hui en se contentant des technologies des années 1990. De nos jours, la lutte contre les malwares ressemble à un jeu du chat et de la souris, dans lequel nos adversaires sont des malfaiteurs professionnels avec une forte motivation (financière). Les entreprises de sécurité informatique doivent donc perfectionner leurs produits en permanence, de manière réactive et proactive, afin d'offrir des solutions multicouches efficaces pour la détection et le blocage des programmes malveillants actuels. En effet, il ne suffit pas de se défendre sur un seul front ni de compter sur une seule technologie de protection.

C'est pourquoi ESET est passé d'un simple éditeur d'antivirus à une entreprise de sécurité informatique.

Une multitude de menaces visant une multitude de plateformes

Les systèmes d'exploitation de Microsoft ne sont pas les seules cibles des malwares d'aujourd'hui. Le champ de bataille évolue rapidement, au fur et à mesure que les pirates s'attaquent à des plateformes et processus jusqu'alors inexplorés.

- Tout ce qui peut être contrôlé en vue de mener des activités malveillantes est susceptible d'être exploité pour des attaques.

- Tout ce qui exécute du code pour traiter des données externes peut être détourné par des fichiers malveillants.

Les serveurs Linux sont une cible majeure des pirates (Opération Windigo, *Linux/Mumblehard*), les Mac sous OS X ont hébergé l'un des plus grands botnets de tous les temps (*OSX/Flashback*), les téléphones mobiles sont fréquemment visés (*Hesperbot*) et les attaques sur les routeurs représentent une menace de plus en plus sérieuse (*Linux/Moose*). Les rootkits s'en prennent désormais au matériel (en particulier au firmware ou à l'*UEFI*) tandis que la virtualisation ouvre la voie à de nouveaux vecteurs d'attaque (notamment Bluepill et l'évasion de machine virtuelle). Par ailleurs, les navigateurs et autres applications Web étant devenus aussi complexes que des systèmes d'exploitation, leurs mécanismes d'écriture de scripts sont souvent utilisés à des fins malveillantes (*Win32/Theola*).

Une multitude de vecteurs de propagation

Historiquement, les premiers malwares étaient des processus capables de se répliquer, tout d'abord dans les systèmes, puis en tant que virus infectant les fichiers ou les disques et se propageant d'un ordinateur à un autre. Avec la généralisation de l'utilisation d'Internet, les modes de propagation des logiciels malveillants se sont fortement diversifiés.

Les malwares peuvent être envoyés par e-mail sous forme de pièces jointes ou de liens, téléchargés depuis des pages Web, intégrés dans des documents à l'aide de scripts, diffusés par le biais de périphériques amovibles, déployés à distance en profitant de droits d'accès et de mots de passe faibles, exécutés via des exploits ou encore installés par des utilisateurs finaux manipulés par des techniques d'ingénierie sociale.

Conception d'un malware

Le temps où les logiciels malveillants étaient surtout développés par des adolescents farceurs ou en quête de reconnaissance est révolu. De nos jours, les malwares sont conçus à des fins d'escroquerie ou de vol d'informations, et font l'objet d'importants investissements de la part aussi bien des criminels que des autorités.

Pour une détection plus difficile, les malwares sont codés dans divers langages de programmation et exécutés à l'aide de différents compilateurs ou interpréteurs. Le code est obscurci et protégé par des logiciels personnalisés afin de rendre la détection et l'analyse plus ardues. Il est injecté dans des processus inoffensifs pour esquiver la surveillance comportementale (conçue pour repérer les activités suspectes), éviter d'être supprimé et assurer ainsi sa persistance dans le système. Les scripts sont utilisés pour échapper aux techniques de contrôle d'applications, tandis qu'un code malveillant résidant uniquement dans la mémoire permet de contourner les outils d'analyse de fichiers.

Pour passer entre les mailles du filet, les cybercriminels sèment des milliers de variantes de leurs malwares partout sur Internet. Une autre stratégie consiste à cibler un faible nombre de victimes, afin de ne pas attirer l'attention des entreprises de sécurité informatique. Le code malveillant passe inaperçu grâce au détournement de composants logiciels anodins ou à l'utilisation de certificats numériques de confiance.

Au niveau du réseau, les malwares se servent moins des serveurs de commande et contrôle (C&C) codés en dur pour envoyer des instructions aux systèmes compromis et recevoir des données de leur part. Les botnets sont généralement contrôlés de façon décentralisée à l'aide d'un réseau peer-to-peer, et les communications chiffrées rendent l'identification des attaques plus difficile. Les algorithmes de génération de domaines réduisent l'efficacité d'une détection reposant sur le blocage d'URL connues.

Les sites Web de bonne réputation et les services de publicité légitimes peuvent également être piratés pour diffuser des contenus malveillants.

REMARQUE IMPORTANTE
Comme les attaques peuvent échapper à la détection de nombreuses façons, une solution limitée à une seule technologie n'est pas suffisante. Chez ESET, nous sommes convaincus qu'une protection multicouche en temps réel est nécessaire pour assurer une sécurité optimale.

LES AVANTAGES DE LA TECHNOLOGIE ESET

Le moteur d'analyse d'ESET est au cœur de nos solutions. Sa technologie sous-jacente, bien qu'issue d'un « antivirus traditionnel », a été perfectionnée et fait l'objet d'un développement continu de façon à prendre en charge les menaces actuelles.

L'objectif du moteur d'analyse est d'identifier les éventuels malwares et de déterminer automatiquement la probabilité que le code évalué soit malveillant.

Pendant de nombreuses années, ESET utilisait des algorithmes intelligents et un code assembleur écrit manuellement pour pallier les problèmes de performances causés par l'analyse de code approfondie à l'aide de la technologie sandbox intégrée. Depuis, nous avons optimisé cette approche en combinant la traduction binaire avec l'émulation interprétée.

Avec une sandbox intégrée, pour exécuter un programme dans un environnement virtualisé, vous devez émuler différents composants matériels et logiciels, notamment la mémoire, le système de fichiers, les API de système d'exploitation et le processeur.

Par le passé, le processeur était émulé à l'aide d'un code assembleur sur mesure. Il s'agissait cependant d'un « code interprété », c'est-à-dire que chaque instruction devait être reproduite séparément. Avec la traduction binaire, les instructions émulées sont exécutées en natif sur un processeur réel, ce qui est beaucoup plus rapide, en particulier pour les boucles présentes dans le code. Les boucles multiples sont couramment employées dans les exécutables pour déjouer l'analyse effectuée par les produits anti-malware et les chercheurs en sécurité.

Les solutions d'ESET analysent des centaines de formats de fichier différents (exécutables, programmes d'installation, scripts, archives, documents et bytecodes), afin d'y détecter les éventuels éléments malveillants avec précision.

Le schéma figurant à la page suivante présente les différentes technologies d'ESET, le moment où elles peuvent détecter et/ou bloquer une menace durant son cycle de vie dans le système, ainsi que la manière dont elles procèdent.

