Module Veille Technologique & Outils

Yannis El HAJAOUI

Table des matières

Introduction

L'enjeu de la sécurité informatique prend une ampleur grandissante dans un monde hyperconnecté au caractère parfois extrêmement vulnérable. Les cyberattaques font la « une » des news tous les jours ou à n'importe quelle heure. Une telle concentration de menaces et d'attaques dans toute cette société hyperconnectée, tant sur la sphère privée que celle des entreprises ou des États. Devant de telles menaces, les antivirus classiques basés principalement sur la reconnaissance des signatures des virus, semblent avoir montré leurs limites. Ainsi, l'évolution exponentielle des attaques de ransomware, du phishing et des menaces zero day est l'indice d'une obsolescence progressive.

Il est de l'histoire des solutions antivirus que le périmètre d'alerte se limitait au répertoire des virus connus. Les pirates ont travaillé pour pallier ces faiblesses ici rencontrées et la solution fondée uniquement sur la signature ne suffit plus. Aujourd'hui, l'algorithme, l'ingénierie sociale, le bot, l'automatisation des attaques en temps réel dépassent les capacités d'alerte qui assuraient jusqu'à présent protection.

C'est dans cette optique que l'intelligence artificielle (IA) s'impose comme une solution à privilégier pour accroître la défense de la cybersécurité avec le machine learning et l'analyse comportementale qui sont au cœur des nouvelles générations d'antivirus permettant de déceler les menaces que l'on pouvait jusqu'à lors ignorer, avant même leur officialisation. Fin de détection basée sur une simple base de signatures, mais analyse de comportements suspects, détection d'anomalies et anticipation des attaques éventuelles avant leur survenance.

Cette veille a donc pour objet d'étudier l'évolution du marché de la cybersécurité, et d'analyser comme l'IA transforme la protection des systèmes informatiques, tout en prenant en considération les tendances observées, les limites des antivirus conventionnels, mais également des avancées en matière de cybersécurité pilotée par l'intelligence artificielle.

Présentation du thème

Historiquement, les antivirus traditionnels ont effectué une reconnaissance d'une signature de virus et verrouillé l'exécution uniquement de ceux pour lesquels il a trouvé cette signature. Or, d'autres méthodes, comme le changement en permanence de signature des différents malwares, sont récentes. Il n'en demeure pas moins que les attaques (cyberattaque, phishing avancé, ransomware) se développent dans un environnement en mutation permanente, les cybercriminels modifient leur manière d'attaquer, notamment avec des ransomwares évolutifs (offre de ransomwares pris en charge par un service client) ….

En tant que nouvelles menaces, le phishing avancé et les ransomwares évolutifs, faisant appel à l'AI afin de s'adapter au profil de la cible et répondre à ses besoins, un ransomware bondé, constitué de malware agissant ensemble, étant un excellent exemple et cible de choix d'un piratage à visée souvent personnelle et visant à tromper la cible, l'objet connecté que le phishing va attirer. La technologie IoT est par ailleurs visée ici par des cybercriminels exploitant sa fragilité ou celle des services d'interconnexion des objets.

Définition des menaces principales

Une attaque zero-day exploite une vulnérabilité encore inconnue des développeurs et éditeurs de logiciels. L'ampleur des conséquences adverses de ces attaques est d'autant plus préoccupante qu'aucun correctif n'est en l'état disponible.

Dans le cas des techniques de phishing, il s'agit plus explicitement d'une fraude par l'ingénierie sociale lors de laquelle un individu est trompé afin de lui soutirer des informations sensibles dont le fraudeur se servira malencontreusement à son détriment. Dans ce cas, le fraudeur se présente comme un acteur de confiance.

Le ransomware est un logiciel malveillant qui chiffre des fichiers d'un usager ou d'une structure pour ensuite demander une rançon au quidam afin qu'il puisse retrouver les fichiers à l'aide de la clé de chiffrement de ces derniers.

Méthodologie de veille

Pourquoi cette veille ?

Aux prises avec l'évolution accélérée des cybermenaces, la nécessité de surveiller les nouvelles techniques d'attaques et les nouveaux moyens de protections, afin d'anticiper l'impact de l'intelligence artificielle sur la cybersécurité et de dresser le bilan des innovations émergentes, se révèle indispensable.

L'enjeu d'une telle veille est donc double :

D'une part, il s'agit de comprendre pourquoi les antivirus traditionnels peinent à être efficaces contre la nouvelle économie des ransomwares,
De l'autre, de se pencher sur les solutions issues de l'intelligence artificielle pour une meilleure protection des infrastructures numériques.

