Les Malwares et attaques

I. Introduction

Un malware est un logiciel créé dans le but de compromettre un système informatique sans l'accord du propriétaire de ce système.

Les premiers malwares sont nés dans les années 1970. Le premier malware, nommé *Creeper*, pouvait se connecter à un système distant en utilisant un modem et afficher le message d'erreur suivant : « I'M THE CREEPER: CATCH ME IF YOU CAN ». Depuis, les malwares ont évolué, ils sont capables à présent de modifier la vitesse de rotation d'une centrifugeuse comme l'a fait en 2010 le malware *Stuxnet* dans une centrale nucléaire iranienne, de voler des informations sensibles comme *Flamer* en 2012, d'utiliser des liaisons satellites pour communiquer avec l'attaquant, comme ce fut le cas pour *Turla* en 2015, ou encore plus récemment en 2017, de détruire des systèmes informatiques d'usines et de nombreuses sociétés cotées en Bourse, ce qui a conduit à fermer des entités durant des mois.

Il existe des millions de malwares différents. Ces malwares ont des fonctionnalités différentes, ils peuvent être classés par familles. Il est important de pouvoir classer un malware en fonction de son impact et de son but.

II. Les différents types de malware

a. Backdoor

Les *backdoors* sont des malwares permettant à un attaquant de prendre la main sur le système infecté. Au début, ces malwares ouvraient un port en écoute sur la machine infectée. Grâce à ce port ouvert, l'attaquant pouvait se connecter à la machine afin de l'administrer à distance. Cette technique impose une connexion à chaque machine et l'administration d'un parc de machines infectées est alors des plus laborieuses. On comprend que cette approche limite le nombre de machines humainement gérables par un seul attaquant. Pour pallier cette limitation, ces *backdoors* ont évolué en *botnet*. Un *botnet* est un ensemble de machines infectées reliées entre elles par un serveur central qui diffuse les ordres au travers du botnet. Ce serveur central est communément appelé C&C ou C2 (*Command and Control*). Ces serveurs peuvent être des serveurs web. De cette manière, l'attaquant peut administrer des milliers de machines depuis un point central.

Des frameworks ont été créés pour faciliter l'administration de ces machines infectées. Ces frameworks, appelés RAT (*Remote Administration Tool*), permettent de prendre la main sur les machines infectées, mais également d'automatiser la capture d'écran, le transfert de fichiers entre l'attaquant et la machine infectée, de gérer la base de registre Windows, etc.

Les fonctionnalités de ces RAT sont seulement limitées par l'imagination des développeurs. Ces frameworks sont parfois appelés des chevaux de Troie, en référence à la mythologie grecque.

Pour ce type de malware, le premier travail de l'analyste de malwares consiste à trouver le C&C afin de bloquer tout accès à ce serveur. Certes, ce blocage ne nettoie pas les machines infectées par le malware, mais l'attaquant sera neutralisé. En effet, il ne pourra plus donner d'ordre au botnet. Cette approche permet de gagner du temps pour continuer les analyses. La deuxième étape consiste alors à comprendre comment éradiquer le malware, c'est-à-dire désinfecter la machine. Dans un troisième temps, on s'attachera à cerner les fonctionnalités du malware pour en cerner l'impact, ainsi que son protocole de communication avec le C&C, par exemple pour définir une détection générique de son trafic réseau.

b. Ransomware et locker

Les *ransomwares* sont des malwares créés pour que l'utilisateur infecté ne puisse plus utiliser son système d'information ou consulter ses documents sans payer une rançon à l'attaquant.

Quand ce sont les données qui ne peuvent plus être consultées, le ransomware chiffre les fichiers et l'attaquant ne donnera la clé de déchiffrement qu'après avoir reçu la rançon. Ce type de malware est appelé un *locker*.

Dans le cas où le système d'information est visé, la machine est limitée dans son utilisation. Par exemple, il est impossible de se connecter sur Internet. Dans ce cas, l'attaquant fournit un logiciel de déblocage après avoir reçu la rançon.

Pour ce type de malware, l'analyste devra comprendre l'algorithme de chiffrement ou les mécanismes de blocage de la machine mis en place par l'attaquant. En effet, des erreurs d'implémentation ou des algorithmes faibles permettent souvent de restaurer les fichiers de la victime sans payer aucune rançon.

Il existe de nombreux ransomwares, parmi ceux-ci *Matsnu* (ou *Rannoh*) est particulièrement intéressant. Une des caractéristiques de ce malware est sa grande vitesse de propagation ainsi que le nombre important de machines bloquées. Ce ransomware était interfacé avec plusieurs serveurs d'administration. De plus, pour rendre l'analyse encore plus complexe, le malware générait des clés de chiffrement uniques pour chaque fichier chiffré. Le chiffrement utilisé était le RC4, qui est considéré comme un algorithme de chiffrement fort.