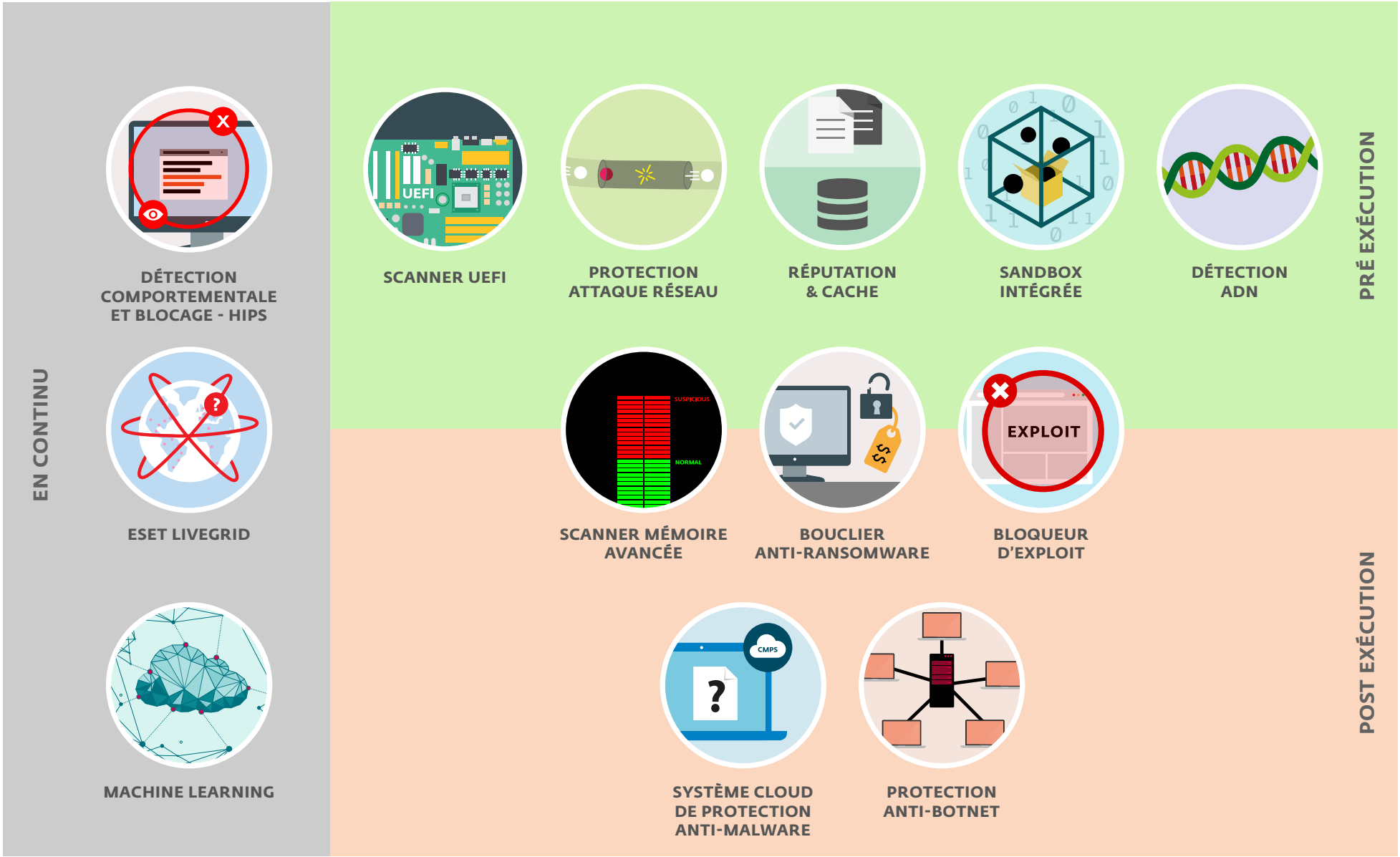
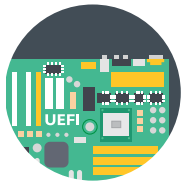


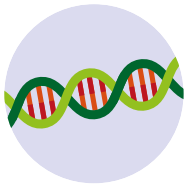
Fig. 1 : Les couches de protection ESET



Scanner UEFI

ESET est le premier éditeur de cybersécurité à intégrer dans sa solution une technologie dédiée à la protection de l'UEFI (Unified Extensible Firmware Interface). Scanner UEFI d'ESET vérifie et assure la sécurité de l'environnement pré-démarrage conformément aux spécifications UEFI. Elle est conçue pour détecter les éléments malveillants du firmware et les signaler à l'utilisateur.

L'UEFI est une spécification normalisée définissant l'interface logicielle entre le système d'exploitation et le firmware d'un ordinateur, et qui remplace le BIOS (Basic Input/Output System) anciennement utilisé depuis le milieu des années 1970. Grâce à sa structure bien documentée, l'UEFI est plus facile à analyser, ce qui permet aux développeurs de créer des extensions pour le firmware. Cependant, cette caractéristique ouvre également la voie aux cybercriminels, qui peuvent infecter l'UEFI avec des modules malveillants.



Détection ADN

Il existe divers types de détection, allant du hachage spécifique (utilisé notamment pour cibler des codes binaires malveillants ou des versions de malwares, à des fins statistiques ou encore comme nom de détection plus précis pour les malwares précédemment identifiés par heuristique) à la détection ADN d'ESET, qui repose sur des définitions complexes des comportements malveillants et des caractéristiques des malwares.

La reconnaissance de constantes employées par les antivirus traditionnels peut être facilement contournée par simple modification du code ou à l'aide de techniques d'obscurcissement. En revanche, le comportement des objets est plus difficile à changer.

La détection ADN d'ESET est justement conçue pour tirer profit de ce principe. Nous effectuons une analyse approfondie du code pour en extraire les « gènes » responsables de son comportement. De tels gènes comportementaux contiennent bien plus d'informations que les indicateurs de compromission (IOC) qui, pour certains éditeurs « next-gen », seraient une « meilleure alternative » à la détection par signature. Ces gènes sont utilisés pour construire des définitions comportementales ADN, qui servent à évaluer le code suspect présent sur le disque ou dans la mémoire des processus en cours d'exécution.

Notre moteur d'analyse extrait également de nombreux gènes discriminants utilisés pour détecter les anomalies, tout ce qui semble illégitime étant potentiellement malveillant.

Selon le seuil et les critères de reconnaissance définis, la détection ADN permet d'identifier des échantillons de malwares connus, de nouvelles variantes d'une famille répertoriée, voire des malwares inédits contenant des gènes indicateurs d'un comportement malveillant. En d'autres termes, avec une seule description comportementale ADN bien conçue, il est possible de détecter des dizaines de milliers de variantes de malwares apparentées. Nos antivirus peuvent ainsi identifier les logiciels

malveillants déjà rencontrés, mais aussi des variantes auparavant inconnues. Par ailleurs, grâce au regroupement automatisé de nos échantillons de malwares et à l'application d'algorithmes de machine learning, nous identifions de nouveaux gènes et motifs de comportements malveillants pour notre moteur d'analyse. Ces gènes peuvent être comparés à une liste blanche de façon à éviter les faux positifs.