Comment a-t-elle été réalisée ?

Cette veille a été menée en plusieurs étapes méthodiques visant à s'assurer de la complémentarité et de la pertinence des informations collectées. Dans un premier temps, j'ai défini des axes de recherche, en centrant l'analyse sur les thèmes suivants :

- L'évolution des menaces informatiques.
- Les limites des antivirus classiques
- Les avancées en matière de cybersécurité pilotée par l'IA.

Dans cette première étape, un choix des sources a été ensuite effectué, privilégiant la fiabilité et le secteur, tel que des sites de cybersécurité, des blogs d'experts, des articles académiques ou encore des rapports d'entreprises, permettant ainsi de suivre en temps réel des sources d'information pertinentes. La mise en relation d'un outil d'agrégation de contenu a permis en effet de s'informer des dernières diverses informations en lien avec les acteurs du secteur.

Enfin, les données ont été analysées et classées, afin de dégager les tendances et les innovations majeures, permettant dès lors de disposer d'un état de la cybersécurité sur le temps long, ayant permis d'identifier les enjeux relatifs à l'usage de l'intelligence artificielle dans ce champ d'action.

Outils utilisés

Feedly : pourquoi et comment ?

Feedly revêt une importance cruciale pour mener à bien une veille, puisqu'il permet de rassembler plusieurs sources d'information au sein d'un même espace. Plutôt que d'aller consulter les sites un à un, l'agrégateur facilite le suivi des flux RSS et permet d'accéder en temps réel aux nouvelles publications.

J'ai paramétré Feedly de façon à suivre des sources en cybersécurité, selon les sites spécialisés, les blogs d'experts, les publications scientifiques. J'ai également utilisé des mots-clés directement correspondants à notre recherche, tels que « cybersécurité IA », « menace zero-day », « antivirus nouvelle génération ».

L'un des grands avantages de Feedly est de pouvoir ordonnancer les articles dans différentes catégories pour faciliter leur analyse et leur exploitation. L'outil a donc été précieux pour structurer notre veille et obtenir une vue globale sur les tendances du marché.

Sources et classement

Les sources utilisées ont été mises en forme faisant l'objet d'un tri selon leur degré de fiabilité et de pertinence, se concentrant sur des sites d'instituts spécialisés, des études et rapports universitaires ainsi que des rapports d'organismes et experts en cybersécurité, parmi les principales sources ont été rapportés ceux de l'ANSSI (Agence National de la Sécurité des Systèmes d'Information), du NIST (National Institute of Standars and Technology) et du CERT-FR (Centre Gouvernemental de Veille, d'Alerte et de Réponse aux Attaques Informatiques).

Ces sources ont été choisies en raison de leur qualification et leur notoriété dans le domaine de la sécurité informatique, l'ANSSI notamment (Agence Nationale de la Sécurité des Systèmes d'Information) qui donne des recommandations à respecter dans la protection des infrastructures critiques, le NIST qui produit un certain nombre de standards et de cadres de référence repris largement à l'international pour la gestion de la sécurité des systèmes d'information, et le CERT-FR exerçant ses expertises dans le gouvernement français en matière de détection et de gestion d'incidents de sécurité.

Les travaux de recherche ont par ailleurs intégré des articles référence provenant de conférences telles que Back Hat et DEF CON. Black Hat est en effet la conférence mondiale de la cybersécurité où des experts présents leur expertise pour exposer les nouvelles menaces et nouvelles techniques d'attaques.

DEF CON est pour sa part la conférence hacker où chercheurs et professionnels de la sécurité explorent les failles et les vulnérabilités critiques et proposent des contre-mesures.

Parallèlement, ont été également consultés les rapports provenant d'entreprises comme Kaspersky, Symantec et Palo Alto Networks qui permettent d'obtenir une vision plus précise et plus pratique des menaces en cours.

Kaspersky, entreprise de sécurité CIS, plutôt tournée vers la sécurité, se présente comme un fabricant de solutions antivirus et d'analyses des cybermenaces.

Symantec aujourd'hui racheté par Broadcom est connu comme pionnier dans le secteur en cybersécurité, par ses outils de protection des endpoints qui désignent toutes les cibles potentielles pour les actions de cyberattaques ainsi que ses solutions de gestion des risques.

Palo Alto Networks entreprise américaine, construit des solutions de cybersécurité innovantes pour les rendre plus efficaces grâce à l'IA et s'appuie sur une approche par la surveillance du trafic réseau pour contrebraquer les menaces émergentes et les effets de surprise.