Au cours des dernières années, il y a eu une évolution de l'utilisation des ransomwares. Au début, les attaquants ciblaient des particuliers et demandaient des rançons de quelques centaines d'euros. Les attaquants jouaient sur le volume de victimes pour se rémunérer.

Aujourd'hui, les acteurs derrière les ransomwares ciblent des sociétés de toute taille et peuvent demander des rançons allant jusqu'à plusieurs millions d'euros.

c. Stealer

Les *stealers* (voleurs) sont des malwares créés dans le but de voler des informations ou des données sur la machine infectée. Comme dans le cas des backdoors, ces malwares se connectent à des serveurs centraux pour envoyer les données volées. Ces données peuvent être de tout type : des e-mails, des plans, des numéros de carte de crédit, des bitcoins (monnaie virtuelle), etc.

Tout comme pour les backdoors, le but de l'analyste de malwares est de trouver le C&C afin de bloquer toutes les communications avec celui-ci. La seconde étape est d'analyser quels types de données ont été exfiltrées par ce malware afin d'évaluer l'impact.

Il existe de nombreuses manières pour faire sortir les données d'un système : l'attaquant peut utiliser de nombreux canaux de communication tels que l'envoi d'e-mails ou encore le Web. Avec l'arrivée des messageries instantanées, les attaquants ont aussi commencé à exfiltrer les données sur celles-ci. Par exemple, il existe des stealers qui envoient les documents volés sur des salons Telegram.

Ce type de malware peut être illustré par le cas de *Duqu*, découvert en 2011 dans le laboratoire de cryptographie et de sécurité système de l'université polytechnique et économique de Budapest. Ce malware a été conçu pour capturer les frappes du clavier de la machine infectée et également pour récupérer des informations sur le système infecté. Les cibles de ce malware étaient peu nombreuses et concernaient essentiellement des systèmes de contrôle industriel. Les malwares permettant de capturer ce qui est saisi au clavier sont appelés des *keyloggers*.

d. Miner

Les *miners* (ou mineurs) sont des malwares qui utilisent les ressources des machines compromises afin de créer de la monnaie virtuelle, telle que le bitcoin par exemple. Ce type de malware fait généralement fonctionner le processeur des machines compromises à 100 %, ce qui le rend assez facilement détectable. Par exemple, le ventilateur de la machine se met à tourner très rapidement tout le temps.

e. Banking trojan

Les *banking trojans* sont des malwares ciblant les banques. Leur but est de modifier le comportement du navigateur des cibles afin de générer des virements bancaires sans que les

cibles s'en rendent compte. Généralement, ce type de malware s'injecte dans le navigateur et attend que l'utilisateur se connecte à son compte en banque. À ce moment-là, le malware ajoute du code sur la page web de la banque cible afin de réaliser des virements. Ce fut le cas de Trickbot par exemple, qui a ciblé des utilisateurs américains afin de voler de l'argent sur des comptes bancaires situés aux États-Unis.

f. Rootkit

Les *rootkits* sont des malwares servant à dissimuler l'activité de l'attaquant sur la machine infectée. Les premiers rootkits sont nés en 1994 sur Linux, en 1998 sous Windows et en 2004 sous Mac OS X.

Le premier but d'un rootkit est de se dissimuler. Pour cela, le rootkit va supprimer sa trace dans les journaux système. Il va également cacher son existence au niveau de la base de registre, mais aussi au niveau du système de fichiers via des mécanismes de *hook*.

Un *hook* consiste à remplacer un appel système du système d'exploitation par un autre appel. Le malware peut par exemple remplacer l'appel système permettant d'afficher les fichiers présents dans un répertoire par un appel modifié listant seulement les fichiers non liés au rootkit. Ainsi, les fichiers nécessaires au fonctionnement du malware restent cachés.

Un rootkit cachera par exemple son activité de processus ou son activité réseau. De cette manière, l'utilisateur de la machine infectée sera incapable de voir qu'un logiciel non voulu est en cours de fonctionnement sur sa machine. De plus, les rootkits peuvent également stopper les antivirus ou les *firewalls* pour ne pas être interrompus pendant que l'attaquant se connecte à la machine infectée. À la manière d'une backdoor, les rootkits laissent généralement une porte dérobée pour permettre à l'attaquant d'utiliser la machine infectée.

