La Threat Intelligence

Mathieu Thuaire

La Threat
Intelligence

Par Mathieu Thuaire

La crise sanitaire mondiale que nous traversons actuellement rappelle que le coronavirus COVID-19 tout comme les virus informatiques n'est pas soumis à la notion de frontières. Par ailleurs, il nous rappelle la nécessité de travailler ensemble pour obtenir au plus vite le traitement et surtout signaler les clusters afin de préserver la population.
En matière de cybersécurité cela revient à disposer de la capacité de détecter le signaux des attaques, même faibles, de bâtir une stratégie sur des bases techniques et organisationnelles et de partager, en sûreté, les informations récoltées par les systèmes dans un mode collaboratif.

MATHIEU THUAIRE

RSSI
Secrétariat Général de la Défense et de la Sécurité Nationale

Fort de cette actualité « pandémique », dans le cadre de la cybersécurité et de ses moyens déployés par les entités qu'elles soient privées ou publiques, un des outils qui intègre la boite à outil du RSSI est constitué du SOC (Security Operating Center)[1]. La détection des empreintes ou des signaux faibles - constituant notamment les APT[2] (Advanced Persistant Threat) – est assurée par les mécanismes de corrélation des logs concentrés par le SOC, et restituée au travers du SIEM[3] (Security Information and Event Management) aux analystes. Bien évidemment, malgré l'automatisation possible, ainsi que le machine learning implémenté dans cet outil, tout signal qui se glisserait dans un comportement normal défini par les métiers de l'entité

(1) SOC : « Security Operation Center », le SOC est un département de sécurité qui est en charge de superviser et protéger les systèmes d'information des entreprises contre les cyber attaques.

(2) APT : « Advance Persistent Threat » menace avancée persistante, c'est-à-dire une attaque cyber précise, ciblée, souvent complexe et furtive. L'acronyme APT est aussi utilisé pour décrire les groupes responsables de ces attaques (exemple : APT 1, présumé chinois et supposé troisième département de l'état major de l'Armée Populaire de Libération, connu sous le code Unité 61398.

considérée risquerait de passer inaperçu. Cela souligne ainsi la nécessité et la difficulté de corréler l'ensemble des signaux de manière globale afin d'identifier une attaque potentielle. La notion d'indicateur, que nous retrouvons plus régulièrement sous le terme d'IOC : Indicator Of Compromise, est ici primordiale[4].

(3) SIEM : « Security Information and Event Management » les SIEM sont des outils de gestion de l'informationde sécurité qui aident les organisations et les entreprises à gérer tous leurs évènements de sécurité (les logs ou journaux systèmes) afin d'en extraire les alertes et, potentiellement, de remonter à la source de l'attaque.

(4) IOC : « Indicator of Compromise » on pourrait traduire par indicateur de compromission, les IOCs classiques sont les signatures de virus, les signatures de trafic reseau, les « hashes » (MD5) de malwares, les URL et les noms de domaine des serveurs de commande et de contrôle…

Nous pressentons ici la limite de l'exercice si chaque entité travaille de manière isolée. En effet, afin de couvrir le spectre le plus large possible, il est nécessaire de détenir les IOC les plus pertinents couvrant les risques des SI considérés de l'entité, ce qui nécessite donc de maîtriser son infrastructure et sa configuration, et surtout de les ***partager*** au plus vite pour limiter l'impact des attaques.

L'état de la menace

Ce qui se cache derrière les menaces aujourd'hui peut prendre plusieurs formes : les attaquants peuvent avoir des visées purement économiques, des groupes criminels parfois multinationaux vont extorquer votre argent, voler vos cartes de crédit et vider vos comptes en banque. Le but des attaquants peut aussi être de capturer de nombreuses informations sensibles tels des secrets de fabrication ou même des données personnelles et de voyage. D'autres attaques ont comme finalité de réduire les moyens de communication ou même de complètement détruire les moyens informatiques de grands groupes industriels ou d'États ennemis. Les tactiques, les techniques et les procédures utilisées diffèrent car une attaque persistante pour le vol des données se construit différemment d'une attaque purement destructrice. Ces éléments sont notamment identifiés dans la méthode EBIOS RM[5], éditée et préconisée par l'ANSSI, dans le cadre des analyses de risques servant de base à l'homologation des systèmes d'informations.

