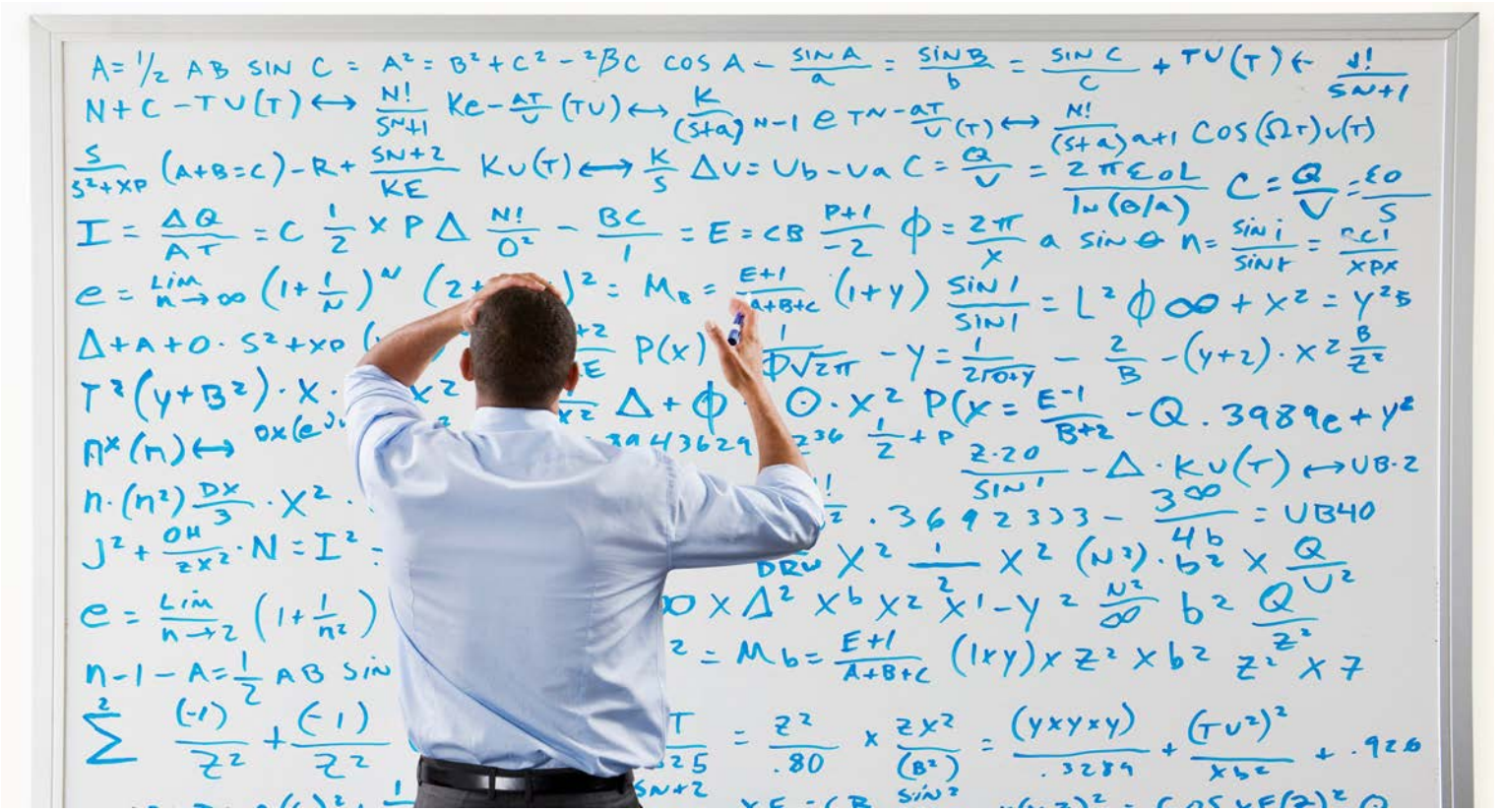
Comparatif entre les solutions de prévention et l'approche « détecter et réagir »



Risques associés à l'exécution des logiciels malveillants

Sur Internet, il n'y a que des victimes ou des victimes potentielles. Tout le monde est concerné, les particuliers comme les grandes entreprises. Chaque minute qui passe, de nouveaux appareils connectés deviennent la cible potentielle d'une attaque. Dans la course à l'extension et au renforcement de la protection, les équipes chargées de la sécurité doivent faire face à une complexité accrue, ce qui représente un défi supplémentaire. En raison de la multiplication des produits, des événements et de la surveillance, il est de plus en plus difficile de trouver les indicateurs pertinents et exacts d'une compromission. La sécurité se retrouve alors réellement menacée. Cette spirale de la complexité réduit la vigilance et la réactivité de l'équipe chargée de la sécurité, ce qui, au final, augmente le coût réel de la sécurité opérationnelle.

