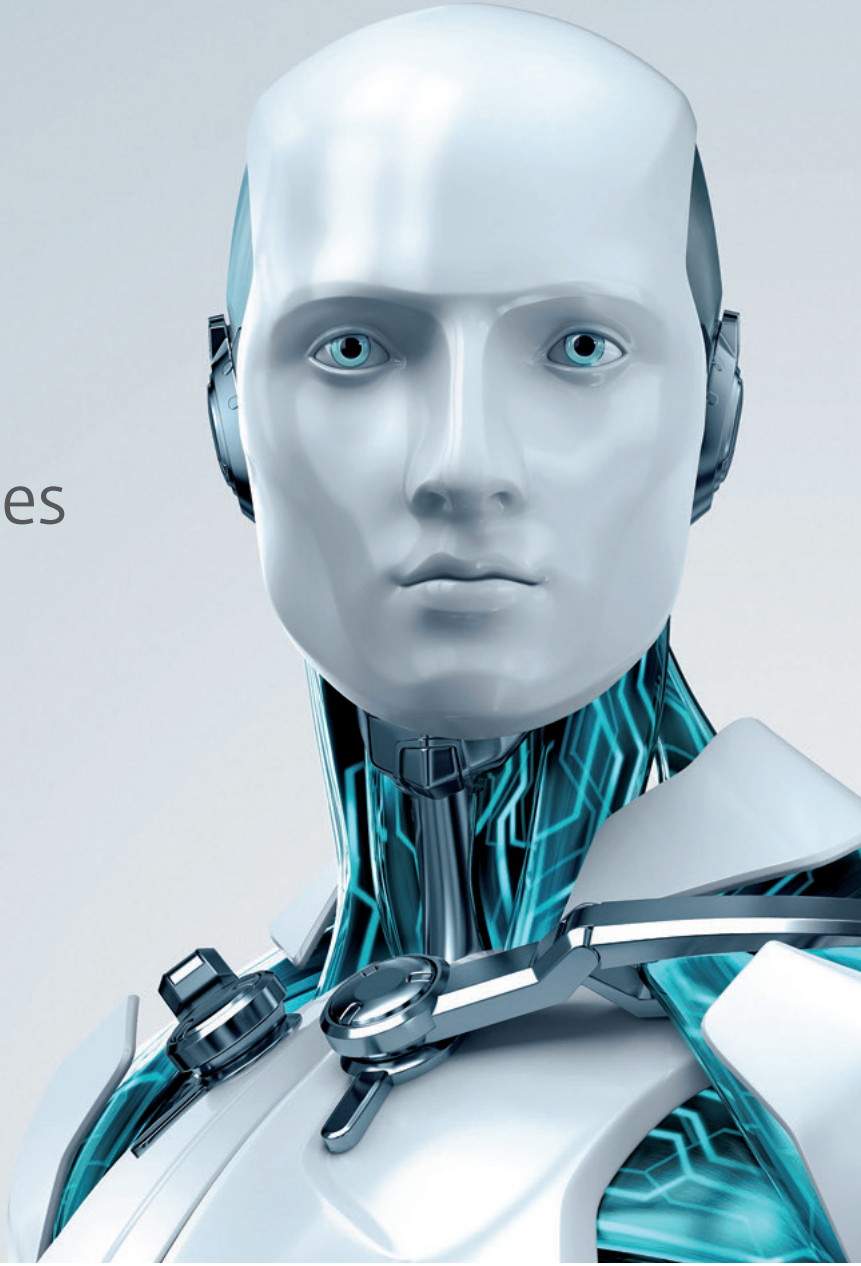
Technologie ESET

L'efficacité d'une approche multicouches



Version du document :
1.0

Auteurs :
Jakub Debski, Directeur du développement technologique
Juraj Malcho, Directeur de recherche
Peter Stancik, Chercheur en sécurité

ENJOY SAFER TECHNOLOGY™

SOMMAIRE

OBJECTIFS

Dans ce document, nous présentons l'utilisation par ESET de technologies multicouche, qui permettent d'aller au-delà du simple antivirus.
Nous expliquerons quelles couches supplémentaires sont utilisées pour résoudre des problèmes spécifiques et quels en sont les avantages pour les utilisateurs.

POURQUOI L'ANTIVIRUS EST ET N'EST PAS MORT ?

Les éditeurs d'antivirus les plus reconnus ont évolué avec l'envie d'aider les personnes rencontrant des problèmes avec des virus ou logiciels malveillants, c'est pourquoi ils ont développé des technologies qui répondent au large éventail de menaces auxquels les utilisateurs peuvent faire face. Aujourd'hui, l'antivirus est perçu comme un produit de base, et la sécurité est un sujet qui touche tout le monde, qu'ils en mesurent ou non les conséquences.