Les rootkits ont besoin de privilèges élevés pour pouvoir fonctionner. Il est donc fréquent que ces rootkits soient des drivers du noyau chargés automatiquement au démarrage de la machine. Ces dernières années, de nouveaux types de rootkits apparaissent, agissant au niveau du firmware ou du BIOS de la machine. Ces rootkits sont très compliqués à identifier, car le système d'exploitation n'est pas capable de les analyser. En 2010, un chercheur a publié une méthode permettant de remplacer le firmware d'une carte réseau. Ce nouveau firmware permettait une prise de main à distance de la machine infectée sans rien modifier au système d'exploitation.

Ce type de malware est le plus compliqué à analyser. Ses fonctionnalités sont multiples, sa taille est généralement grande et sa dissimulation rend l'analyse encore plus ardue.

III. Scénario d'infection

1. Introduction

Il est important de comprendre comment un malware peut être installé sur une machine. Il existe une multitude de scénarios d'injection, et les attaquants ne manquent pas de créativité pour infecter le plus de machines possible. Certains botnets, comme *Cutwall*, contiennent plus de deux millions de machines à la disposition des administrateurs.

2. Scénario 1 : exécution d'une pièce jointe

Ce scénario est le plus simple et le plus courant, il joue sur la crédulité des utilisateurs d'ordinateurs. Le principe est d'inciter l'utilisateur à infecter sa propre machine. Le malware au format exécutable peut être diffusé par e-mail ou encore par des liens sur les réseaux sociaux. Il est accompagné d'un message visant à tromper la victime par l'intermédiaire des techniques d'arnaque usuelles, jouant par exemple sur l'appât du gain. Ces malwares sont parfois même envoyés par des proches de confiance dont l'identité a été usurpée.

Ainsi, il est recommandé de ne pas ouvrir les pièces jointes exécutables envoyées par e-mail si celles-ci ne sont pas attendues, ou si l'e-mail est écrit d'une manière inhabituelle. Certains sites proposent également des vidéos ou des photos pour pousser les utilisateurs à télécharger des applications et à les installer.

3. Scénario 2 : clic malencontreux

Le deuxième scénario est plus complexe que le premier et l'infection n'est pas réalisée directement par l'utilisateur. Les attaquants utilisent des vulnérabilités dans le navigateur (ou ses extensions) pour déployer automatiquement leurs malwares. Cette méthode exploite le fait que beaucoup d'utilisateurs ne mettent pas à jour leur système d'exploitation ou leur navigateur ou encore les extensions utilisées par le navigateur.

En août 2015, une vulnérabilité majeure dans Flash a été rendue publique suite à la compromission de la société Hacking Team. Cette vulnérabilité permettait d'exécuter des commandes sur la machine d'un utilisateur. Pour cela, l'utilisateur de la machine devait simplement se rendre sur la page malveillante. Rien ne laissait voir qu'une infection était en cours pendant qu'il était simplement connecté à cette page web. Des développeurs de malwares ont très largement utilisé cette vulnérabilité pour infecter un grand nombre de machines.

Dans ce scénario, une action de l'utilisateur est tout de même nécessaire, mais cette action est limitée à un simple clic. Avec les services de raccourcissement d'URL utilisés par les réseaux sociaux, il est de plus en plus fréquent de cliquer sur des liens sans savoir vers quels sites ils pointent.

Depuis quelques années, l'écosystème des cybercriminels a vu une croissance fulgurante des *exploit-kits*. Ceux-ci sont des frameworks vendus sur le marché noir permettant d'exploiter plusieurs vulnérabilités sur une cible pour augmenter les chances de compromission. Par exemple, certains exploit-kits détectent les versions du navigateur des cibles, ainsi que les versions des extensions (Flash, Java, Silverlight, etc.), et déclenchent un *exploit* en fonction des résultats pour exécuter le malware sur la machine cible.

4. Scénario 3 : ouverture d'un document infecté

Ce scénario est un mélange des deux premiers. En effet, de plus en plus d'utilisateurs sont méfiants vis-à-vis des binaires inconnus. Les attaquants envoient donc des documents médias qui eux sont trop souvent considérés sans risque.

Les fichiers de type PDF ou encore les fichiers liés à la bureautique tels les DOCX, XLSX ou PPTX (de la suite Office de Microsoft) ne sont en effet pas des exécutables, ils ne modifient en rien la configuration de la machine qui ouvre ce type de document. Mais comme tout logiciel, les applications permettant de lire ces documents peuvent comporter des vulnérabilités. Ainsi, certains attaquants utilisent ces documents pour déployer du code malveillant sans que l'utilisateur se doute de quoi que ce soit. De plus, certains formats de fichiers permettent l'exécution de scripts intégrés, tels que les macros dans les documents de la suite Office.