Les entreprises ne se confrontent pas à cette réalité. La prolifération des fournisseurs et des produits, résultant d'une augmentation vertigineuse des besoins et de la croissance de l'économie de la sécurité, a créé une grande diversité d'approches visant à résoudre les différents problèmes de sécurité. Cependant, dans leur quête d'un nouvel angle d'attaque, souvent centré sur les informations, la majorité de ces solutions ont créé par inadvertance de nouveaux problèmes sans améliorer la sécurité.

Certains types de logiciels malveillants sont présents, au moins en partie, dans presque tous les incidents de sécurité (dont 10,6 % en interne[1]). Ainsi, l'un des principaux défis que les équipes chargées de la sécurité doivent relever consiste à se doter d'une stratégie de sécurité efficace au niveau des points de terminaison. Dans ce livre blanc, nous analyserons les stratégies actuelles les plus populaires en termes de détection des attaques. Nous traiterons exclusivement des pièges liés aux stratégies post-exécution et passerons en revue l'élément central sous-jacent de la détection des logiciels malveillants qui pose tant de problèmes à la plupart des entreprises.

Nous soutenons que, finalement, le meilleur remède reste la véritable prévention à l'aide de technologies et stratégies pré-exécution (et non pas post-exécution). Nous pensons également qu'une solution de prévention efficace réduit les coûts et la complexité relatifs à la sécurité.

Évolution de la stratégie

Les stratégies de détection des attaques peuvent se diviser en trois grandes catégories, selon le moment où l'intervention est prévue : avant l'exécution du logiciel malveillant (pré-exécution), pendant son exécution (exécution) ou après son exécution (post-exécution).

- Basé sur le hachage - (semi-) Automatisé
- Règles génériques et heuristiques humaines (signature manuelle)
- Basé sur la réputation des fichiers - Cloud/en local (fin des années 2000)
- Politique de liste blanche uniquement (fin des années 2000)
- Modèles basés sur l'apprentissage automatique (2012)

- Basé sur la mémoire (signature)
- Système de détection des intrusions (IDS)
- Détection des vulnérabilités (exploits)

- Système de détection des intrusions (IDS)
- Analyse de la mémoire
- Comportemental
- Analyses - Gestion des informations et des évènements de sécurité (SIEM)
- Détecter et réagir – Détection et réaction aux menaces au niveau des points de terminaison (ETDR, Endpoint Threat Detection and Response)

Les premières technologies de détection des logiciels malveillants utilisaient des signatures heuristiques et génériques pour détecter un fichier malveillant dès son écriture sur un disque. Les éditeurs de logiciels antivirus pouvaient auparavant s'en sortir en écrivant manuellement les signatures, car les types de logiciels malveillants ne changeaient pas souvent. Pendant un moment, le coût de la gestion des solutions de sécurité antivirus au sein de l'entreprise était en général fixe. Une fois installée, la solution antivirus fonctionnait automatiquement pour détecter et corriger les programmes malveillants connus. Ces solutions antivirus, dotées de signatures heuristiques et basées sur des émulations, se sont imposées. Mais les temps ont changé.

Au milieu des années 2000, une vague de logiciels malveillants et rootkits polymorphes et évoluant rapidement est apparue : dotés de nombreux stratagèmes, ils contournaient les protections traditionnelles des antivirus. Pour conserver des taux élevés de détection, les fournisseurs de solutions de sécurité ont créé des solutions automatisées de traitement des logiciels malveillants équipées de technologies de hachage. La principale lacune du hachage, c'est que chaque spécimen malveillant, même si la différence est minime, semble totalement différent et nouveau, une fois haché. La vague suivante de logiciels malveillants polymorphes et destructeurs de hachage s'est servie de cette limite des technologies de hachage automatisées. Le coût des logiciels malveillants non détectés augmentant rapidement pour les entreprises, les éditeurs se sont donc mis à proposer des services de réparation et correction. Pour contrer les problèmes de détection, les fournisseurs de solutions de sécurité ont ajouté de nouvelles technologies d'analyses de mémoire, de réputation et de comportement. Les couches de sécurité se sont multipliées au fil du temps. Ces nouvelles stratégies de détection des logiciels malveillants ont été créées pour répondre à l'échec des solutions antivirus en termes de prévention des attaques. Malheureusement, d'un point de vue collectif dans le secteur de la sécurité, cette situation a empêché d'investir dans des solutions de prévention ainsi que dans d'autres technologies qui pouvaient contribuer à réduire le coût de gestion de la sécurité.