Récemment, nous avons constaté la prolifération d'une « nouvelle génération » d'entreprises qui ont peu d'expérience dans le développement de solutions anti-malware, mais qui commercialisent activement leurs solutions sur la base de « l'innovation » en rejetant les éditeurs actuels considérés comme « des dinosaures ». Comme la plupart des vendeurs de solution miracle, beaucoup de leurs affirmations sont mensongères et, ironiquement, leur capacité de détection repose généralement sur le moteur d'un autre éditeur établi. En effet, sur la douzaine de fournisseurs actuellement sur le marché, très peu ont l'expérience ou la capacité de développer leur propre technologie de détection. Les technologies d'ESET sont propriétaires et sont exclusivement développées en interne.

L'antivirus n'est pas mort. Cependant, la détection simple par signature statique qui – selon les nouveaux arrivants – compromet l'efficacité des anti-malware actuels, est seulement un composant infime du large éventail de technologies que déploie un produit de sécurité contre les menaces modernes.

MENACES MULTIPLES, PROTECTION MULTICOUCHES

Les éditeurs d'anti-malware qui sont encore sur le marché ont maintenu leurs parts de marché en évoluant pour contrer les menaces actuelles. Ces menaces ne sont pas statiques, et ne cessent d'évoluer depuis les années 2000. Les menaces d'aujourd'hui ne peuvent être combattues efficacement par des technologies des années 1990. Combattre les logiciels malveillants modernes est un jeu du chat et de la souris, où les cybercriminels sont qualifiés et (financièrement) motivés. C'est pourquoi les éditeurs de sécurité doivent constamment améliorer leurs produits, avec à la fois réactivité et proactivité pour fournir des solutions efficaces avec plusieurs niveaux, ainsi détecter et bloquer les malwares modernes. Un point et une méthode unique de défense ne suffisent pas. C'est une des raisons pour lesquelles ESET n'est plus seulement un éditeur d'antivirus, mais un éditeur de sécurité informatique.

MENACES MULTIPLES, PLATEFORMES MULTIPLES

De nos jours, les systèmes d'exploitation Microsoft ne sont pas les seules plateformes où les malwares sévissent. Le champ de bataille s'étend et les attaquants tentent de prendre le contrôle de plateformes auparavant inexplorées.

- Tout ce qui peut être contrôlé pour accomplir des activités malveillantes peut être utilisé pour des attaques
- Tout ce qui exécute du code pour traiter des données externes peut potentiellement être détourné par des logiciels malveillants

Les serveurs Linux ont été une cible majeure pour les attaquants (*Opération Windigo, Linux/Mumblehard*), les Macs fonctionnant sous OS X ont hébergé un des plus gros botnet jamais connu (*OSX/Flashback*), les mobiles sont des cibles communes (*Hesperbot*) et les attaques sur routeurs deviennent une sérieuse menace (*Linux/Moose*). Les rootkits s'attaquent aux matériels (Firmware ou utilisation du *rootkit UEFI*) et la virtualisation ouvre de nouveaux vecteurs d'attaques (Bluepill, VM escape vulnerabilities). Egalement, les navigateurs Internet et autres applications sont devenus aussi complexes que les systèmes d'exploitation, et leurs mécanismes de script sont souvent utilisés à des fins malveillantes (*Win32/Theola*).

DIFFERENTS VECTEURS DE DIFFUSION

Historiquement, le premier malware est apparu comme un processus à autoréplication, tout d'abord dans les systèmes, ensuite en tant que virus infectant les fichiers ou le disque, se propageant d'ordinateur à ordinateur

Comme l'utilisation d'Internet est devenue universelle, le nombre de façons de diffuser un malware s'est fortement accru. Les objets malveillants peuvent aussi être envoyés par email à travers des liens ou des pièces jointes, téléchargés depuis des pages web, déposés dans les documents par des scripts, partagés sur des périphériques amovibles, déployés à distance en profitant d'une autorisation et de mots de passes faibles, exécutés via des exploits ou installés par l'utilisateur final piégé par des techniques de piratage.

CONCEPTION D'UN MALWARE

Le temps où les malwares étaient écrits principalement par des adolescents pour s'amuser, ou pour se mettre en valeur est révolu. De nos jours, les malwares sont conçus avec pour objectif de voler des informations, et de les monétiser. D'importantes ressources financières sont investies tant par les criminels que par les gouvernements dans leur développement.

Pour rendre leur détection plus difficile, les malwares sont écrits dans différents langages de programmation, utilisent différents compilateurs et différents langages interprétés. Le code est obscurci et protégé par un logiciel qui rend la détection et l'analyse plus difficile.

Au niveau du réseau, les malwares utilisent moins de serveurs de commande et contrôle (C&C) codés pour envoyer des instructions et recevoir les données des systèmes compromis. Le contrôle décentralisé des botnets utilisant un réseau peer-to-peer est communément utilisé, et les communications cryptées rendent l'identification des attaques plus difficile. Les algorithmes de génération de domaine réduisent l'efficacité d'une détection basée sur le blocage d'URLs connues. Les hackers prennent le contrôle de sites web légitimes, qui ont une bonne réputation, et même des services de publicité légaux sont utilisés pour servir du contenu malicieux.