5. Scénario 4 : attaques informatiques

Ce scénario concerne davantage les entreprises que les particuliers. Les attaquants peuvent chercher et trouver des vulnérabilités sur les systèmes ouverts sur Internet. Les serveurs web ou les serveurs e-mails sont des exemples de systèmes frontières faisant office d'interface entre Internet et le réseau interne.

Une fois qu'un attaquant découvre une vulnérabilité permettant d'exécuter des commandes, il est en mesure de déployer un malware. Sur de tels serveurs, la suite de l'attaque consiste à pouvoir progresser depuis cette frontière vers le réseau interne de l'entreprise pour atteindre les machines qui intéressent les attaquants tels que les contrôleurs de domaines, les serveurs e-mails ou les serveurs de fichiers.

En 2021, une vulnérabilité a été découverte sur l'application Exchange, permettant d'exécuter des commandes sur les serveurs e-mails de Microsoft. Cette vulnérabilité a été nommée *ProxyLogon*, elle a permis à de nombreux attaquants de compromettre de nombreuses sociétés et organisations utilisant ce produit pour gérer leurs e-mails.

6. Scénario 5 : attaques physiques - infection par clé USB

Pour être réalisé, ce scénario nécessite un accès physique à la machine à compromettre. Il existe des clés USB (par exemple l'*USB Rubber Ducky*) pouvant se faire passer pour un clavier. Il est possible de configurer cette clé pour que, une fois connectée sur une machine, elle saisisse ce que l'attaquant a préalablement configuré. La machine pourra alors télécharger un logiciel malveillant et l'exécuter.

Cette technique peut sembler complexe à mettre en place, cependant il existe de nombreuses bornes multimédias en libre-service dans les lieux publics et dont les ports USB sont parfaitement accessibles.

7. Scénario 6 : attaques de type supply chain

Depuis 2017, un nouveau vecteur d'infection a fait couler beaucoup d'encre : les attaques par *supply chain*. Dans ce type d'attaque, les machines sont compromises par un fournisseur de confiance. Par exemple, en 2017, le logiciel CCleaner (produit de sécurité utilisé par des millions d'utilisateurs) a été compromis et modifié afin de déployer des malwares.

Cette campagne malveillante a permis à l'attaquant de compromettre plus de 2,7 millions de systèmes. En 2019, la société ASUS a subi le même type d'attaque et le logiciel de mise à jour de cet éditeur a déployé des versions compromises et malveillantes de ses outils.

Ce type d'attaque est très complexe à identifier. En effet, les malwares sont signés par des sociétés de confiance et les utilisateurs ainsi que les applications de sécurité leur font confiance et les laissent s'exécuter.

IV. Mode opératoire en cas d'attaques ciblées persistantes (APT)

1. Introduction

Le mode opératoire lors d'une attaque ciblée persistante n'est pas le même que celui ciblant des personnes au hasard via des campagnes de spam massives. Sur une attaque ciblant une entité professionnelle spécifique, l'attaquant aura affaire à un environnement professionnel, avec une infrastructure complexe, une configuration d'entreprise, des systèmes de détection d'intrusion, etc.

Cependant, la complexité du réseau de l'entité cible peut, aussi surprenant que cela puisse paraître, faciliter le travail de l'attaquant. Il ne sera pas obligé de cibler la personne à atteindre spécifiquement, mais il pourra cibler un de ses collègues ou un employé d'une tout autre équipe, voire sur un autre site. Les interconnexions entre chaque poste des employés faciliteront le travail de rebond jusqu'à atteindre la cible souhaitée.

Comprendre le mode opératoire de l'attaquant peut aider un analyste à identifier un malware. Il est plus facile d'organiser son temps de travail dédié à l'identification de

machines infectées ou à l'identification d'un malware si le mode opératoire de l'attaquant est parfaitement maîtrisé.

2. Phase 1 : reconnaissance

Pour l'attaquant, la première étape est de connaître sa cible. Les informations peuvent être acquises via des moteurs de recherche, via les réseaux sociaux orientés vers les entreprises tels que LinkedIn ou même via les réseaux sociaux grand public. Elles peuvent également être récupérées physiquement sur le terrain, dans les locaux de la cible, en fouillant les poubelles, etc.