C'est à cette époque que des solutions basées uniquement sur les politiques ont été introduites. Seuls les fichiers connus pouvaient être exécutés (liste blanche). Cette approche était limitée à des utilisations spécifiques dont le contrôle des modifications était très restrictif, telles que les systèmes de points de vente.

Aujourd'hui, la plupart des solutions de sécurité « de pointe » répondent à l'augmentation des cyberattaques par l'analyse de logiciels malveillants post-exécution qui inclut une surveillance permanente des points de terminaison et une réaction rapide aux attaques. Bien que cette solution semble répondre aux besoins du moment, il est nécessaire de comprendre les implications de cette nouvelle tendance et de chercher à améliorer davantage la sécurité.

Vous vous préparez à un scénario catastrophe ?

L'exécution d'un programme malveillant sur un point de terminaison comporte toujours des risques. Une compromission arrive à l'étape de la post-exécution uniquement lorsque les solutions de prévention préalables ont échoué. Ce type d'analyse de logiciels malveillants compte sur le fait que les actions de ce logiciel vont trahir son comportement malveillant ou que l'entreprise touchée sera en mesure d'utiliser cette nouvelle couche de surveillance pour assurer la reprise après une attaque. La surveillance post-exécution consigne et analyse le comportement des applications et généralement, analyse et archive également la majorité du trafic réseau. Tout est fait pour détecter et restaurer les systèmes en cas de scénario catastrophe de compromission. Le mot clé en l'occurrence est « catastrophe ». Nous pensons que le secteur de la sécurité peut faire bien mieux qu'attendre qu'un scénario catastrophe se produise avant de prendre des mesures.

Revenons au problème de l'exécution des logiciels malveillants et de l'analyse sur un point de terminaison. Il faut d'abord répondre à la question suivante : quels sont les éléments que ces solutions devraient surveiller ? L'objet de la surveillance reste un point important. Si une solution consigne la plupart des données de comportement des applications, du système d'exploitation et du réseau en anticipation d'un scénario catastrophe, elle collecte d'innombrables données.

Les solutions post-exécution sont visibles. Leur autonomie étant limitée, elles ne peuvent tout simplement pas risquer de rater un élément important. Elles doivent donc collecter et analyser un nombre incalculable de données. Cela inclut les écritures sur disque (et processus connexes), les événements d'exécution, certains sous-ensembles de réglementations, les communications RPC, les activités utilisateurs (notamment les URL consultées et les cookies écrits), les requêtes DNS et les données de suivi réseau, tels que pcap ou NetFlow, pour chaque opération.

La quantité de données augmente rapidement. Considérons que ces systèmes collectent 1 mégaoctet par heure et par hôte (ou 1 000 kilooctets de dossiers après compression). Si vous multipliez ce chiffre par 24 heures pour 1 000 hôtes, vous obtenez 24 millions d'événements ou 24 gigaoctets de données par jour. Au bout de 90 jours, vous avez récolté 2,1 milliards de dossiers, soit 2,1 téraoctets de données. Imaginez la quantité de données collectée par une entreprise dotée de 50 000 ou 100 000 hôtes.

Même avec cette approche contraignante d'extraction de données, il est possible que les défenseurs du système ne soient pas capables de retrouver une aiguille dans une botte de foin. Cette approche est extrêmement complexe et gaspille de l'énergie, de la mémoire, de l'espace disque et des ressources réseau. Analysons les coûts cachés pour une entreprise si une solution de sécurité utilise uniquement l'approche « détecter et réagir » après l'exécution du logiciel malveillant.