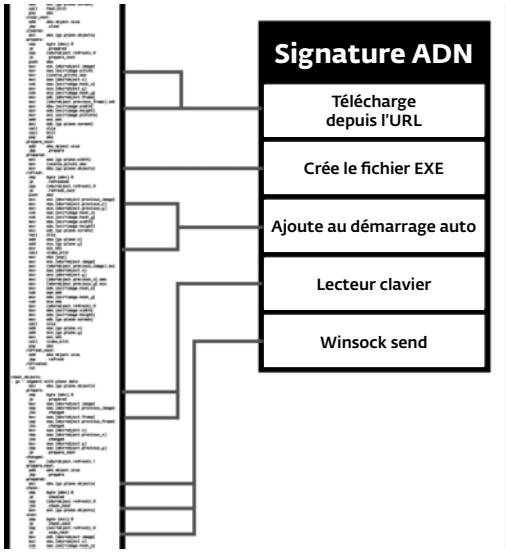


Fig. 2 : Exemple de détection ADN

Machine Learning

ESET s'intéresse aux algorithmes de machine learning pour la détection et le blocage des menaces depuis les années 1990, intégrant les réseaux neuronaux dans ses produits dès 1998. Depuis, nous avons appliqué cette technologie prometteuse à l'ensemble de nos solutions multicouches.

À titre d'exemple, notre détection ADN repose sur des modèles de machine learning, ce qui lui permet d'être efficace avec ou sans connexion au Cloud. Les algorithmes de machine learning jouent également un rôle central dans le tri et la classification initiaux des échantillons entrants, ainsi que dans leur positionnement sur une « carte de cybersécurité » imaginaire.

Mais ESET a surtout développé en interne son propre moteur de machine learning, baptisé Augur. Il tire sa puissance de l'alliance entre les réseaux neuronaux — tels que l'apprentissage profond et la mémoire à court terme persistante (LSTM, Long Short-Term Memory) — et un groupe de six algorithmes de classification triés sur le volet. Il peut ainsi générer un résultat consolidé et étiqueter correctement les échantillons entrants comme inoffensifs, potentiellement indésirables ou malveillants.

Le moteur Augur d'ESET est optimisé de façon à exercer une action synergique avec d'autres technologies de protection (telles que la détection ADN, la sandbox et l'analyse de la mémoire), mais aussi avec l'extraction de caractéristiques comportementales, pour offrir des taux de détection inégalés ainsi qu'un nombre minimal de faux positifs.

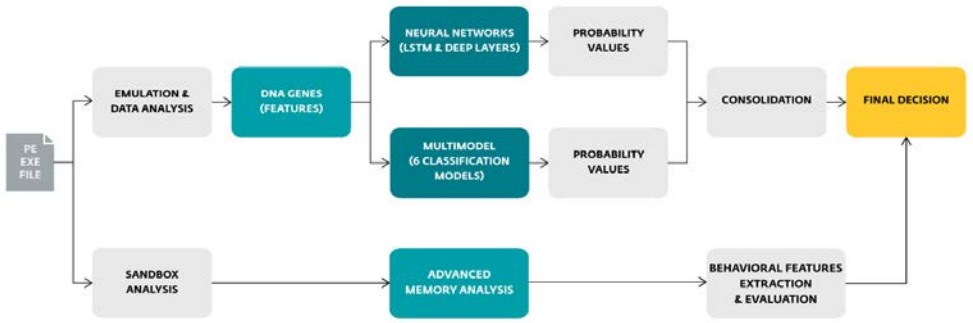


Fig. 3 : Principe du moteur de machine learning Augur d'ESET

ESET LiveGrid

La façon la plus simple d'assurer une protection via un système Cloud consiste à établir une liste noire stricte par hachage exact. Cette méthode fonctionne aussi bien pour les fichiers que les URL, mais elle ne permet de bloquer que les objets correspondant exactement aux empreintes. Cette limite a donné naissance au hachage approximatif, qui prend en compte la similarité binaire, étant donné que des objets similaires présentent une empreinte identique ou semblable.

ESET a élevé le hachage approximatif à un tout autre niveau, en l'appliquant non pas aux données, mais aux définitions comportementales ADN. Grâce aux empreintes ADN, nous sommes en mesure de bloquer instantanément des milliers de variantes de malwares (voir graphiques ci-contre).

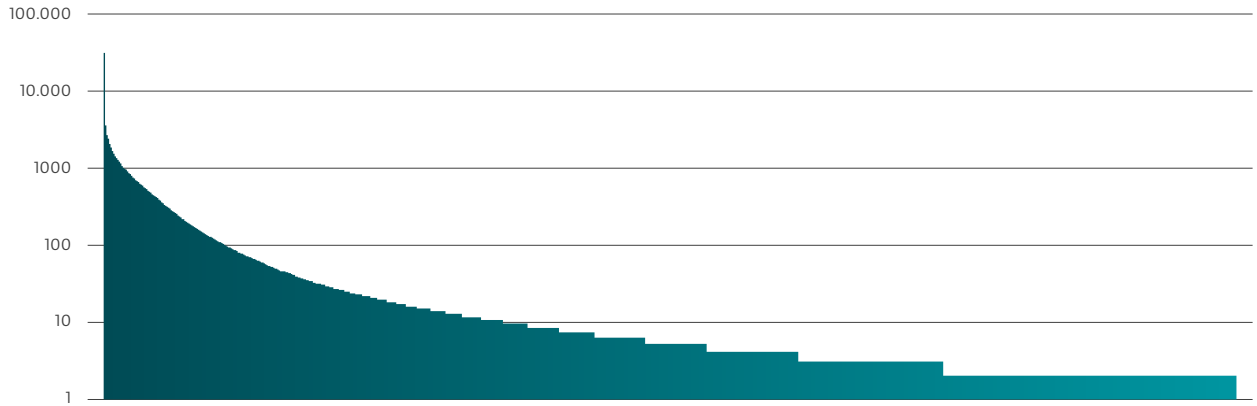


Fig. 4 : Nombre de fichiers uniques (axe des ordonnées) détectés par des empreintes ADN individuelles (axe des abscisses)