(5) EBIOS RM : « Risk manager » méthode française d'identification et de compéhension des risques numériques au sein d'une entreprise.

(6) Script kiddie ou lamer désigne des néophytes, ne disposant pas de compétences sérieuses en sécurité informatique, qui tentent de forcer des systèmes au moyens de scripts dont ils ne maîrisent qu'imparfaitement les ressorts.

Toutefois, la stratégie est commune pour certaines phases de ces différentes attaques (dans le scénario décrit ci-dessous les trois premières phases se retrouvent dans les attaques citées plus haut). Bien évidemment nous parlons ici d'attaques élaborées et non pas de simples scan de ports ou d'attaques de script kiddies[6].

- Une première phase dite de **reconnaissance**, où se mêle de l'ingénierie sociale pour apprendre à connaître ses victimes,

(7) Identifiants de connexion à un espace à accès restreint.

du phishing avec des pièces jointes ciblées et piégées, ou le vol de credentials[7].

- Une seconde phase dite d'**exécution**, où l'attaquant s'installe dans le système en utilisant des chevaux de Troie (appelés aussi Trojan) à accès distant.

- Une troisième phase de **persistance** qui caractérise le fait de rester caché au fond des systèmes informatiques de la victime. Cette phase est réalisée quand l'attaquant a pris le contrôle de comptes dit à privilège, comme des comptes « administrateurs ».

- Une quatrième phase dite de **collection** où les informations sensibles de la victime sont capturées : données sensibles, identifiants et mots de passe, courriels.

- Une étape finale d'**extraction**, où les données sont compressées, chiffrées et envoyées sur le réseau à un ou des serveurs externes.

Sans préjuger d'un ordre de criticité de ces différentes phases, intéressons-nous à la troisième phase qui est l'objet de beaucoup d'attention de la part d'attaquants que nous qualifierons d'experts. En effet, la capacité à se dissimuler dans un réseau et à exploiter le plus longtemps possible une attaque relève souvent de capacités techniques élevées. Par ailleurs, cette phase est souvent la plus difficile à identifier, d'où la nécessité d'indicateurs pertinents et un besoin de corrélation prégnant.

Afin de définir une stratégie de sécurité pertinente, il est nécessaire de se baser sur une approche multi-factorielle : technique, organisationnel ou encore métier.

Sans décrire ici l'ensemble des briques nécessaires à l'exploitation d'une bonne politique de sécurité des systèmes d'information (PSSI), quelques bases sont à respecter :

Les bases techniques (liste non exhaustive) :

- La maîtrise de la configuration de ses systèmes (version logicielle, équipements installés, politique de gestion du changement, politique de maintien en condition opérationnelle et de sécurité, …) ;

- La politique de journalisation des logs de tous les équipements du proxy au serveur métier (les équipements dits de sécurité ne sont pas les seuls à pouvoir fournir des logs pertinents, d'autant plus dans le cadre d'une surveillance comportementale) ;

- La maîtrise de ses annuaires (AD[8], LDAP[9], … toutes ces briques doivent être maîtrisées et respecter un cloisonnement fort) ;

- Une architecture suffisamment cloisonnée

pour garantir le service métier et assurer une protection contre les mouvements latéraux, tout en mélangeant des technologies issues de fournisseurs différents ;

- Une maîtrise forte des comptes à hauts privilèges (PAM - Privileged Account Management, bastion d'administration, coffre fort à mots de passe, réseau d'administration dédié…) ;

- La capacité à faire ressortir les bonnes informations parmi ces quantités de données (d'où le besoin de règles de corrélation pertinentes en prenant en compte les comportements dits « normaux » de son entité).