Les hackers ont de nombreuses façons d'éviter la détection, c'est pourquoi une solution simple à un seul niveau n'est pas suffisante pour fournir une protection. Chez ESET, nous pensons que cette protection multicouches, en temps réel et constante est nécessaire pour assurer un niveau de sécurité le plus élevé possible.

LES AVANTAGES DE LA TECHNOLOGIE ESET

Le moteur d'analyse d'ESET est au cœur de nos produits, et tandis que la technologie sous-jacente a été héritée de l'ancien antivirus, elle a été grandement étendue et améliorée et est **constamment développée pour apporter une réponse aux menaces modernes.**

Le but du moteur d'analyse est d'identifier les possibles malwares, et de prendre des décisions de façon automatique pour évaluer le niveau de malveillance.

Depuis des années, la performance d'ESET était basée sur des algorithmes intelligents et un assemblage manuel de code pour contrer les problèmes de performance causés par une analyse de code approfondie utilisant la technologie de sandboxing intégrée dans le produit. Cette approche a été améliorée. Maintenant, pour optimiser les performances, nous utilisons une **translation binaire et une émulation interprétée.**

Avec l'intégration de sandboxing dans le produit, vous devez émuler différents composants du matériel et du logiciel de l'ordinateur pour exécuter un programme dans un environnement virtualisé. Ces composants peuvent inclure la mémoire, le système de fichiers, le système d'exploitation, les APIs, et le CPU.

Auparavant, le CPU était imité en utilisant un code d'assemblage sur mesure. Cependant, il s'agissait d'un « code interprété », ce qui signifie que chaque instruction devait être imitée séparément. Avec la translation binaire, vous exécutez des instructions imitées nativement sur un CPU réel. Cela est beaucoup plus rapide, particulièrement dans le cas de boucles dans le code : introduire plusieurs boucles est une technique de protection commune à tous les exécutables où des mesures ont été appliquées pour les protéger d'une analyse faite par des produits de sécurité et des chercheurs.

Les produits ESET analysent des centaines de formats de fichier différents (exécutables, installeurs, scripts, archives, documents et bytecodes) dans le but de détecter avec précision les composants malicieux incorporés.

Le schéma ci-dessous présente les différentes technologies ESET, le moment et la manière dont elles peuvent détecter/bloquer une menace pendant son cycle de vie dans le système.

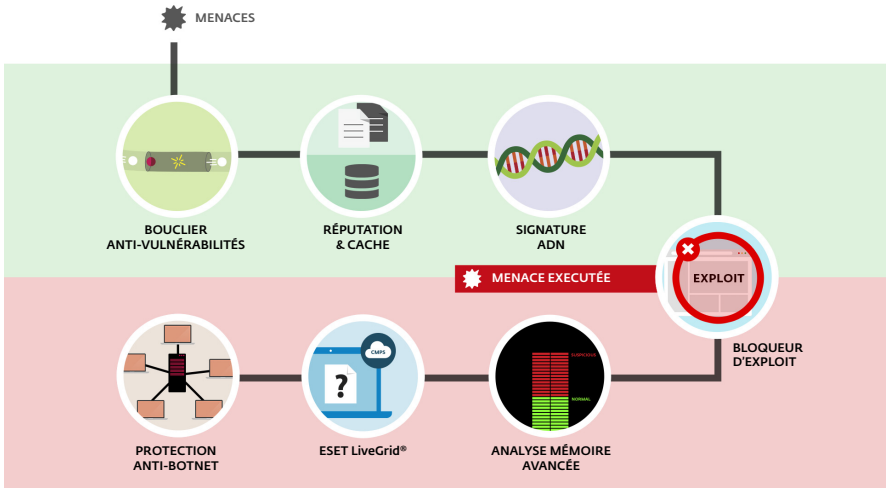
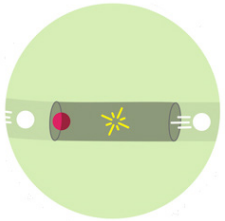


Figure 1 : Les couches de protection ESET



BOUCLIER ANTI-VULNÉRABILITÉS

Le bouclier ESET anti-vulnérabilités **est une extension du pare-feu qui améliore la détection des vulnérabilités connues au niveau du réseau.** En mettant en oeuvre la détection des vulnérabilités communes dans les protocoles *SMB*, *RPC* et *RDP*, **le bouclier anti-vulnérabilités protège** contre la propagation de logiciels malveillants, les attaques de réseau ciblées et l'exploitation de vulnérabilités pour lesquelles un patch n'a pas encore été créé ou déployé.

RÉPUTATION & CACHE

Lors de l'inspection d'un objet tel qu'un fichier ou une URL, avant toute analyse, nos produits vérifient le cache local (et **ESET Shared Local Cache**, dans le cas d'une licence ESET Endpoint Security) pour les objets malicieux connus ou mis sur liste blanche. Cela **améliore la performance d'analyse.** Ensuite, notre **système de réputation ESET LiveGrid® est sollicité pour la réputation d'objet** (i.e si l'objet a déjà été vu ailleurs et classifié comme malicieux ou autrement). Cela **améliore l'efficacité d'analyse et permet le partage plus rapide de malware identifié avec nos clients.** Appliquer des listes noires URL et vérifier la réputation empêche les utilisateurs d'avoir accès à des sites au contenu malveillant, et des sites de phishing.