Coûts de gestion

La collecte et la maintenance du volume d'informations nécessaire à l'exécution d'une solution « détecter et réagir » sont des engagements qui augmentent avec le temps, tout comme le coût de l'extraction de valeur issue des informations. Les entreprises doivent être conscientes des préoccupations et coûts cachés suivants :

- Analyse d'événement de sécurité : davantage d'événements de sécurité impliquent davantage d'analyses et donc une augmentation des coûts.
- Performances du système au niveau des points de terminaison : la surveillance permanente des points de terminaison conduit à des goulets d'étranglement, alors même que la collecte de données inutiles surcharge un peu plus le point de terminaison.
- Recherche sur le Cloud/bande passante réseau : le fournisseur de solution de sécurité paie le stockage sur le Cloud, mais c'est l'entreprise qui paie l'utilisation des données réseau.
- Analyse du Big Data sur site : l'hébergement et la gestion d'une solution Big Data sur site afin de gérer le volume de données augmentent la complexité ainsi que les coûts matériels et logiciels.

Préoccupations relatives à la confidentialité

Les solutions qui collectent et stockent la majorité des événements système pour des opérations de détection et réaction pourraient finir par collecter davantage d'informations que nécessaire ou souhaité. Les contrôles d'accès, l'emplacement, les périodes de conservation et les politiques de chiffrement des données collectées peuvent varier en fonction des éditeurs.

Certaines solutions de sécurité dépendent des données Open Source pour obtenir des informations sur les fichiers suspects. Ces sources se révèlent souvent inutiles, car la détection des logiciels malveillants pré-exécution n'est plus utilisée et les fournisseurs de solutions de sécurité n'investissent pas suffisamment dans l'amélioration des fonctionnalités de détection de fichiers.

Par exemple, la famille de logiciels malveillants Dyre a été détectée pendant deux jours consécutifs en juin. Un système post-exécution interrogeant tous les fournisseurs le 4 juin n'aurait pas reconnu le fichier comme logiciel malveillant, sur la base des connaissances collectives du secteur. Il existe de nombreux exemples de logiciels malveillants qui ne sont pas identifiés à l'origine comme malveillants et qui ne seront pas signalés avant des semaines, des mois, voire des années. De tels retards soulignent le fait que les systèmes doivent combler les lacunes existantes en termes d'identification des logiciels malveillants sans dépendre de solutions d'analyse réactives de détection de fichiers.

What You See is What You Get (WYSIWYG, « tel affichage, tel résultat »)

Lorsque vous laissez un logiciel malveillant s'exécuter, vous créez des défis techniques majeurs, car vous étendez son champ d'action, plutôt que de limiter ses options. Vous trouverez ci-dessous des exemples de points faibles des nouvelles technologies basées sur l'approche « détecter et réagir ».

Bons et mauvais comportements

Au cours d'une analyse post-exécution de logiciels malveillants, les solutions de sécurité des points de terminaison doivent surveiller le fichier suspect dans son environnement naturel pour détecter, consigner et bloquer les événements afin d'assurer une reprise après les attaques. Cependant, même sous surveillance, il est très difficile de prévoir le moment où un spécimen malveillant, tel que Rombertik, va se révéler.[2,3,4] Il peut se passer plusieurs jours avant qu'il n'exécute son code malveillant. L'exécution du programme malveillant peut aussi dépendre d'une action utilisateur, comme faire défiler un document jusqu'à la seconde page. De nombreuses recherches ont tenté de résoudre certains de ces problèmes, mais les solutions mises en place ont été contournées à nouveau.[5,6] Une des alternatives possibles serait de surveiller toutes les applications en permanence dans l'attente d'un événement de sécurité, ce qui nous ramène au problème du coût de gestion de la sécurité.

À quel moment est-il trop tard pour agir ?

Une technologie de surveillance peut-elle détecter le premier « événement négatif » ? L'installation d'un pilote est-elle un événement malveillant en soi ? Bien souvent, la réponse est non, mais à partir du moment où un pilote noyau malveillant s'exécute, il est sûrement trop tard pour sauver le système. Ce ne sont que quelques exemples des inconvénients de la surveillance post-exécution. Le plus souvent, une série de comportements constitue un comportement malveillant. Cependant, il est peut-être trop tard pour bloquer le logiciel malveillant si cette détermination n'est pas faite à temps, et plus important encore, de manière systématique. Nous en revenons au bon vieux jeu du chat et de la souris qu'est la « détection de signature », dans lequel les défenseurs tentent de détecter un problème le plus tôt possible alors que les attaquants essaient de s'échapper en mélangeant les bons et les mauvais événements et parfois même des événements à la fois positifs et négatifs.