Les bases organisationnelles (liste non exhaustive) :

- Connaître, identifier et responsabiliser les acteurs des équipes réseaux, systèmes et sécurité, et garantir que ces derniers sont bien informés de leur rôle dans le cadre de la gestion de la sécurité et des incidents ;

- Disposer d'un RSSI (Responsable de la Sécurité des Systèmes d'Information), capable d'assurer en gestion de crise le management tranverse des équipes, mais aussi, en temps calme la sensibilisation et le respect des politiques de sécurité (ce poste peut couvrir bien plus de responsabilité en fonction des entreprises, par exemple : pilotage des audits, management des équipes SOC, …) ;

- Disposer d'une organisation claire des responsabilités d'un point de vue SSI, ayant une certaine indépendance par rapport à la DSI et à ses contraintes budgétaires.

Les bases métiers (liste non exhaustive) :

- Maîtriser les comportements métiers normaux et tenir informé les équipes techniques des changements potentiels dans les activités ;

- Assurer la sensibilisation à l'outil informatique des équipes, ainsi qu'à la bonne gestion de la sécurité des comportements utilisateurs (un grand nombre de guide existent, notamment ceux de l'ANSSI permettant d'obtenir un socle solide sur les bons comportements) ;

- Restreindre au juste nécessaire les accès des utilisateurs (mise en place d'une politique de gestion des accès et des identités basée sur chacun des rôles des membres de l'entreprise).

(8) AD et GAD : « Active Directory et Global Active Directory » ce sont des annuaires qui fournissent des fonctionalités d'authentification, de gestion des identités, de gestion des groupes et des services d'administration des services d'annuaire de l'entreprise.

(9) LDAP : « Lightweight Directory Access Protocol » Si LDAP était à l'origine un protocole standard pour accéder à des services d'annuaire (« AD »), c'est surtout maintenant une norme pour ces services.

Ces éléments permettent ainsi de réduire considérablement le périmètre d'attaque, et optimisent les travaux des équipes de sécurité. Toutefois, ils ne garantissent aucunement un risque zéro des attaques informatiques. Il est donc nécessaire d'anticiper les scénarios de crise, et surtout de maintenir une politique de veille de sécurité.

L'identification de la menace

Face à une cyber menace si bien organisée, comment doit-on réagir ? La communauté cyber a ainsi commencé à partager l'ensemble de ses indicateurs, permettant d'informer la communauté au plus tôt des chemins d'attaques rencontrés. À l'instar des tests de robustesse des algorithmes confiés à l'ensemble des acteurs du monde cyber, il est illusoire de pouvoir imaginer bénéficier uniquement de ses propres indicateurs de compromission (IOC « Indicator Of Compromise ») et de vivre en autarcie.

Ces initiatives sont donc vitales à la maturité de la sécurité des systèmes d'information à plusieurs titres :

- Informer la communauté pour anticiper et freiner la diffusion de la menace ;

- Circonscrire, voir rendre inopérant les codes ou attaques malveillantes.

Quelles sont ces communautés ou organisations en capacité de fournir ces indicateurs :

- Les entreprises ou les administrations qui se sont dotées des technologies nécessaires pour détecter les attaques dont elles sont ou pourraient être les victimes. Certaines d'entre elles, surtout celles dont les comités exécutifs ont pris la mesure du risque cyber, se sont équipées d'un CERT, une équipe de veille et surveillance de la menace et de réponse rapide à incident (« Computer Emergency Response Team ») et ont la possibilité de conserver et de trier leurs propres indicateurs ;

- Les CERT nationaux, comme le CERT-FR dont le rôle au sein de l'ANSSI (Agence nationale de la sécurité des Systèmes d'information) est notamment de corréler les informations sur les incidents, de traiter les alertes et d'échanger avec les autres CERT nationaux et privés. Certains gouvernements, comme celui du Royaume-Uni, favorisent ces échanges dans le cadre de partenariat privé-public comme le CISP (« Cyber-security Information Sharing Partnership ») initié par le NCSC (« National Cyber Security Center »).

- Des regroupements internationaux indépendants de CERT, comme l'organisation FIRST (siège basé à Cary en Caroline du Nord - USA), dont l'objectif est de mutualiser les informations de CERT issus de toutes les cultures et régions du monde. Les menaces étant globales, la réponse elle aussi doit l'être. FIRST regroupe plus de 500 CERT,

dont 16 en France. En sont membres pour la plupart des grandes institutions bancaires françaises comme la Banque de France, le Crédit Agricole, La Société Générale, BNP Paribas, la Poste mais aussi le CERT-FR, le SIRP[10] d'Interpol et quelques autres.