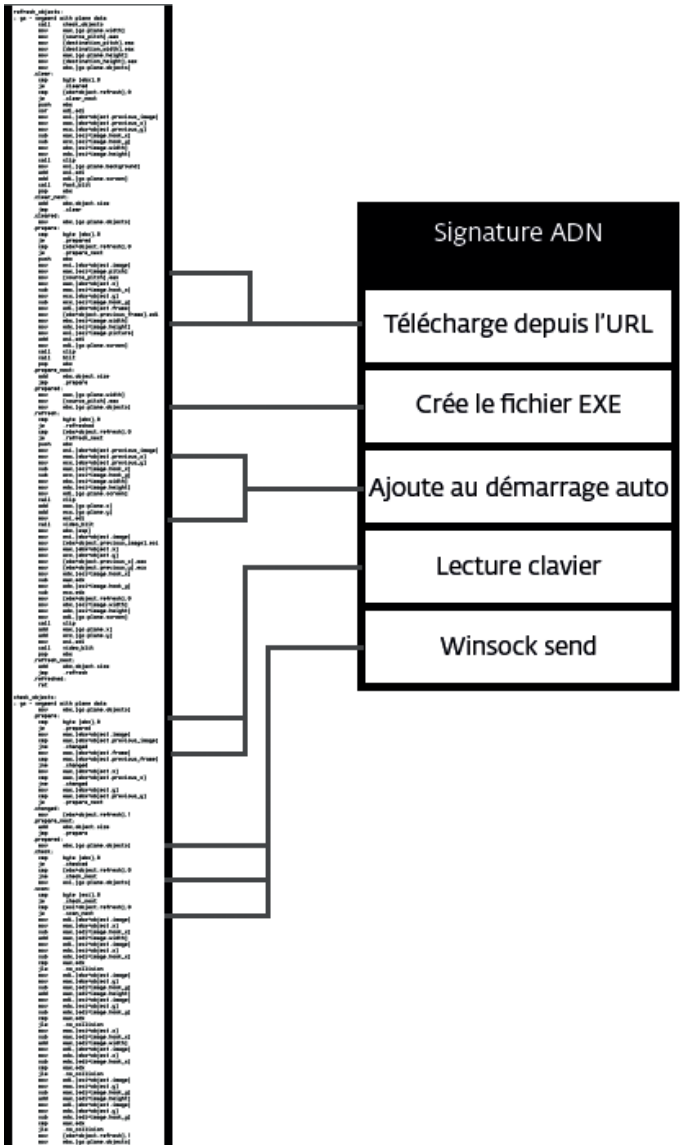
SIGNATURES ADN

Les types de signature vont d'un hachage très spécifique (utile, par exemple, lorsqu'on vise un binaire malicieux bien précis, ou une version spécifique du malware, à des fins statistique ou simplement pour donner un nom de détection plus précis au malware que nous avons identifié précédemment de façon heuristique) aux **signatures ADN ESET**, qui **sont des définitions complexes du comportement malveillant et des caractéristiques du malware.**.

La reconnaissance géométrique utilisée par les antivirus de la vieille école peuvent être contournés facilement, par une simple modification du code, ou encore par des techniques d'obscurcissement. Cependant, le comportement des objets ne peut pas être changé si facilement. Les signatures ADN ESET sont précisément conçues pour tirer parti de ce principe. Nous réalisons une analyse profonde du code, en extrayant les « gènes » responsables de ce comportement. **De tels gènes comportementaux contiennent beaucoup plus d'informations que les indicateurs de compromis (IOCs)** dont certains sont appelés « solutions de la nouvelle génération » et prétendent être « la meilleure alternative » à la détection par signature. Les gènes de comportement ESET sont utilisés pour construire les Signatures ADN, elles-mêmes utilisées pour évaluer le code suspect, s'il est trouvé sur le disque ou dans la mémoire du processus en cours.

De plus, notre moteur d'analyse extrait de nombreux gènes discriminateurs, utilisés pour la détection d'anomalie : tout ce qui ne semble pas légitime est potentiellement malveillant.

Selon le seuil ajustable et la correspondance aux conditions, les Signatures ADN peuvent identifier des échantillons de malware connu, de nouvelles variantes d'une famille de malware connue ou même inconnue, ou encore un malware inconnu qui contient des gènes indiquant un comportement malveillant. En d'autres termes, **une signature ADN bien lisible peut détecter des dizaines de**



milliers de variantes de malwares qui y sont associés et permet à notre logiciel antivirus de ne pas seulement détecter les malwares que nous connaissons déjà, ou que nous avons déjà vu, mais **aussi d'identifier les nouveaux, dont les variantes étaient auparavant inconnues**. De plus, la clusterisation automatisée et le recours à l'apprentissage automatique de l'ensemble de notre échantillon malveillant nous permet d'identifier de nouveaux gènes malveillants, de nouveaux comportements pour renforcer la détection de notre moteur d'analyse. De tels gènes peuvent être facilement intégrés dans une liste blanche pour s'assurer qu'ils ne génèreront pas de faux positifs.