Parmi les exemples de dommages irréversibles provoqués par un programme malveillant, s'il n'est pas bloqué à temps, on trouve :

- Infections parasitaires : si un agent infectieux parasitaire peut s'exécuter et infecter des fichiers critiques, le coût de la récupération et de la restauration du système augmente considérablement. Le fichier peut subir des dommages permanents, ce qui nécessite de recréer ou restaurer le système à partir d'une sauvegarde.
- Destruction des données : ces deux attaques majeures n'auraient pas pu être évitées par les défenseurs en se basant uniquement sur une approche « détecter et réagir » post-exécution. Les attaques contre Saudi Aramco et Sony Pictures ont toutes les deux utilisé un pilote noyau signé pour détruire les machines cibles.[7] Un autre exemple simple est l'exécution d'un ransomware, tel que CryptoWall ou CryptoLocker, qui chiffre tous les fichiers du système, puis exige de l'argent en échange de la récupération des données. Les solutions post-exécution détectent ces attaques trop tard, car les machines ne peuvent pas être restaurées.

- Détection des solutions de sécurité et évasion hostile : les recherches effectuées sur le logiciel malveillant Rombertik illustrent parfaitement les ravages provoqués par l'exécution de ce programme malveillant. Rombertik essaie de contourner les vérifications de sécurité, puis tente de détruire les environnements et machines qui cherchent à l'analyser.[2]
- Exfiltration de données : au fil des années, nous avons vu de nombreux types de logiciels malveillants ciblant les points de vente, tels que Framework POS, qui utilisait un mécanisme DNS pour exfiltrer les données des cartes bancaires[9] et le fameux programme malveillant BlackPOS, qui a atteint sa cible en 2013. La détection post-exécution n'aurait pas réduit le risque d'attaque pour ces types de logiciels malveillants. Une fois que les données ont quitté le système, les dommages sont quasiment impossibles à réparer. Une fois que le code malveillant s'exécute, il dispose de nombreuses méthodes pour exfiltrer les données, et la solution de sécurité doit à nouveau implémenter de nombreuses défenses au fil du temps.
- Attaques sur les solutions de sécurité : si les logiciels malveillants sont exécutés, certains programmes en profitent pour attaquer directement les solutions de sécurité et les agents de points de terminaison. Ainsi, l'an dernier, le logiciel malveillant Vawtrak a tenté de désactiver le logiciel de sécurité à l'aide de politiques de restriction de logiciels.[10]

Retour vers le futur

Qu'est ce que les fournisseurs et spécialistes de la sécurité ont appris après presque une décennie d'augmentation des coûts de sécurité et de développement des nouvelles solutions ? Si nous avions pu changer une seule chose, qu'aurions-nous fait ?

Il est évident qu'il n'est pas viable de se fier à des solutions qui cherchent à détecter les programmes malveillants uniquement APRÈS leur exécution. Lorsque le secteur de la sécurité a commencé à s'éloigner du confinement pré-exécution, les technologies sont devenues réactives et trop dépendantes des créations de signatures et des analyses manuelles de fichiers. Les fournisseurs de solutions de sécurité espéraient que l'analyse et les solutions post-exécution leur donneraient le répit nécessaire vis-à-vis du problème des programmes malveillants. Ils se sont finalement rendu compte qu'elles ne faisaient que rendre le système plus complexe, plus cher et plus sujet aux attaques et contournements.

Dell a résolu ces problèmes en proposant le premier et unique environnement de détection pré-exécution basé sur l'apprentissage automatique. Le principal défi de l'environnement pré-exécution est d'analyser le programme et de déterminer si un fichier est bon ou mauvais en se basant uniquement sur les informations contenues dans le fichier lui-même, et de le faire à grande échelle et dans la durée. La capacité à réaliser cette action sur une très grande quantité de fichiers est essentielle, car la création de logiciels malveillants modernes est automatisée. Aujourd'hui, la mutation d'un logiciel malveillant est banale pour un cybercriminel. Les signatures génériques manuelles (sur une base heuristique ou d'émulation) étaient suffisantes en matière de protection, lorsque la création de programmes malveillants était manuelle, mais ce n'est plus le cas.

Pour revenir aux fondamentaux et arrêter un programme malveillant avant qu'il n'ait la possibilité de s'exécuter, Dell utilise l'apprentissage automatique pour générer des modèles qui peuvent prédire si un programme est malveillant. Cette approche de la détection des fichiers s'avère extrêmement efficace et permet aux solutions Dell d'éviter 99 % des logiciels malveillants, bien au-dessus de la moyenne de 50 % des menaces identifiées par les principales solutions antivirus.[11] Dell a prouvé qu'il est en effet possible d'identifier un logiciel malveillant avec une exactitude surprenante, sans l'avoir vu auparavant. Revenons à l'exemple de Dyre : notre moteur a réussi à détecter un fichier à l'aide d'un modèle d'apprentissage automatique qui est sorti en août 2014, soit 10 mois avant l'arrivée de la variante. Notre moteur a détecté Dyre en phase de pré-exécution, bien avant qu'il ne soit identifié post-exécution par les solutions antivirus traditionnelles.