- Les acteurs privés spécialisés dans l'orchestration, de l'automatisation et des solutions de réponses aux incidents de cyber sécurité[11]. Toutes ne fournissent pas exactement les mêmes services mais leur utilisation est bien sûr payante ;

- Les organisations sectorielles qui regroupent des acteurs d'un même type d'industrie (comme Aviation-ISAC pour le secteur aérien ou RH-ISAC pour les secteurs grande distribution et chaines d'hôtels) afin d'échanger des informations sur les cybermenaces. Ces organisations favorisent aussi les échanges entre acteurs publics et privé, surtout aux US.

Ces organisations issues des US sont très fortement orientées pour défendre les actifs Américains.

Comment s'organiser face à la menace et anticiper pour être prêt, par exemple en cas de pandémie mondiale

En effet, reprenant ainsi l'analogie de la pandémie, il est nécessaire de veiller à alerter l'ensemble de la chaîne dès l'apparition des premiers « clusters » de diffusion afin de se prémunir de la pandémie. L'étape suivante est de fournir l'antidote ou le vaccin afin de rendre cette menace mineure et être ainsi capable de vivre avec.

Ces éléments sont devenus vitaux, notamment du fait d'un marché parallèle au sein duquel sont vendus ces malwares, trojans ou concepts d'attaques. Il n'est pas rare de voir ressurgir des versions mutantes des malwares quelques années après la diffusion de ces « zero day ».
Compte tenu de la rapidité de mutation de ces malwares, il est donc indispensable d'agir sur la rapidité de diffusion des symptômes permettant de déceler ces attaques informatiques.

Une fois les informations collectées, le problème est souvent dans la détermination de leur pertinence. L'idée d'organiser ces IOCs a émergé et certaines plateformes ont ainsi pris naissance notamment en open source tel que OPENCTI

(10) SIRP : « Security Resonse incident platform » est une plateforme dédiée à la gestion des incidents de sécurité qui avec le SIEM réalise la corrélation des « logs » (journaux systèmes) pour en extraire les alertes de sécurité. Le SIRP aide les CERT et les équipes de sécurité à gérer leurs incidents.

(11) https://www.ivision.fr/
NDLR : On définit par l'acronyme SOAR ces technologies logicielles qui permettent d'automatiser certaines tâches liées à la gestion de la sécurité informatique, et notamment, à la détection des incidents.
Le terme SOAR (Security Orchestration, Automation and Response, qui signifie en français « Orchestration, automatisation et réponse aux incidents de sécurité informatique ») a été utilisé pour la première fois par le cabinet Gartner, en 2018.

ou MISP[12]. Par exemple, le projet OpenCTI (Open Cyber Threat Intelligence) est développé par l'ANSSI en partenariat avec le CERT-EU. C'est un outil de gestion et de partage de la connaissance en matière d'analyse de la cybermenace (Threat Intelligence). Initialement conçue pour structurer les informations de l'agence relatives à la menace informatique, la plateforme facilite aussi les interactions entre l'ANSSI et ses partenaires. L'outil, intégralement libre, est aujourd'hui disponible pour l'usage de l'ensemble des acteurs de la « threat intelligence ».
Un éco système complémentaire de logiciel libre est disponible, permettant ensuite de centraliser la gestion et le suivi de la reponse (The Hive), et Cortex x permettent d'utiliser des données MISP (Malware Information Sharing Platform) ainsi que des données provenant d'autres sources pour enrichir le contexte.

(12) MISP : « Malware Information Sharing Platform » une plateforme "open-source" pour rassembler, stocker, partager et corréler les informations sur les attaques cyber, les informations sur les vulnérabilités, et même de l'information liée au contre-terrorisme.