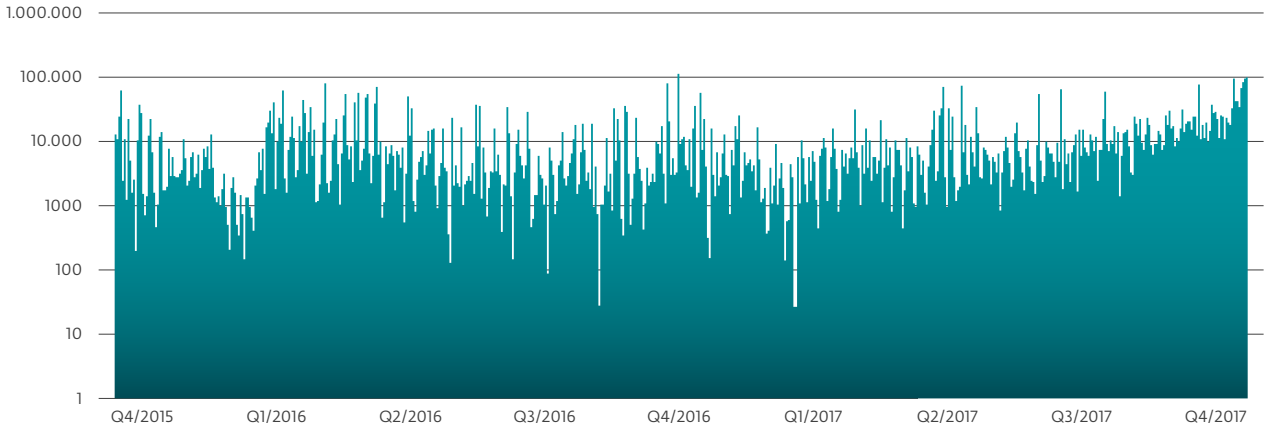


Fig. 5 : Nombre de fichiers uniques (axe des ordonnées) détectés par empreintes ADN par jour (axe des abscisses)

Système Cloud de protection anti-malware

Le système Cloud de protection anti-malware d'ESET fait partie des nombreuses solutions qui reposent sur notre technologie ESET LiveGrid. Les applications inconnues potentiellement malveillantes et autres menaces sont surveillées et signalées à la plateforme Cloud d'ESET via le système de feedback ESET LiveGrid. Les échantillons collectés sont automatiquement placés en sandbox et soumis à une analyse comportementale, qui génère des alertes automatisées en cas de confirmation des caractéristiques malveillantes. Nos clients sont informés de ces alertes via le système de réputation ESET LiveGrid, sans devoir attendre la mise à jour suivante du moteur de détection. Le processus dure généralement moins de 20 minutes, ce qui permet la détection efficace de menaces émergentes avant même que les alertes régulières ne soient envoyées aux utilisateurs.

Le système Cloud de protection anti-malware d'ESET n'a pas pour seul objectif de fournir aux utilisateurs une liste noire en temps réel. Chez les utilisateurs ayant activé l'envoi d'échantillons, tout nouvel échantillon identifié avec une réputation douteuse est envoyé à ESET pour une analyse approfondie. Pour tirer le meilleur parti du système Cloud de protection anti-malware d'ESET, il est recommandé d'activer le système de feedback ESET LiveGrid, qui nous permet de collecter tous les échantillons suspects en vue d'une évaluation avancée.

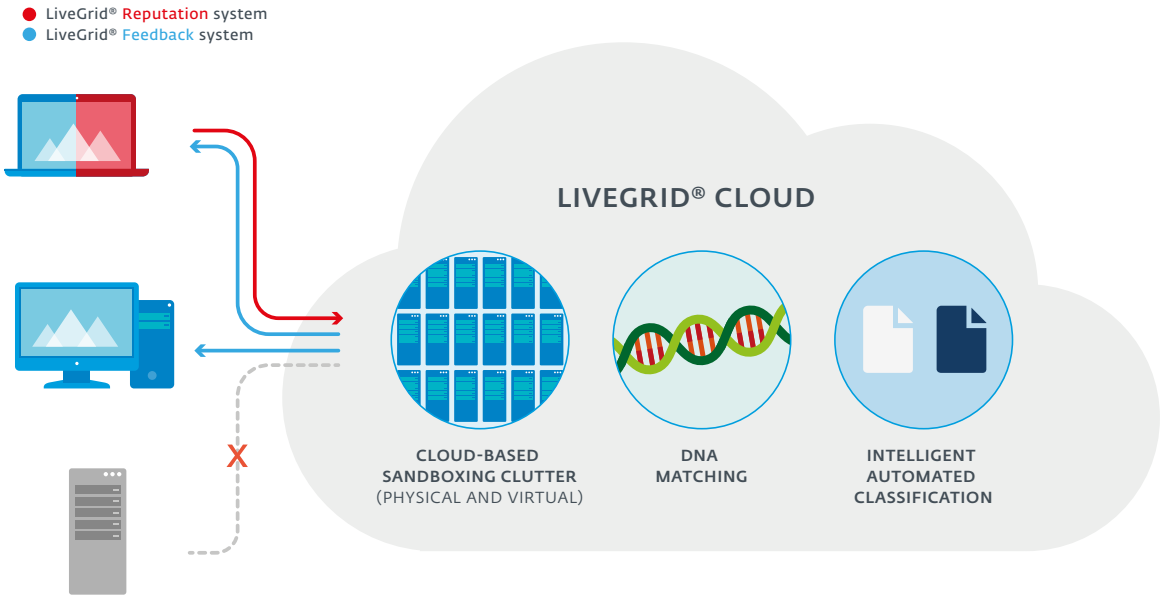


Fig. 6 : Système Cloud de protection anti-malware d'ESET

Réputation et cache

En amont de l'analyse d'objets tels qu'un fichier ou une URL, nos solutions vérifient si des éléments malveillants connus ou des éléments inoffensifs figurant dans la liste blanche sont présents dans le cache local (et ESET Shared Local Cache, dans le cas d'ESET Endpoint Security), ce qui améliore les performances de l'analyse.

Ensuite, une recherche de réputation est effectuée au niveau du système de réputation ESET LiveGrid® (de façon à vérifier si l'objet est déjà connu et classé comme malveillant ou autre), pour une analyse plus efficace et un partage plus rapide des informations relatives aux malwares avec nos clients.

Grâce aux listes noires d'URL et à la vérification de réputation, l'accès aux contenus Web malveillants ou à des sites d'hameçonnage est bloqué.

Détection et blocage comportementaux — Système HIPS

Le système de prévention des intrusions sur l'ordinateur hôte d'ESET (HIPS, Host-based Intrusion Prevention System) surveille les activités du système et reconnaît les comportements suspects en fonction de règles prédéfinies. Le mécanisme d'autodéfense du système HIPS empêche le programme ou le processus mis en cause de mener des activités potentiellement nuisibles. Les utilisateurs peuvent personnaliser les règles par défaut, à condition de posséder une connaissance approfondie des applications et des systèmes d'exploitation.