L'attaquant est à la recherche de tout type d'information sur les employés (hobbies, noms, adresses e-mail, etc.), le type de logiciels et matériels utilisés chez l'entité cible, ses fournisseurs, etc. Le but de cette collecte d'informations est de trouver le maillon faible de la chaîne et de tenter l'intrusion via ce maillon. Il n'est pas rare de voir des cas où un attaquant cible un fournisseur peu sécurisé afin de rebondir vers la véritable cible.

3. Phase 2 : intrusion

La deuxième phase consiste à mettre un premier « pied numérique » dans l'infrastructure cible. Il existe quantité de manières. En voici quelques exemples :

- *Spear phishing* : cette méthode consiste à envoyer à un destinataire qui aura été identifié lors de la phase de reconnaissance, un e-mail avec une pièce jointe (ou comprenant un lien vers un document ou un site web). Cette pièce jointe contiendra un malware (directement ou via un fichier multimédia malveillant). Une fois la pièce jointe ouverte, le malware s'exécutera sur la machine. Pour optimiser les chances d'ouverture, l'attaquant doit attiser la curiosité de la personne cible et l'inciter à cliquer.

L'attaquant pourra jouer sur les passions de la cible en lui proposant des réductions sur des produits, il pourra proposer des photos dénudées ou encore se faire passer pour un collègue envoyant un document de travail pour une relecture. Les attaquants font généralement preuve d'une grande imagination pour parvenir à leurs fins.

- *Water holing* : cette méthode consiste à compromettre un site légitime, fréquemment consulté par l'entité cible (par exemple, un fournisseur ou partenaire), afin de diffuser le malware sur les machines ayant consulté ce site. Les utilisateurs visitant ce site tous les jours et parfois depuis des années ne se douteront généralement de rien.
- *Social engineering* : le facteur humain peut s'avérer être le maillon le plus faible. Le social engineering consiste à exploiter cette faiblesse en poussant la personne à

installer elle-même le malware sur sa machine sans s'en rendre compte. L'attaque peut, par exemple, téléphoner à la cible en se faisant passer pour le support technique et demander à l'utilisateur d'effectuer un ensemble de manipulations afin d'installer le malware sur sa propre machine.

4. Phase 3 : persistance

Cette phase consiste, pour l'attaquant, à avoir accès à sa première machine infectée via la phase précédente. À présent, il peut administrer à distance cette machine et y déposer ses outils de post-exploitation.

5. Phase 4 : pivot

Cette phase consiste, pour l'attaquant, à se « promener » dans le réseau interne de l'entité cible. Les systèmes d'exploitation Microsoft permettent de réaliser très facilement cette tâche via le *pass-the-hash* ou le *pass-the-ticket*. Dans ces systèmes, une empreinte, appelée *hash* en anglais (ou un ticket en cas d'utilisation de Kerberos, protocole d'authentification), est stockée en mémoire de la machine une fois qu'un utilisateur s'est connecté. Cette empreinte peut rester en mémoire plusieurs jours, voire plusieurs mois. Elle permet à l'utilisateur de se connecter à un autre système Windows sans qu'il lui soit demandé nécessairement son mot de passe (à condition qu'il ait l'autorisation de se connecter sur la machine cible, bien évidemment).

L'attaquant peut tenter de récupérer cette empreinte dans la mémoire de la machine infectée et l'utiliser pour se connecter à d'autres machines. Généralement, dans les sociétés utilisant une gestion de comptes centralisée (de type Active Directory), un utilisateur peut se connecter sur n'importe quelle machine. Il aura automatiquement accès à son profil et à ses fichiers. L'attaquant va en quelque sorte utiliser cette fonctionnalité pour se déplacer de machine en machine.

Le but pour l'attaquant va être de compromettre davantage de machines et d'avoir des « roues de secours » dans le cas où l'infection serait détectée. En plus des autres machines bureautiques, l'attaquant cible en général les serveurs Active Directory où sont stockés tous les comptes de la société (afin de voler les comptes d'autres usagers), les serveurs e-mails, car ils contiennent énormément d'informations, et les serveurs de stockage de fichiers, car ils contiennent tout le savoir de l'entité cible.

6. Phase 5 : exfiltration

La dernière étape pour l'attaquant est de voler les données souhaitées. Grâce aux accès obtenus lors de la phase précédente, celui-ci sera capable de sélectionner les données

intéressantes et de les exfiltrer via une des machines bureautiques compromises ayant accès à Internet.

7. Traces laissées par l'attaquant

Certaines des phases décrites précédemment laissent des traces dans les journaux des systèmes Windows (si ceux-ci sont correctement configurés). De plus, l'utilisation de certains outils de post-exploitation laisse également des traces (certains créent des services afin d'obtenir les droits *SYSTEM* sur le système). La phase d'intrusion peut également laisser des traces dans les journaux des serveurs e-mails ou dans les journaux de connexion internet. Toutes ces informations peuvent aider l'analyste à identifier une machine compromise au sein de son parc informatique et à identifier le malware lui-même.