BLOQUEUR D'EXPLOIT

Les technologies ESET protègent de nombreuses sortes de vulnérabilité, et à différents niveaux : notre moteur d'analyse couvre les exploits qui apparaissent dans des fichiers de document ; Le bouclier anti-vulnérabilités se situe au niveau des communications ; et enfin, le bloqueur d'Exploit bloque le processus d'exploitation lui-même.

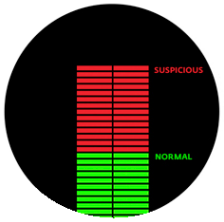
Le bloqueur d'Exploit surveille les applications fréquemment exploitées tels que les navigateurs, les lecteurs de PDF, les clients de messagerie, Flash, Java, etc. **Au lieu** de simplement viser un *identifiant CVE* en particulier, **il se concentre sur les techniques d'exploitation.** Chaque exploit est une anomalie dans l'exécution du processus, et nous cherchons les anomalies qui suggèrent la présence de techniques d'exploitation. La technologie étant en constant développement, les nouvelles méthodes de détection sont ajoutées régulièrement pour couvrir les nouvelles techniques d'exploitation. Une fois déclenché, le comportement du processus est analysé, et s'il est considéré suspicieux, **la menace peut être immédiatement bloquée sur la machine**, et les métadonnées liées à l'attaque sont envoyées à notre système cloud ESET LiveGrid. Ces informations sont traitées et corrélées, ce qui nous permet **de découvrir de nouvelles menaces auparavant inconnues, qu'on appelle les attaques zero-day.**

Le bloqueur d'exploit apporte une couche de protection supplémentaire, se rapprochant un peu plus des attaquants, grâce à une technologie complètement différente des techniques de détection qui se concentrent sur l'analyse de codes malveillants.

ANALYSE MÉMOIRE AVANCÉE

L'analyse mémoire avancée est **une technologie ESET unique, qui s'adresse** efficacement aux malwares modernes – utilisation importante de **l'obscurcissement et/ou le cryptage**.

Ces tactiques de protection malware, souvent utilisées dans les exécutables et les protecteurs de code, posent des problèmes pour les approches de détection qui utilisent des techniques d'émulation ou de sandboxing. Qui plus est, si la vérification est faite en utilisant un émulateur ou un sandboxing virtuel/physique, il n'y a aucune garantie que durant l'analyse, le malware dévoilera son comportement malveillant, ce qui aurait permis de le classifier comme tel. Le malware peut être obscurci de telle manière que toutes les voies d'exécutions ne peuvent être analysées : il peut contenir un code conditionnel ou ponctuel ; et très fréquemment, il peut télécharger de nouveaux composants au cours de sa durée de vie.



Pour régler ces problèmes, l'Analyse Mémoire Avancée surveille le comportement des processus malveillants et les analyse une fois qu'ils se dévoilent en mémoire. Cela complète la fonctionnalité plus traditionnelle d'analyse de code proactive de pré-exécution ou sur-exécution.

Egalement, les processus sains peuvent soudainement devenir malveillants en raison d'une injection de code ou d'exploitation. Pour ces raisons, réaliser une seule analyse n'est pas suffisant. Il est nécessaire d'effectuer une surveillance constante, et c'est là le rôle de l'Analyse Mémoire Avancée. **Lorsqu'un process fait un appel système depuis une nouvelle page exécutable, l'Analyse Mémoire Avancée effectue une analyse de code comportemental, en utilisant les signatures ADN ESET.**

L'analyse de code est réalisée pour la mémoire exécutable standard mais aussi pour .NET MSIL (Microsoft Intermediate Language), utilisé par les auteurs de malware pour entraver les analyses dynamiques. En raison de l'implémentation de smart caching, l'analyse mémoire avancée ne cause pas de détérioration dans la vitesse de traitement.

L'analyse mémoire avancée s'accorde bien avec le bloqueur d'exploit. Contrairement à ce dernier c'est une méthode post-exécution, ce qui signifie qu'il y a un risque que certaines activités malveillantes soient déjà apparues. **Néanmoins, c'est une protection de dernier ressort** si un attaquant réussit à contourner les autres niveaux de protection.