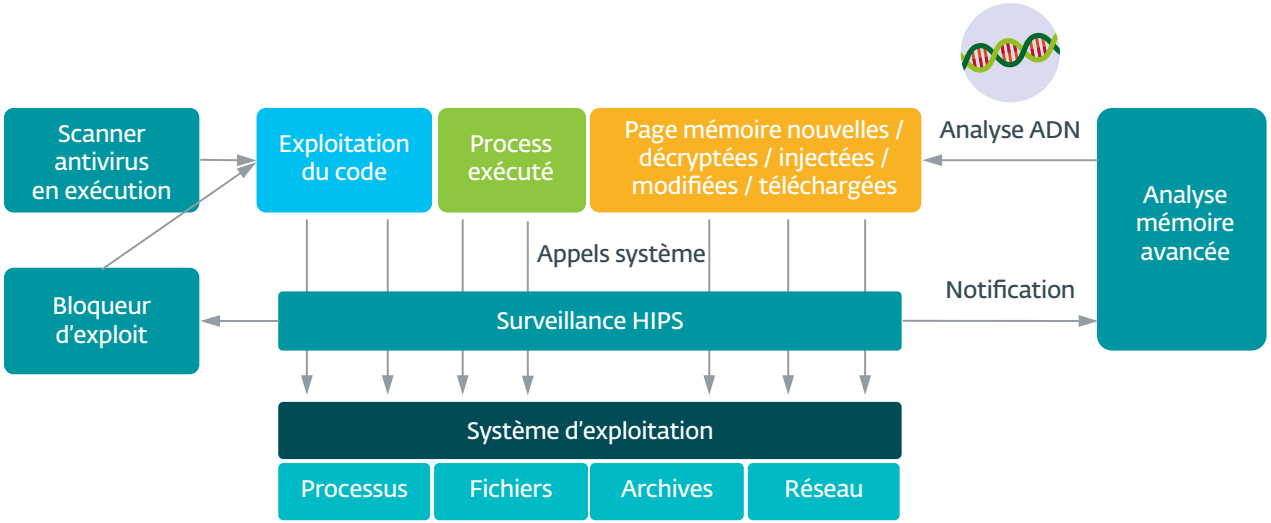
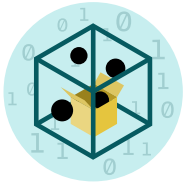


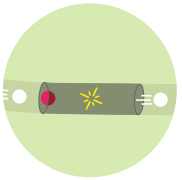
Fig. 7: Principe de la détection comportementale d'ESET



Sandbox intégrée

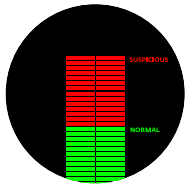
Nous avons divisé la détection ADN en deux parties pour une meilleure compréhension de l'ensemble du processus. En 1995, nous avons introduit notre premier émulateur, dans lequel il était possible d'exécuter le célèbre jeu Doom. L'émulation nous permet d'extraire les métadonnées comportementales que nous utilisons dans notre détection ADN. Les malwares étant de plus en plus souvent obscurcis pour échapper à la détection, nous devons connaître et cibler leurs comportements concrets. Nous utilisons également des traductions binaires afin de ne pas ralentir la machine.

Fig. 8 : Avantage de la sandbox intégrée d'ESET



Protection contre les attaques réseau

La protection contre les attaques réseau est une extension du pare-feu qui améliore la détection des failles connues à l'échelle du réseau. En détectant les vulnérabilités courantes dans les protocoles les plus utilisés (tels que *SMB*, *RPC* et *RDP*), cette fonctionnalité offre une couche de protection supplémentaire importante contre la propagation des malwares, les attaques réseau et l'exploitation de failles pour lesquelles aucun correctif n'a encore été publié ou installé.



Analyse mémoire avancée

L'analyse mémoire avancée est une technologie ESET unique qui résout de manière efficace un problème majeur lié aux malwares actuels : le recours fréquent à des techniques d'obscurcissement et/ou de chiffrement.

Souvent employées dans les programmes de compression d'exécutables et de protection de code, ces stratégies causent des difficultés aux approches de détection qui utilisent des techniques de décompression telles que l'émulation ou le sandboxing. De plus, que la vérification ait lieu dans un émulateur ou une sandbox virtuelle/physique, il n'est pas garanti que le malware affiche durant l'analyse un comportement malveillant permettant de le classer comme tel.

Les malwares peuvent être obscurcis de façon à ce que certains chemins d'exécution ne puissent pas être analysés, contenir des déclencheurs conditionnels ou temporels et, dans de nombreux cas, télécharger de nouveaux éléments au cours de leur existence. Pour remédier à ces problèmes, la technologie d'analyse mémoire avancée surveille le comportement des processus malveillants et les analyse lorsqu'ils se montrent sous leur vrai jour dans la mémoire. Cela permet de compléter la fonctionnalité traditionnelle d'analyse de code proactive avant et pendant l'exécution.

D'autre part, les processus inoffensifs peuvent soudainement devenir malveillants par exploitation d'une faille ou par injection de code. Ainsi, une seule analyse n'est pas suffisante et une surveillance continue est nécessaire — c'est ce qu'offre l'analyse mémoire avancée. Chaque fois qu'un processus appelle le système depuis une nouvelle page exécutable, cette technologie réalise une analyse de code comportementale à l'aide de la détection ADN d'ESET.

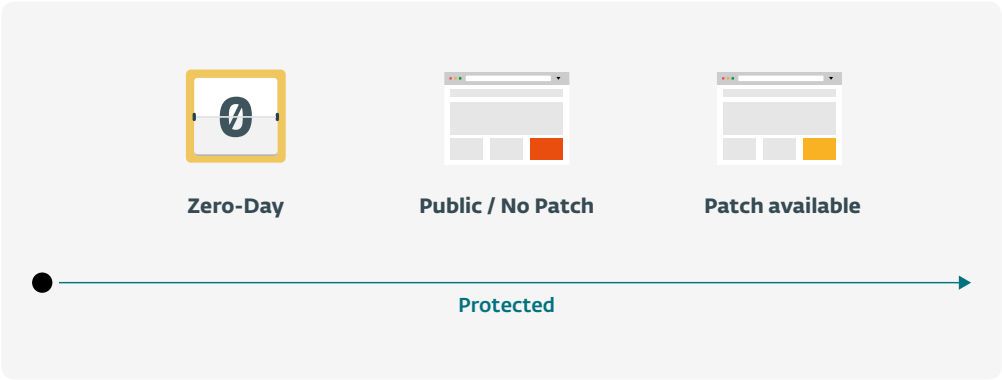
Cette analyse est effectuée non seulement sur la mémoire exécutable standard, mais aussi sur le code en .NET MSIL (Microsoft Intermediate Language), utilisé par les auteurs de malwares pour ralentir l'analyse dynamique. Grâce à une mise en cache intelligente, la technologie d'analyse mémoire avancée ne présente pas de surcharge et n'entraîne aucune réduction notable de la vitesse de traitement.

Contrairement au bloqueur d'exploits avec lequel elle agit en synergie, l'analyse mémoire avancée est une méthode post-exécution, ce qui signifie qu'une activité malveillante risque d'avoir déjà eu lieu. Toutefois, elle complète la chaîne de protection en tant que solution de dernier recours, dans l'éventualité où un pirate parviendrait à contourner les autres technologies.

Par ailleurs, une nouvelle tendance a fait son apparition dans le domaine des malwares sophistiqués : dans certains cas, le code malveillant reste confiné dans la mémoire, sans nécessiter aucun composant persistant dans le système de fichiers pouvant être détecté par une méthode conventionnelle.