V. Ressources sur Internet concernant les malwares

1. Introduction

Il existe de nombreux sites internet aidant à l'analyse de malwares. Ils peuvent être classés en trois catégories :

- les sites faisant des analyses en ligne ;
- les sites expliquant certaines analyses techniques ;
- les bases de données de malwares.

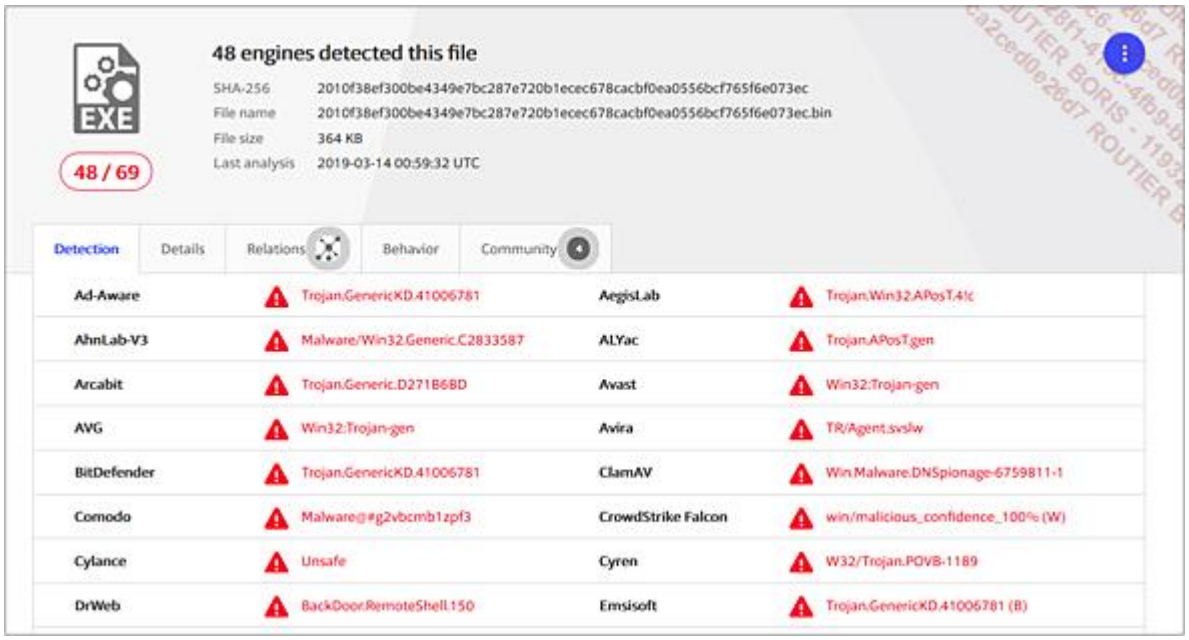
2. Sites permettant des analyses en ligne

Il existe de nombreux sites permettant ces types de travaux, en voici quelques-uns :

- https://www.virustotal.com

Ce site permet de tester des binaires sur 60 produits de sécurité du marché. Une fois l'analyse effectuée, un rapport est affiché avec le nombre d'antivirus ayant détecté un malware.

Voici un exemple de détection sur le malware DNSpionage :



Ce malware est détecté par 48 antivirus sur 69. Cet outil est très puissant, mais il est important de souligner que les fichiers envoyés à VirusTotal peuvent être partagés avec ses partenaires ou les éditeurs d'antivirus. Il est donc fortement déconseillé de soumettre des fichiers confidentiels ou privés.

- https://any.run

Pour soumettre une analyse, allez dans le menu **New Task** et choisissez le binaire à envoyer. Un rapport sera généré dans les minutes qui suivent sa soumission :

Tout comme pour VirusTotal, les fichiers soumis à ce site peuvent être partagés. Il est donc déconseillé d'utiliser ce site pour des documents confidentiels ou privés.

- https://www.joesandbox.com/

Ce site est une version en ligne de la *sandbox* Joe Sandbox. Il permet de contrôler les exécutables, mais également les fichiers PDF et les documents Office. Il est possible de réaliser des analyses privées qui ne seront pas partagées avec les autres utilisateurs (mais les analyses seront bien évidemment disponibles pour les administrateurs du site).