L'ensemble de ces sources très variées et spécialisées permettent d'appréhender les enjeux contemporains en cybersécurité ainsi que les réponses à ordonnancer à l'endroit des nouvelles menaces.

Synthèse de la méthodologie

Dans le cadre des travaux présentés ici, a été adoptée une méthodologie de veille basée sur le principe d'une rigueur systématique et scientifique dans la collecte et le traitement de données jugées qualitatives, fiables et à jour, dans le champ de l'évolution de la cybersécurité et de l'obsolescence des antivirus classiques. Ces travaux visent à assurer le suivi des évolutions des menaces et des technologies de défense, tout en réfléchissant sur les incidences de l'intelligence artificielle dans les modalités d'évolutions empruntées. Celles-ci étant orientées vers un véritable renforcement de la protection des infrastructures numériques.

L'une des premières étapes de cette méthodologie a été de déterminer avec précision les axes de recherche. Avec un choix consistant en trois Thématiques Identifiées :

- L'émergence de nouvelles menaces Informatiques
- L'obsolescence des antivirus classiques
- L'essor des solutions artificielles basées sur l'intelligence artificielle

J'ai réussi à poser une solide fondation pour comprendre les enjeux de la sécurité numérique aujourd'hui. Ces enjeux ont été choisis en fonction du risque qu'ils couvrent et de leur rapidité d'évolution. L'ambition était de comprendre des menaces émergentes (qu'il s'agisse de ransomwares, d'attaques zero-day ou encore de phishing intelligents) tout en cherchant à cerner les limites des solutions en place tout en explorant les innovations dans le domaine de la défense, notamment basées sur l'intelligence artificielle.

La phase du choix de sources a joué un rôle déterminant dans l'acquisition d'informations durables comme fiables et pertinentes. Ainsi, l'un des temps forts de cette veille est de chercher des sources considérées (en matière de cybersécurité notamment) comme indiscutables. Il a été retenu des rapports de l'ANSSI (Agence nationale de la sécurité des systèmes d'information), du NIST (National Institute of Standards and Technology) et du CERT-FR (Centre de réponse aux incidents de sécurité des systèmes d'information) qui sont réputés pour leur connaissance du milieu, en tant que rédacteurs avec les capacités de fournir des recommandations stratégiques et des données sur le sujet abordé, voire de croiser des données sur des menaces comme l'actualité l'atteste sur certains thèmes.

L'ANSSI propose une vision singulière des questions de cybersécurité en France, ainsi que des outils d'accompagnement à la protection des entreprises face à des menaces informatiques de plus en plus raffinées.

Le NIST, au niveau international, joue un rôle de premier plan avec son Cybersecurity Framework pour accompagner les entreprises vers des pratiques de sécurité efficaces.

Le CERT-FR, dont l'élément principal est l'alerte et l'assistance à l'incident, publie des alertes et des analyses sur les vulnérabilités et les attaques en temps réel, véritable aide indispensable à une vigie précise et réactive.
Aux côtés de telles sources, s'y ajoutent les sources des articles académiques, des rapports des entreprises du secteur et des conférences de haut niveau, où certaines telles Black Hat, DEF CON, jouent un rôle historique prépondérant.
Black Hat, une conférence de renommée mondiale, rassemble les experts de la cybersécurité pour discuter des dernières découvertes en matière de vulnérabilités et de menaces.

DEF CON est un point de rencontre pour les chercheurs, hackers et acteurs de la sécurité informatique pour tester et partager leurs découvertes sur les failles de sécurité. Ces événements sont une excellente source d'informations car ils donnent accès aux recherches les plus récentes mais permettent aussi d'identifier des tendances de pointe sur la cybersécurité.

Les entreprises Kaspersky, Symantec et Palo Alto Networks se sont aussi révélées être des sources des éléments d'information constitutifs de cette veille. Ces entreprises, reconnues dans le domaine de la cybersécurité, sont souvent à la pointe du domaine et réalisent des publications de rapports de bonne qualité sur les menaces, les tendances et les innovations de la sécurité.

Kaspersky est une référence en matière d'analyses parfois fouillées sur les menaces informatiques et les ransomwares, ainsi qu'en termes de données sur les malwares.

Symantec, fort de sa compétence sur les solutions pour la sécurité des entreprises, a pu éclairer sur la mutation des systèmes de protection en réaction aux attaques.

Pour finir, Palo Alto Networks, le spécialiste de la sécurité du cloud et des menaces avancées, a donné des éléments de réponse pour que les entreprises se préparent à affronter de nouvelles cyberattaques.