Au début, de tels malwares n'apparaissaient que sur les serveurs en raison de leur temps de fonctionnement prolongé : étant donné que

ces derniers restent allumés plusieurs mois voire années à la fois, les processus malveillants peuvent résider dans la mémoire indéfiniment, sans devoir survivre à un redémarrage. Cependant, comme le montrent de récentes attaques contre des entreprises, cette tendance évolue et les terminaux sont désormais ciblés de la même façon. Seule une analyse de la mémoire peut permettre de détecter ce type d'attaques malveillantes — un défi qu'ESET est prêt à relever grâce à sa technologie d'analyse mémoire avancée.



Bloqueur d'exploits

Les technologies d'ESET vous protègent contre divers types de failles à différents niveaux : notre moteur d'analyse détecte les exploits dans les fichiers documents vulnérables ; la protection contre les attaques réseau cible les communications ; et le bloqueur d'exploits bloque le processus d'exploitation de failles.

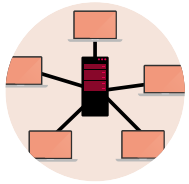
Le bloqueur d'exploits surveille les applications vulnérables (navigateurs, lecteurs de documents, clients de messagerie, Flash, Java, etc.). Au lieu de se limiter à des *identifiants CVE* spécifiques, il cible les techniques d'exploitation de failles.

Les exploits sont des anomalies dans l'exécution des processus et nous recherchons celles qui suggèrent l'emploi de techniques d'exploitation de failles. Avec le développement continu de notre technologie, les méthodes de détection sont mises à jour régulièrement pour prendre en compte les nouvelles techniques d'exploitation. Lorsqu'un processus est enclenché, son comportement est analysé. S'il est considéré comme suspect, il est immédiatement bloqué sur l'ordinateur, et les métadonnées relatives à l'attaque sont envoyées à notre système Cloud ESET LiveGrid. Ces données sont traitées et mises en corrélation, ce qui nous permet d'identifier les vulnérabilités auparavant inconnues ou « zero-day », et fournit à notre laboratoire de précieuses informations sur les menaces.

Le bloqueur d'exploits offre une couche de protection supplémentaire et nous rapproche des attaquants, grâce à une technologie totalement différente des techniques de détection axées sur l'analyse du code malveillant proprement dit.

Bouclier anti-ransomware

Le bouclier anti-ransomware d'ESET protège les utilisateurs contre les rançongiciels. Cette technologie surveille et évalue toutes les applications exécutées en réalisant une analyse heuristique comportementale et fondée sur la réputation. Lorsqu'un comportement assimilé à celui d'un ransomware est identifié ou que le malware potentiel tente d'apporter des modifications non sollicitées à des fichiers existants (pour les chiffrer, par exemple), notre fonctionnalité informe l'utilisateur, qui peut bloquer l'activité. Le bouclier anti-ransomware est optimisé pour offrir un niveau de protection inégalé contre les rançongiciels conjointement avec d'autres technologies ESET, telles que le système Cloud de protection anti-malware, la protection contre les attaques réseau et la détection ADN.



Protection anti-botnet

Un changement de mode de communication avec les serveurs C&C est coûteux pour les auteurs de malwares.

La protection anti-botnet d'ESET détecte les communications malveillantes des botnets, tout en identifiant les processus en cause.

La détection réseau d'ESET complète la protection anti-botnet en résolvant les problèmes généraux liés à l'analyse du trafic réseau. Ces technologies permettent une détection rapide et flexible du trafic malveillant. De nombreuses attaques peuvent être détectées avec les signatures standards du secteur telles que Snort ou Bro, mais la détection réseau d'ESET est conçue pour cibler les failles du réseau, les kits d'exploit et les communications des malwares avancés en particulier.

L'analyse du trafic réseau au niveau des terminaux offre d'autres avantages : elle permet d'identifier précisément le processus ou le module impliqué dans la communication malveillante, de prendre des mesures contre l'objet en question, voire dans certains cas de contourner le chiffrement de la communication.

Suivi des botnets

Les échantillons identifiés comme « botnet » par les solutions d'ESET (ou dont l'image mémoire est classée comme tel) sont envoyés à notre système de suivi des botnets, qui détermine la variante exacte du malware et, à l'aide d'un programme de décompression/déchiffrement spécifique, extrait des informations sur ses serveurs C&C et clés de chiffrement/communication. Une fois celles-ci obtenues, le système engage de fausses communications depuis différents lieux géographiques. Toutes les données extraites sont ensuite soumises à un post-traitement et utilisées pour protéger nos clients partout dans le monde, par exemple en bloquant des URL, en créant de nouvelles alertes pour les contenus malveillants et en informant les utilisateurs d'ESET Threat Intelligence.