3. Sites présentant des analyses techniques

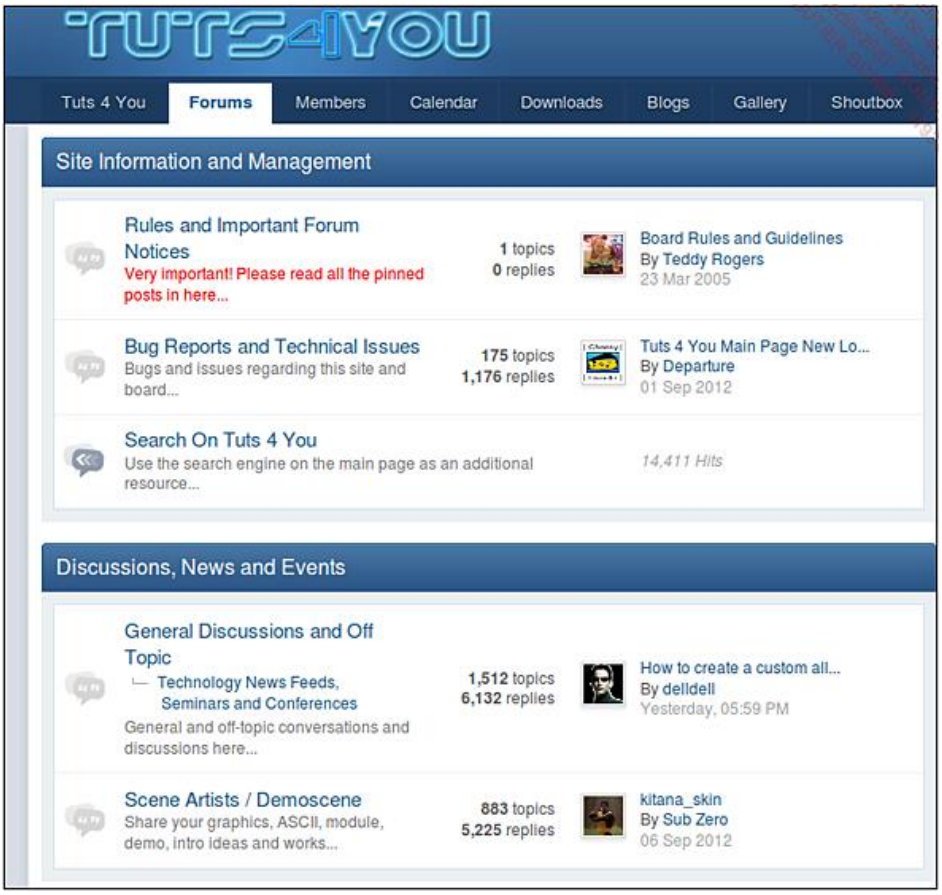
Il existe des sites expliquant des analyses de malwares ou des techniques d'analyse. Ces sites proposent généralement des analyses de *reverse engineering*

- http://fumalwareanalysis.blogspot.fr/

Ce blog est maintenu par Dr Fu et propose des dizaines d'articles sur l'analyse de malwares et le reverse engineering. Le niveau technique des articles est progressif et permet de correctement appréhender l'analyse de malwares.

- https://tuts4you.com/

Ce site regroupe une communauté de personnes passionnées par le reverse engineering. Il contient de nombreuses documentations sur les packers, les astuces pour se lancer dans le reverse engineering, etc. Il dispose également d'un forum très actif :



- https://malware.lu/articles/

Malware.lu est un site proposant une rubrique **Articles** où sont exposées des analyses de malwares.

4. Sites permettant de télécharger des échantillons de malwares

Afin de pouvoir analyser certains malwares, des sites proposent de télécharger des échantillons (fichiers). Pour éviter que des malwares ne circulent n'importe où, les mainteneurs de ce type de site choisissent de ne pas rendre librement téléchargeables les échantillons. Pour pouvoir les télécharger, il est nécessaire d'envoyer un e-mail au mainteneur du site afin qu'il crée un compte sur la plateforme.

- http://contagiodump.blogspot.fr/

Contagio est un blog contenant des échantillons de malwares visant essentiellement la plateforme Android de Google. Les archives contenant les échantillons sont protégées par un mot de passe. Il suffit d'envoyer un e-mail au mainteneur du site pour qu'il vous communique les mots de passe.

- https://www.malware.lu/

Malware.lu contient une base de données de plus de quatre millions d'échantillons. Pour accéder à cette base de données, il faut également demander la création d'un compte utilisateur par e-mail au mainteneur du site. Ce site limite le nombre de téléchargements à 15 par jour. Il propose également une API pour uploader des échantillons, vérifier leur existence dans la base de données ou les télécharger. Il est possible de rechercher un malware par son hash, son nom, mais également par le type de fichier ou le packer.