Le besoin de protéger les acteurs qui échangent des informations sur les menaces

Cependant, malgré cette volonté et nécessité de partage de l'information, des réticences sont encore nombreuses. En effet, la collaboration atteint ses limites quant à la diffusion d'une information permettant de déduire qu'une grande entreprise ou administration a été victime d'une cyber attaque. Qui n'a jamais pensé qu'une entité victime de cyber attaque n'était donc pas de confiance ? Quel impact pour sa santé financière, non pas à cause de l'attaque elle-même mais à cause de la notoriété impactée par cette attaque ? Autant de questions qui soulignent les réserves potentielles à partager ces informations.

Il est donc nécessaire de se pencher sérieusement sur la protection des entités qui consentent à partager leurs indicateurs de compromission. Beaucoup hésitent encore même si tout le monde s'accorde à dire qu'ensemble face à une menace toujours plus variée et toujours plus sophistiquée, nous serons plus forts. En Europe et en France en particulier, il n'existe pas de garantie légale que ce partage de l'information ne se retournera pas contre ceux qui ont eu l'honnêteté et le courage de partager leurs IOCs et ce dans le but même d'aider et renforcer nos défenses face à des ennemis de mieux en mieux organisés et financés alors qu'elle existe bien aux États-Unis. L'administration Obama a, en effet, fait adopter par le Congrès Américain une loi : le CISA (« Cyber Security Information Sharing Act ») dont le but est de fournir une protection juridique aux acteurs qui échangent des informations sur les menaces de cyber sécurité pour peu que ces échanges

soient conformes aux règles stipulées dans la loi. La question est donc posée : comment favoriser l'adhésion du plus grand nombre et protéger les sources d'informations ?

Conclusion

Fort de ces éléments, plusieurs constats sont donc à synthétiser :

A l'instar des US, n'est-il pas souhaitable de fédérer la communauté européenne pour le partage des indicateurs. Pourquoi ne pas imaginer une réponse commune aux attaques cyber ; cela n'aurait-il pas limité les impacts de Wannacry ?

En complément de ces partages d'informations, et toujours dans l'optique d'une amélioration de la circulation de l'information, n'est-il pas nécessaire de protéger les contributeurs afin de défendre des intérêts communs ?

Bien sûr, il est facile d'opposer à ces propositions la souveraineté nationale des différents États,

mais n'est-il pas envisageable de distinguer les actifs primordiaux d'un État et de ne pas exposer ces derniers lors du partage d'IOC. Par ailleurs, un grand nombre de systèmes d'informations sont basés sur des technologies communes. Le partage d'indicateurs ne met donc pas en exergue les architectures des États membres, sauf usage de technologies spécifiques.

Enfin, un volet légal ne permettrait-il pas un partage accru des bonnes pratiques et ne renforcerait-il pas une réaction commune de l'Europe face à des menaces étatiques fortes ?

Ainsi, soutenons ce vœu pieu d'une réponse européenne à la fois technique, organisationnelle et juridique.

Bibliographie

a. https://www.ssi.gouv.fr/administration/bonnes-pratiques/

b. https://www.misp-project.org/

c. https://thehive-project.org/

d. https://www.cert.ssi.gouv.fr/

e. https://www.first.org/

f. https://www.congress.gov/bill/114th-congress/senate-bill/754

g. https://www.fireeye.fr/current-threats/apt-groups.html

h. https://www.ssi.gouv.fr/guide/recommandations-de-seccurite-relatives-a-active-directory/

i. https://www.ssi.gouv.fr/entreprise/management-du-risque/la-methose-ebios-risk-manager

L'AUTEUR

Mathieu Thuaire exerce la fonction de RSSI au sein du SGDSN. Dans le cadre de ses activités, il a en charge la politique de sécurité et ses aspects réglementaires au sein de son entité, la réalisation de la politique d'audit et sa mise en application, et enfin la responsabilité du SOC et le management des programmes cyber.
Mathieu Thuaire a une expérience de plusieurs années dans la cyber sécurité, et plus particulièrement dans l'administration, avec notamment un passage en tant que manager programme à la DGA, puis au SGDSN.
Il est également auditeur IHEDN – INHESJ de la première session nationale Souveraineté Numérique et Cyber-sécurité.