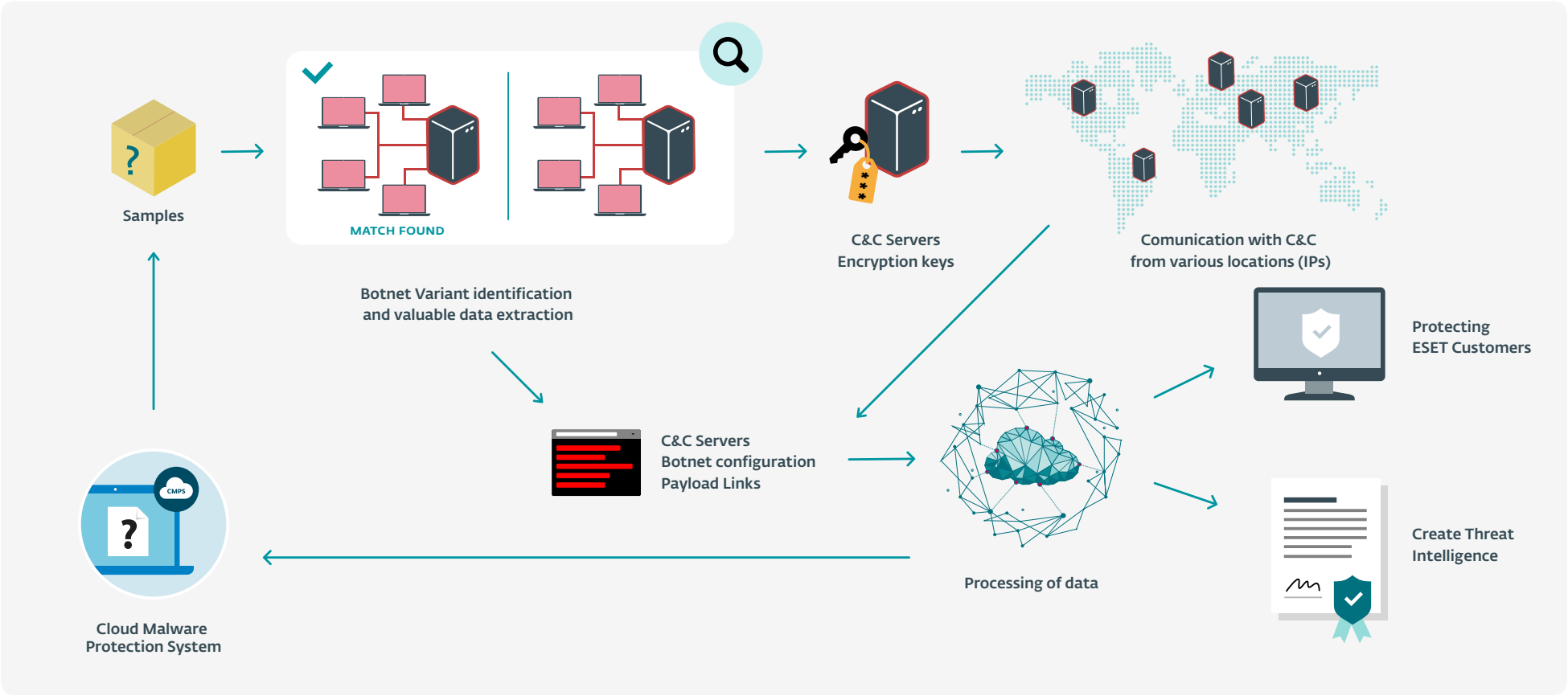


Fig. 9 : Principe du système de suivi des botnets d'ESET

Threat Intelligence

ESET Threat Intelligence (ETI) aide les entreprises à s'adapter aux menaces de cybersécurité ciblées et furtives d'aujourd'hui. Grâce à des données issues de plus de 100 millions de points de détection, ce service offre une excellente vue d'ensemble des menaces, aide les sociétés à anticiper les attaques et augmente l'efficacité du diagnostic post-incident en cas d'infection. Ces informations uniques renforcent la sécurité de l'entreprise, tout en protégeant les utilisateurs finaux. En fonction des besoins de l'organisation, les systèmes et les experts d'ESET peuvent générer des rapports personnalisés sur des botnets et des malwares spécifiques selon des règles YARA, des rapports sur l'hameçonnage ou des flux de données en temps réel au format STIX/TAXII, qui peuvent être intégrés aux outils SIEM existants en toute transparence.

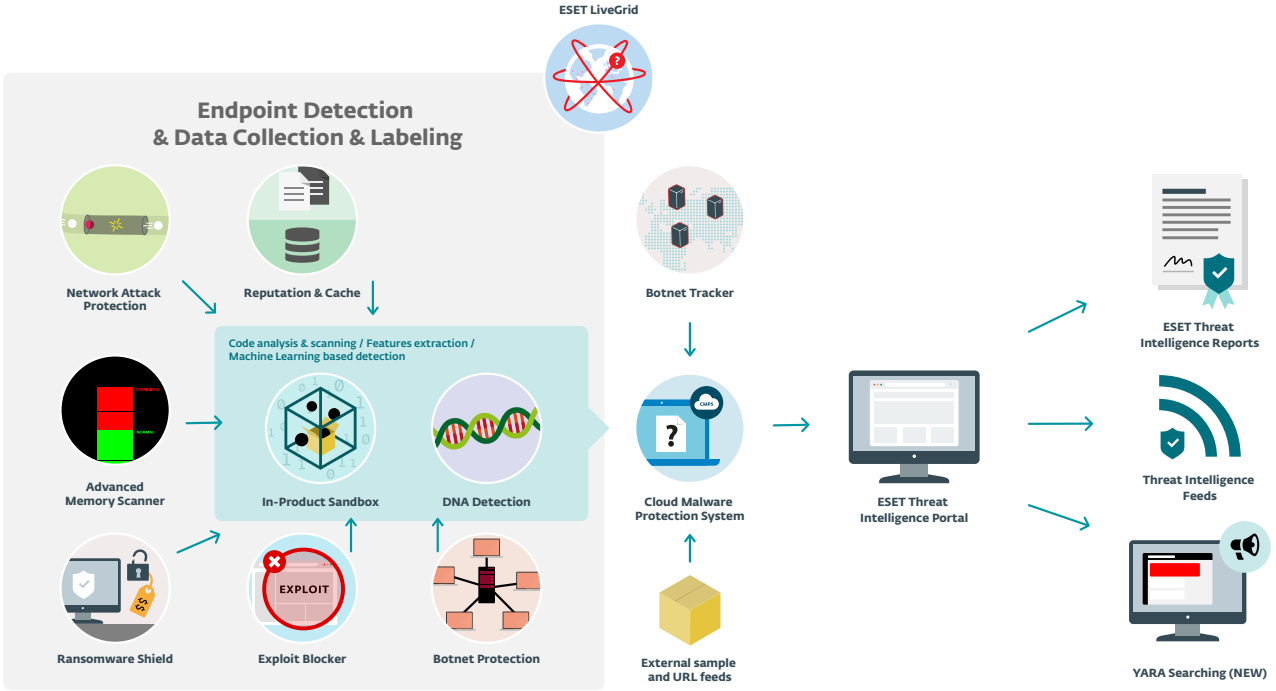


Fig. 10 : Collecte d'informations sur les menaces par les technologies ESET

PROTECTION RÉACTIVE VS PROACTIVE

La détection ADN permet d'identifier des familles entières de malwares, mais encore faut-il diffuser les définitions comportementales auprès des utilisateurs pour que la protection soit effective. Il en est de même pour le moteur d'analyse, l'heuristique ou toute modification ciblant de nouvelles menaces. Aujourd'hui, une communication avec le système Cloud ESET LiveGrid est indispensable pour assurer une protection optimale pour différentes raisons :

- L'analyse hors ligne est principalement réactive. De nos jours, il ne suffit plus de posséder la meilleure solution heuristique pour être proactif.
  Du moment que votre système de protection est accessible aux hackers, peu importe s'il repose sur les signatures, l'heuristique ou le machine learning : les auteurs de malwares peuvent tester votre technologie de détection et modifier leur code malveillant jusqu'à ce qu'il soit indétectable avant de le diffuser. ESET LiveGrid permet de contrer cette stratégie.
- Les mises à jour ne sont pas effectuées en temps réel. Il est possible d'augmenter la fréquence des mises à jour, voire de les envoyer aux utilisateurs à quelques minutes d'intervalle. Mais ESET LiveGrid va encore plus loin et offre une protection en temps réel en transmettant les informations nécessaires à tout moment.
- Les malwares tentent de passer inaperçus. Les auteurs de logiciels malveillants, notamment les cyberespions, s'efforcent d'échapper à la détection le plus longtemps possible. Contrairement aux infections de masse telles que la propagation de vers par e-mail, les attaques ciblées utilisent des malwares individuels et sont dirigées contre un nombre limité de cibles. Nous exploitons ce fait contre les attaquants : les objets peu populaires et ne disposant pas d'une bonne réputation sont considérés comme potentiellement malveillants. Ils sont soit analysés de manière approfondie au niveau du poste de travail, soit envoyés à ESET via notre système de feedback LiveGrid pour une analyse détaillée automatisée. Le système de réputation ESET LiveGrid contient des informations sur les fichiers, leur origine, les similarités, les certificats, les URL et les adresses IP.