La détection de programmes malveillants pré-exécution n'est pas la solution miracle. En effet, les logiciels malveillants peuvent réussir à la contourner. Aucune solution n'est infaillible. Les spécialistes de la sécurité le savent bien : quand on parle de sécurité, il s'agit de réduire les risques, et non pas d'implémenter des absolus.

Une stratégie pré-exécution est la première étape de la constitution d'une gamme efficace de sécurité. La prévention des menaces avancée et révolutionnaire Dell arrête les logiciels malveillants avant leur exécution, sans mises à jour de signature, ni connexion permanente au Cloud. Cette approche permet de limiter les coûts de gestion de la sécurité ainsi que la surcharge au niveau des performances système. Elle peut également réduire les problèmes posés aux environnements d'analyse post-exécution, ce qui diminue considérablement le nombre de fichiers nécessitant une surveillance post-exécution, ainsi que le risque qu'un fichier malveillant passe au travers de cette dernière couche de défense. Se concentrer sur la prévention, plutôt que sur une approche « détecter et réagir », aide à réduire le nombre de couches de sécurité nécessaires pour repousser les pirates.

Conclusion

Le secteur de la sécurité a fait du chemin en termes de défense contre les attaques malveillantes. Cependant, dans sa hâte à créer des solutions rapides, faciles et prêtes à l'emploi, le secteur s'est retrouvé dans un cercle vicieux de signature : les fournisseurs développent de nouvelles solutions et les auteurs de programmes malveillants trouvent des techniques pour les vaincre. Puis, le secteur de la sécurité conçoit une autre solution, ce qui entraîne encore plus de contournements et d'attaques.

De nombreuses solutions de sécurité tentent maintenant de résoudre le problème de la détection de logiciels malveillants avec des approches post-exécution, « détecter et réagir », mais les programmes malveillants ont trouvé de multiples façons d'attaquer et de contourner ces solutions. Non seulement elles sont inefficaces, mais ces solutions « détecter et réagir » génèrent tellement de données, qu'elles créent un besoin croissant artificiel en analyse de sécurité du Big Data que le secteur ne sera peut-être jamais en mesure de gérer.

Les nouvelles couches de sécurité doivent savoir ce qu'elles doivent surveiller et quand le faire. Si une solution consigne aveuglément toutes les informations, elle se prépare simplement à une reprise après sinistre, mais elle ne tente pas vraiment de l'arrêter. C'est une position particulièrement risquée, car si les défenseurs abandonnent tout espoir de prévention des attaques, ils arriveront toujours trop tard et finiront par se concentrer uniquement sur la limitation des pertes de l'entreprise. C'est une solution tout simplement inacceptable.

Pour plus d'informations sur les solutions de points de terminaison Dell qui vous aident à protéger vos données et à éviter les menaces, consultez le site Dell.com/DataSecurity.

[1] Rapport Verizon « 2015 Data Breach Investigations Report » - http://www.verizonenterprise.com/DBIR/2015/
[2] http://blogs.cisco.com/security/talos/rombertik
[3] http://joe4security.blogspot.com/2012/10/defeating-sleeping-malware.html
[4] http://www.networkworld.com/article/2163341/byod/-sleeper--malware-like-nap-trojan-nothing-new.html
[5] http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.361.9423
[6] https://www.lastline.com/papers/acm_ccs11_hasten.pdf
[7] http://arstechnica.com/security/2014/12/sony-pictures-malware-tied-to-seoul-shamoon-cyber-attacks/
[8] http://blogs.cisco.com/security/talos/rombertik
[9] https://blog.gdatasoftware.com/blog/article/new-frameworkpos-variant-exfiltrates-data-via-dns-requests
[10] http://blog.trendmicro.com/trendlabs-security-intelligence/windows-security-feature-abused-blocks-
[11] Selon les résultats des démonstrations réalisées par Cylance à Austin, Dallas et Houston dans l'État du Texas au cours du « Unbelievable Demo Tour », mai 2015