Par ailleurs, la nouvelle tendance est aux malwares avancés : certains codes malveillants agissent maintenant « en mémoire seulement » sans avoir besoin de composants persistants dans le système de fichier qui peut être détecté de manière classique. À la base, ces malwares n'apparaissaient que sur les serveurs, en raison de leur grande disponibilité – puisque les systèmes de serveur peuvent rester actifs pendant des mois voire des années, les processus malveillants peuvent rester en mémoire indéfiniment sans avoir besoin de survivre à un redémarrage – mais les récentes attaques sur les entreprises nous indiquent un changement de cette tendance, les postes de travail sont désormais également ciblés. **Seule une analyse de mémoire peut découvrir ces attaques malveillantes, et ESET est prêt à affronter cette nouvelle tendance grâce à son analyse de mémoire avancée.**

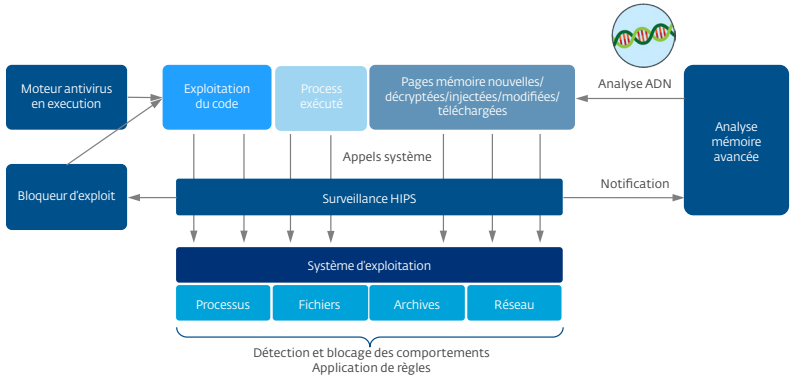


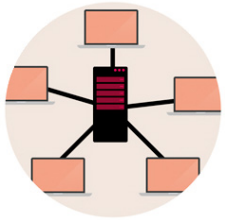
Fig.2: Comment la détection de comportement d'ESET fonctionne ?

ESET LIVEGRID

ESET LiveGrid est une des technologies ESET basée sur le cloud. Elle permet de surveiller les applications inconnues et potentiellement malveillantes, ainsi que d'autres menaces possibles, et de les enregistrer sur le cloud ESET via le système de feedback ESET LiveGrid. Les **échantillons collectés sont soumis à un sandboxing et une analyse du comportement,** qui aboutissent à la création de signatures automatiques si des caractéristiques malveillantes sont confirmées. Les clients ESET s'informent de ces détections automatiques via le système de réputation ESET LiveGrid, sans avoir à attendre la prochaine mise à jour de base de signatures. Le temps d'exécution du mécanisme est d'environ 20 minutes, ce qui permet une détection efficace des menaces émergentes même avant que les signatures régulières ne soient délivrées aux ordinateurs des utilisateurs.

PROTECTION ANTI-BOTNET

La communication avec les C&C est coûteuse à changer pour les auteurs de malware. **La protection Botnet d'ESET est éprouvée à la fois pour détecter les communications malveillantes utilisées par les botnets, mais également pour identifier les processus fautifs.**



Les signatures du réseau d'ESET prolongent la technologie de protection Botnet pour aborder des problèmes généraux associés à l'analyse du trafic réseau. Elles **permettent une détection du trafic malveillant plus rapide et plus flexible.** Les signatures de standards de l'industrie comme Snort ou Bro permettent de détecter de nombreuses attaques, mais les Signatures ESET network sont spécifiquement conçues pour cibler les vulnérabilités du réseau, les kits d'exploits, et en particulier les communications par malware avancé.

La capacité de réaliser des analyses du trafic réseau sur les postes de travail a des avantages. Cela nous permet d'identifier exactement quel processus ou module est responsable d'une communication malveillante et permet d'entreprendre une action contre l'objet identifié. Parfois cela permet également que le cryptage de la communication soit contourné.

Protection réactive vs proactive

Tandis que les signatures ADN sont excellentes pour détecter jusqu'à une famille entière de malwares, elles doivent être distribuées aux utilisateurs pour les protéger. C'est également le cas pour le moteur d'analyse, les heuristiques ou n'importe quel élément visant de nouvelles menaces. De nos jours, la communication avec ESET LiveGrid est nécessaire pour assurer le niveau le plus haut de protection, et ce pour de nombreuses raisons :

- **Une analyse hors-ligne est principalement réactive.** Désormais, être proactif ne signifie plus seulement avoir les meilleurs heuristiques dans notre produit. Aussi longtemps que vos outils de protection seront disponibles pour un hacker, peu importe si vous utilisez des signatures, des heuristiques ou des classificateurs d'apprentissage automatique : un auteur de malware peut expérimenter avec votre technologie de détection et modifier le malware jusqu'à ce qu'il ne soit plus détecté, et seulement le diffuser ensuite. ESET LiveGrid contre cette stratégie de malware.
- **Les mises à jour ne sont pas en temps réel.** Les mises à jour peuvent être publiées plus souvent, et elles peuvent même être envoyées aux utilisateurs à quelques minutes d'intervalle. Peut-on faire mieux ? Oui : ESET LiveGrid offre une protection instantanée, en fournissant les informations chaque fois que cela est nécessaire.
- **Les logiciels malveillants essaient de passer sous le radar.** Les auteurs de malware, principalement dans le cas d'un cyber espionnage, tentent d'éviter toute détection tant que cela est possible. Les attaques ciblées – par opposition aux distributions massives telles que les vers par mail – déploient un malware à un petit nombre de cibles, quelques fois à une seule. Nous utilisons ce fait contre les auteurs de malware : les objets qui ne sont pas populaires et qui n'ont pas bonne réputation sont considérés comme étant potentiellement malveillants et sont ainsi analysés en détail sur chaque poste de travail, ou soumis à une analyse automatisée détaillée via ESET LiveGrid. Le système de réputation ESET LiveGrid contient des informations sur les fichiers, leurs origines, les similitudes, certificats, URLs et adresses IP.