Traitement automatisé et manuel des échantillons

ESET reçoit chaque jour des centaines de milliers d'échantillons. Ceux-ci sont traités automatiquement, semi-automatiquement et manuellement, après prétraitement et regroupement. L'analyse automatisée est réalisée par des outils développés en interne sur une série de machines physiques et virtuelles.

La classification est effectuée sur la base des différents attributs extraits lors de l'exécution, en fonction de l'analyse statique et dynamique du code, des modifications apportées au système d'exploitation, des motifs de communication réseau, de la similarité par rapport à d'autres échantillons de malwares, des caractéristiques ADN, des informations structurelles et des anomalies détectées.

Tous les algorithmes de classification automatique présentent des inconvénients :

- Le choix des caractéristiques discriminantes en vue de la classification n'est pas évident et doit être fondé sur les connaissances d'experts en malwares.
- Les algorithmes de classification reposant sur le machine learning nécessitent l'intervention d'experts humains pour vérifier les données d'entraînement. En cas de traitement entièrement automatisé (avec utilisation des échantillons classés par le système en tant qu'échantillons entrants), un effet boule de neige dû à la boucle de rétroaction positive rendrait rapidement le système instable. En effet, la qualité des résultats dépend de celle des données d'entrée.
- Les algorithmes de machine learning ne comprennent pas les données

et des informations statistiquement correctes ne sont pas nécessairement valides.

- Par exemple, les algorithmes de machine learning ne distinguent pas une nouvelle version d'un logiciel inoffensif d'une version non conforme, ni ne font la différence entre un programme de mise à jour associé à une application saine et un outil de téléchargement utilisé par un malware, ni ne reconnaissent l'utilisation de composants logiciels anodins à des fins malveillantes.
- L'ajout de nouveaux échantillons à un processus de machine learning peut générer de faux positifs, tandis que la suppression de ceux-ci risque de réduire l'efficacité de la détection.
- Si le traitement automatisé des échantillons permet de réagir en temps réel aux nouvelles menaces via ESET LiveGrid, une évaluation supplémentaire effectuée par des ingénieurs est essentielle pour assurer une qualité et un taux de détection exceptionnels, tout en minimisant le nombre de faux positifs.

Services d'évaluation de la réputation

ESET LiveGrid fournit également des informations sur la réputation des objets. Nous évaluons la réputation de différents éléments tels que les fichiers, les certificats, les URL et les adresses IP. Comme mentionné précédemment, la réputation peut être utilisée, entre autres, pour identifier de nouveaux objets malveillants ou sources d'infection.

Liste blanche

La liste blanche est une fonctionnalité qui réduit le nombre de fois où le moteur d'analyse doit examiner un objet. S'il est certain qu'un objet n'a pas été modifié et est inoffensif, aucune analyse n'est nécessaire. Cela améliore grandement les performances et permet aux solutions d'ESET d'être très discrètes. En effet, le code le plus rapide à exécuter est celui que l'on n'exécute pas. Nos listes blanches sont adaptées en permanence au monde informatique en constante évolution.

Collecte d'informations

Nous utilisons les informations transmises par les utilisateurs ayant activé l'envoi de statistiques à ESET LiveGrid pour le suivi et la surveillance des menaces à l'échelle mondiale. Nous analysons cette quantité importante de données afin de concentrer nos efforts sur les problèmes les plus urgents, de dégager les tendances en matière de malwares et de planifier le développement de technologies de protection par ordre de priorité.

FAUX POSITIFS ET INDICATEURS DE COMPROMISSION

Perçus comme des éléments clés dans la sécurité des entreprises d'aujourd'hui, les indicateurs de compromission (IOC) ne sont en réalité pas aussi extraordinaires que certains éditeurs « next-gen » voudraient le faire croire. Le diagramme ci-dessous illustre la répartition des IOC les plus répandus.* Les caractéristiques sur lesquelles ils reposent sont extrêmement basiques : dans un quart des cas, il s'agit d'empreintes MD5 connues, suivies des noms de fichiers, etc. Si ces indicateurs peuvent être utiles en informatique légale, il est évident qu'ils ne conviennent pas à la prévention ni au blocage des menaces. Certains éditeurs « next-gen », qui reprochent pourtant aux méthodes de détection par signature utilisées dans les antivirus traditionnels d'être « obsolètes », font l'éloge des IOC, alors qu'il s'agit justement de la méthode de détection par signature la moins efficace pour identifier les fichiers ou les événements malveillants. Un véritable paradoxe.

*Source : IOC Bucket, avril 2015. IOC Bucket est une plateforme communautaire dédiée au partage d'informations sur les menaces.

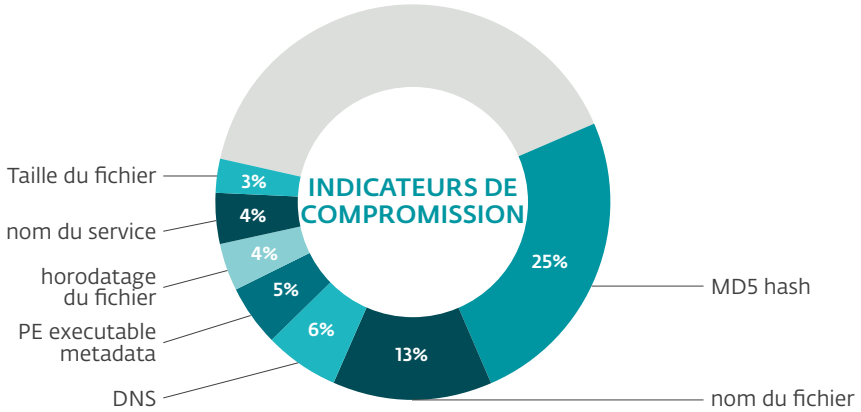


Fig. 11: Analyse des indicateurs de compromission, IOC Bucket (avril 2015)

CONCLUSION

Il n'existe pas de solution miracle en matière de sécurité informatique. Pour contrer les malwares dynamiques et ciblés d'aujourd'hui, il est nécessaire d'adopter une approche multicouche reposant sur des technologies intelligentes et proactives, qui prennent en compte les pétaoctets d'informations recueillies depuis de nombreuses années par des chercheurs expérimentés. Cela fait 20 ans qu'ESET reconnaît les antivirus traditionnels comme une solution incomplète. C'est la raison pour laquelle nous avons intégré des technologies proactives dans notre moteur d'analyse et mis en place progressivement plusieurs couches de protection contre les différents maillons de la chaîne cybercriminelle.

ESET fait partie des rares éditeurs de sécurité capables de fournir un niveau de protection élevé avec plus de 25 ans de recherche. Grâce au développement continu de nos technologies qui vont au-delà des signatures statiques standards, nous gardons une longueur d'avance sur les auteurs de logiciels malveillants. Notre combinaison unique de technologies endpoints et Cloud offre une sécurité inégalée contre les malwares.


ENJOY SAFER TECHNOLOGY™