- https://virusshare.com/

VirusShare propose un peu plus d'un million d'échantillons en téléchargement. Il est également nécessaire de demander la création d'un compte au mainteneur du site internet.

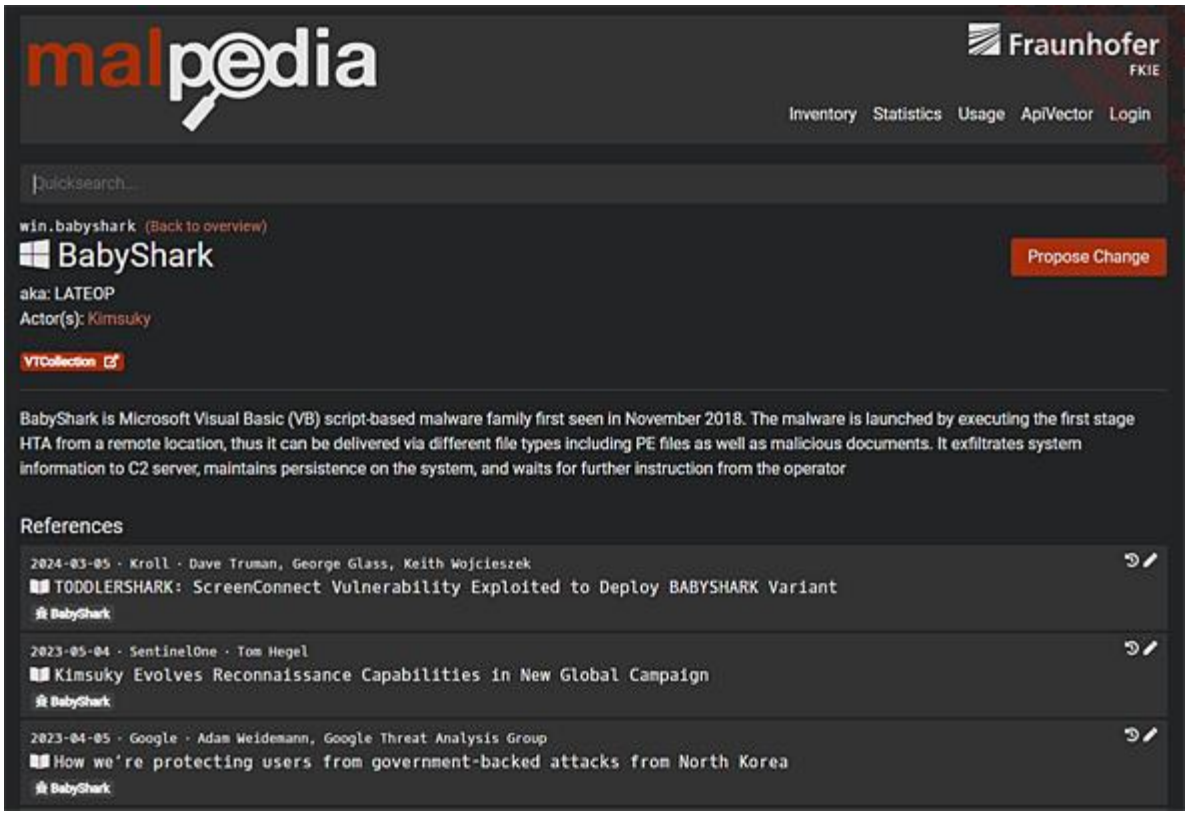
- https://vx-underground.org/

VX Underground propose plusieurs millions d'échantillons en téléchargement. Il n'est pas nécessaire de créer un compte pour les télécharger. L'avantage de cette plateforme est qu'il est possible de télécharger une copie complète de leur base de données pour pouvoir travailler en local sur un ensemble d'échantillons.

5. Encyclopédie Malpedia

Malpedia est une encyclopédie liée à l'analyse de malware maintenue par l'université de Fraunhofer FKIE. Elle est disponible à l'adresse

suivante : https://malpedia.caad.fkie.fraunhofer.de/. Il est possible, sans aucun compte, de rechercher tous les articles qui ont été publié concernant un attaquant ou une famille de malware. Par exemple, voici tous les articles liés au malware BabyShark :



Ce malware est utilisé par Kimsuky, un attaquant d'origine Nord-Coréenne. En créant un compte sur la plateforme, il est également possible de télécharger les échantillons.

Malpédia est l'encyclopédie la plus à jour concernant les domaines de l'analyse de malware et du renseignement sur la menace.