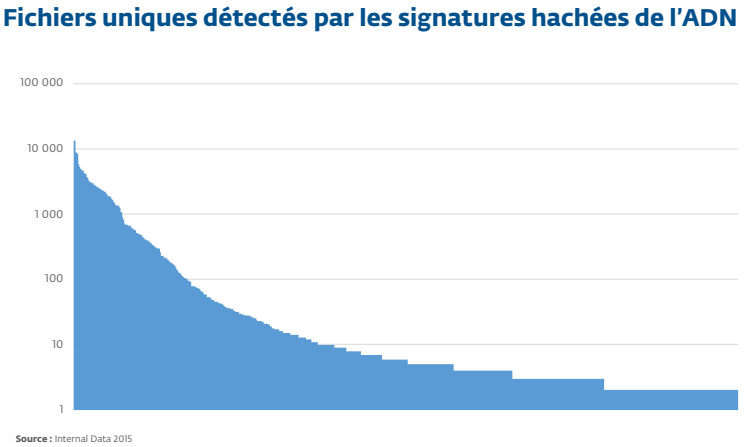
Protection par ESET LiveGrid

Le moyen le plus simple de fournir une protection en utilisant un système cloud est par l'utilisation d'une liste noire et de la technique de hachage. Cela fonctionne bien à la fois pour les fichiers et les URLs, mais il n'est possible de bloquer que les objets qui correspondent exactement au hachage. Cette limitation a mené à l'invention d'un hachage flou. Le hachage flou prend en considération la similitude binaire des objets, comme les objets similaires ont un hachage identique ou presque.

ESET a monté le hachage flou au niveau supérieur. Nous ne réalisons pas de hachage des données, mais un hachage du comportement décrit dans les signatures ADN. En utilisant un hachage ADN nous sommes capables de bloquer des milliers de variantes différentes de malware instantanément.

Fig. 3 : Nombre de fichiers uniques (ordonnée) détectés par les hachés ADN individuels (abscisse)

Fournir une liste noire instantanée aux utilisateurs n'est pas l'unique objectif



d'ESET LiveGrid. Si un utilisateur décide de participer au processus de soumission d'échantillon, chaque fois qu'un nouvel échantillon à la réputation douteuse est identifié, il est envoyé à ESET pour une analyse plus approfondie. Pour utiliser pleinement tout le potentiel de la protection basée sur le cloud, les utilisateurs devraient habiliter ESET LiveGrid Feedback System, qui nous permet de collecter tout échantillon suspicieux à la réputation douteuse et de l'analyser de manière plus approfondie.

TRAITEMENT AUTOMATISÉ ET MANUEL DES ÉCHANTILLONS

Chaque jour, ESET reçoit des centaines de milliers d'échantillons, qui sont traités automatiquement, semi-automatiquement et manuellement après pré-traitement et regroupement. **L'analyse automatisée est effectuée par des outils développés en interne sur un éventail de machines virtuelles et réelles.** La classification est réalisée en utilisant différents attributs extraits lors de l'exécution, selon une analyse de code statique et dynamique, les changements introduits dans le système d'exploitation, les structures du réseau de communication, les similitudes avec d'autres échantillons de malware, les caractéristiques ADN, les informations de structurelles et la détection d'anomalie.

Tous les classificateurs automatisés ont des inconvénients :

- **Le choix de critères discriminateurs pour la classification n'est pas anodin** et doit être réalisé en utilisant la connaissance d'experts dans le domaine du malware.
- **Les classificateurs d'apprentissage automatique nécessitent la participation d'experts** pour vérifier les apports utilisés pour l'apprentissage. Avec un traitement totalement automatisé, où les échantillons triés par le système seraient utilisés comme apport au système, un effet boule de neige de cercle vertueux le rendrait rapidement instable. « Garbage in – Garbage out ».
- L'apprentissage automatique ne comprend pas les données, **et même si les informations sont statistiquement correctes, cela ne signifie pas qu'elles sont valides.** Par exemple, l'apprentissage automatique ne peut pas distinguer les nouvelles versions de logiciel sain des versions qui ne le sont pas, il ne peut pas distinguer un updater lié à une application saine d'un téléchargeur utilisé par un malware. Enfin, il ne peut pas reconnaitre lorsque des composants de logiciels sains sont utilisés à des fins malveillantes.
- Avec l'apprentissage automatique, ajouter de nouveaux échantillons à un processus d'apprentissage peut causer de faux positifs, et enlever ces faux positifs peut réduire l'efficacité d'une réelle détection positive.
- Alors qu'un traitement automatisé permet des réponses instantanées aux nouvelles menaces par la détection via ESET LiveGrid, un traitement des échantillons supplémentaires par des ingénieurs est crucial pour assurer la plus haute qualité, le meilleur taux de détection, et le moins de faux positifs possible.