Le processus de collecte de données s'est fonde sur un outil de veille, Feedly qui a permis de centraliser dans un seul et même lieu l'ensemble des données issues des sources plurielles. Avec Feedly, j'ai été en mesure de suivre de manière instantanée l'actualité en matière de cybersécurité, des publications émanant d'experts, des rapports d'entreprises tout en permettant une bonne organisation de mes informations. Ce choix favorise aussi, par le biais de cet outil, un répertoire d'articles, d'exposés, de rapports tirés de sources sérieuses et laisse entrevoir la possibilité d'une analyse ou interprétation idéalement ne pas trop confirmation du niveau antérieur. Feedly fut un choix déterminant dans cette démarche de la veille, c'est que l'outil permet de manager la matière sans lancement, en centrant une attention continue sur des publications à même de participer à la dynamisation d'une œuvre.

Après avoir procédé à la collecte des informations, j'ai fait un travail de classification et d'analyse systématique des données, qui m'a permis de déceler ici des tendances et évolutions majeures. On note ainsi des avancées considérables que représente la montée en puissance de l'intelligence artificielle dans la détection et la prévention des attaques. L'analyse des comportements des utilisateurs et des logiciels en temps réel à l'aide de l'IA devient finalement un remède de plus approprié pour faire face à des menaces qui évoluent avec une rapidité et un caractère imprévisible. Il est même possible de souligner, à travers cette analyse, les limites des antivirus traditionnels dont l'efficacité passée ne sert plus au bon traitement des menaces présentes.

De fait, la méthode de veille mise en place a conduit à une approche studieuse et conclue, offrant un panorama suggestif des récents bouleversements marquant la sphère de la cybersécurité. Grace à une sélection concrète des sources, d'un usage de Feedly, d'un filtrage des données de façon continue, la veille à conspiré des éléments d'informations pertinents sur les points chauds des entreprises, mais aussi la recherche de solutions novatrices telles que l'intelligence artificielle pour défendre et protéger les systèmes, les infrastructures des menaces brandies. La méthode de veille a été en mesure d'indiquer les récents changements du secteur, tout en offrant des clés de réflexions sur le devenir de la cybersécurité.

Conclusion

À l'issue de cette veille, la cybersécurité émerge et se transforme comme un domaine en constante mutation où la sophistication de la menace augmente. Les antivirus classiques historiques, qui constituent l'un des moyens de garantir la sécurité informatique depuis plusieurs décennies, n'apportent plus de manière suffisante les réponses aux cyberattaques d'aujourd'hui, qui fonctionnent en fonction d'exploitation de vulnérabilités encore inconnues, de phishing plus performant et de techniques d'adaptation en temps réel.

Les configurations fondées sur l'intelligibilité artificielle s'annoncent comme le futur de la cybersécurité. Avec une détection proactive et une analyse comportementale en temps réel, l'IA apporte un nouveau panel de solutions aux problématiques posées par les menaces émergentes. Les systèmes pilotés par l'IA sont, en outre, capables d'analyser des volumes de données bien plus conséquents à une vitesse dépassant bien plus celle des systèmes traditionnels, tout en s'adaptant en permanence aux nouvelles formes de cyberattaques, rendant ainsi la protection plus robuste, plus réactive.

Les sources mobilisées pour la réalisation de cette veille, qu'il s'agisse des rapports officiels de l'ANSSI, du NIST ou du CERT-FR, des publications académiques : de conférence comme Black Hat et DEF CON, ou entreprises comme Kaspersky, Symantec ou Palo Alto Networks, ont été d'un grand secours pour dresser un état des lieux de la cybersécurité d'aujourd'hui. La centralisation de ces informations via un outil comme Feedly m'a permis de suivre les évolutions du secteur en temps réel et d'acquérir les connaissances nécessaires au bon déroulement de notre veille.

En conclusion, il apparaît indiscutable que la cybersécurité est amenée à se réinventer face à la sophistication des attaques modernes. Au regard des solutions plus flexibles, plus dynamiques et plus efficaces offertes par l'intelligence artificielle en matière de protection des systèmes d'information contre les menaces en constante évolution, elle semble être la voix de l'avenir. Mais il reste encore beaucoup à faire, notamment en matière de gestion des risques associés aux nouvelles technologies, et une mise à jour continue du suivi et de l'analyse des tendances émergentes sera nécessaire pour continuer à être en première ligne de la protection des données critiques et des infrastructures critiques.