Services de réputation

ESET LiveGrid fournit aussi une réputation des objets. Nous évaluons la réputation de différentes entités y compris les fichiers, certificats, URLS et adresses IP. Comme décrit précédemment, la réputation peut être utilisée pour identifier de nouveaux objets malveillants, ou des sources d'infection. Il y a cependant d'autres utilisations possibles.

Liste blanche

La liste blanche est une fonctionnalité qui permet de réduire le nombre de temps nécessaire au moteur d'analyse pour analyser un objet. Si nous sommes sûrs qu'un objet n'a pas été modifié et qu'il est sain, alors il n'est pas nécessaire de réaliser une analyse dessus. Cela a un impact très positif sur les performances ce qui permet aux produits ESET d'être peu invasifs. Comme nous le rappelons « le code le plus rapide est celui qui ne s'exécute pas du tout ». Nos listes blanches sont constamment adaptées pour refléter la réalité du monde logiciels.

Collecte intelligente d'informations

Si un utilisateur décide d'envoyer des données vers le ESET LiveGrid, nous utilisons ces informations pour le suivi et la surveillance des menaces au niveau mondial. Ces informations nous fournissent des données à analyser, **nous permettent de nous concentrer sur les cas les plus urgents et les plus problématiques, mais également d'observer les tendances des logiciels malveillants, de planifier et prioriser le développement des technologies de protection.**

A PROPOS DES FPS ET IOCS

Les indicateurs de compromission (IOCs – Indicator of Compromise) sont perçus comme un point important dans la sécurité des entreprises modernes, mais ils sont loin d'être spécifiques ou avancés, même si ils sont parfois mis en avant par les éditeurs de sécurité « nouvelle génération ». L'illustration ci-dessous est une répartition des indicateurs les plus répandus et ce sur quoi ils se basent*. Comme nous pouvons le constater, les caractéristiques présentées sont extrêmement basiques : dans un quart des cas cela concerne les MD5, puis les noms de fichiers ... Ces résultats montrent clairement que ce n'est pas une méthode appropriée pour la prévention et le blocage, même si elle peut être utile pour la criminalistique. C'est assez ironique de constater que certains éditeurs « nouvelle génération » qui rejettent la méthode « obsolète » de détection basée sur les signatures utilisée dans les « anciens antivirus » vantent les mérites de ces indicateurs qui sont finalement trop faibles pour détecter les fichiers ou événements malveillants.

* Source : IOC Bucket, Avril 2015. IOC Bucket est une plateforme de partage d'informations sur les menaces basée sur une communauté libre.

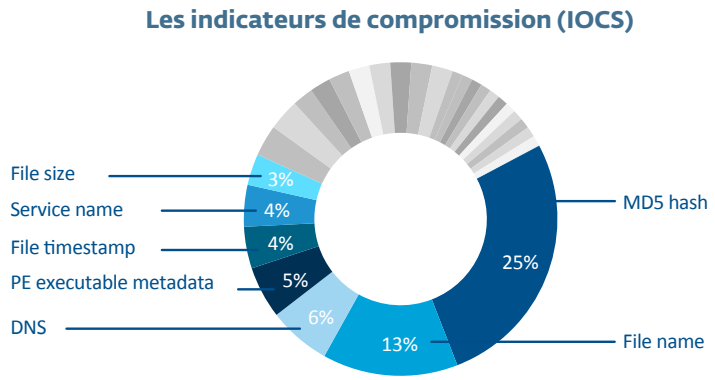


Fig 4 : Analyse des indicateurs de compromission – IOC Bucket (Echantillon Avril 2015)

CONCLUSION

Dans la sécurité, il n'y a pas de solution miracle. Les menaces d'aujourd'hui sont dynamiques et très souvent ciblées. Elles nécessitent une approche multicouches basée sur des technologies intelligentes et proactives qui prennent en compte les pétaoctets de données recueillies depuis de nombreuses années par des chercheurs expérimentés. Depuis 20 ans, ESET reconnait que l'antivirus – l'approche traditionnelle – est une solution incomplète, à tel point que nous avons intégré des technologies proactives dans notre moteur d'analyse et progressivement mis en œuvre différentes couches de protection pour frapper à différents niveaux de la chaîne de cybercriminalité.

ESET est l'un des rares éditeurs de sécurité à fournir un niveau élevé de protection basé sur plus de 25 années de recherche. Cela nous permet aujourd'hui d'être présent face aux logiciels malveillants, de faire évoluer constamment nos technologies au-delà des standards et des signatures statiques. Notre combinaison unique de technologies offre un niveau de sécurité avancé contre les logiciels malveillants du marché.