swisscom

L’attaque ciblée

Cyber Security Report 2019

Swisscom (Suisse) SA
Group Security
Alte Tiefenaustrasse 6
3048 Worblaufen
www.swisscom.ch

Table des matières

Introduction

Le Cyber Security Report 2019 de Swisscom a été publié. A partir de l'état des menaces, que nous avons à nouveau actualisé cette année, nous examinons en détail un sujet qui intéresse particulièrement la Security Community au sein de Swisscom, chez nos partenaires et nos clients, mais aussi à l'échelle internationale: les APT.

Les menaces persistantes avancées (Advanced Persistent Threats, APT) se caractérisent par le fait que des assaillants disposant d'un grand nombre de ressources attaquent une cible clairement définie en vue d'obtenir des informations spécifiques ou de causer des dommages durables. Afin de mieux évaluer la pertinence de cette menace, nous la plaçons dans le contexte d'autres menaces, comme les criminels, les terroristes et les hacktivistes. Qu'est-ce qui rend les APT si spéciales?

Alors que les criminels empruntent la voie de la moindre résistance pour faire le plus de profit possible, à la différence des terroristes et hacktivistes qui utilisent les attaques à des fins publicitaires et disposent de relativement peu de ressources et de savoir-faire, les attaquants qui utilisent des APT adoptent une approche beaucoup plus subtile. La cible est soigneusement choisie et surveillée pendant des mois, voire des années. Des ressources pratiquement illimitées sont libérées pour développer le savoir-faire et les outils appropriés. Pendant et après l'attaque, la plus grande discrétion est de mise afin que ni l'assaillant ni la cible ne soient connus trop tôt.

Le rapport décrit la motivation et les moyens de l'assaillant. Sur la base des données collectées et évaluées par Swisscom, il montre quelles méthodes et quels outils les assaillants utilisent le plus fréquemment. Il montre également quelles contre-mesures sont particulièrement efficaces détecter au mieux une attaque.

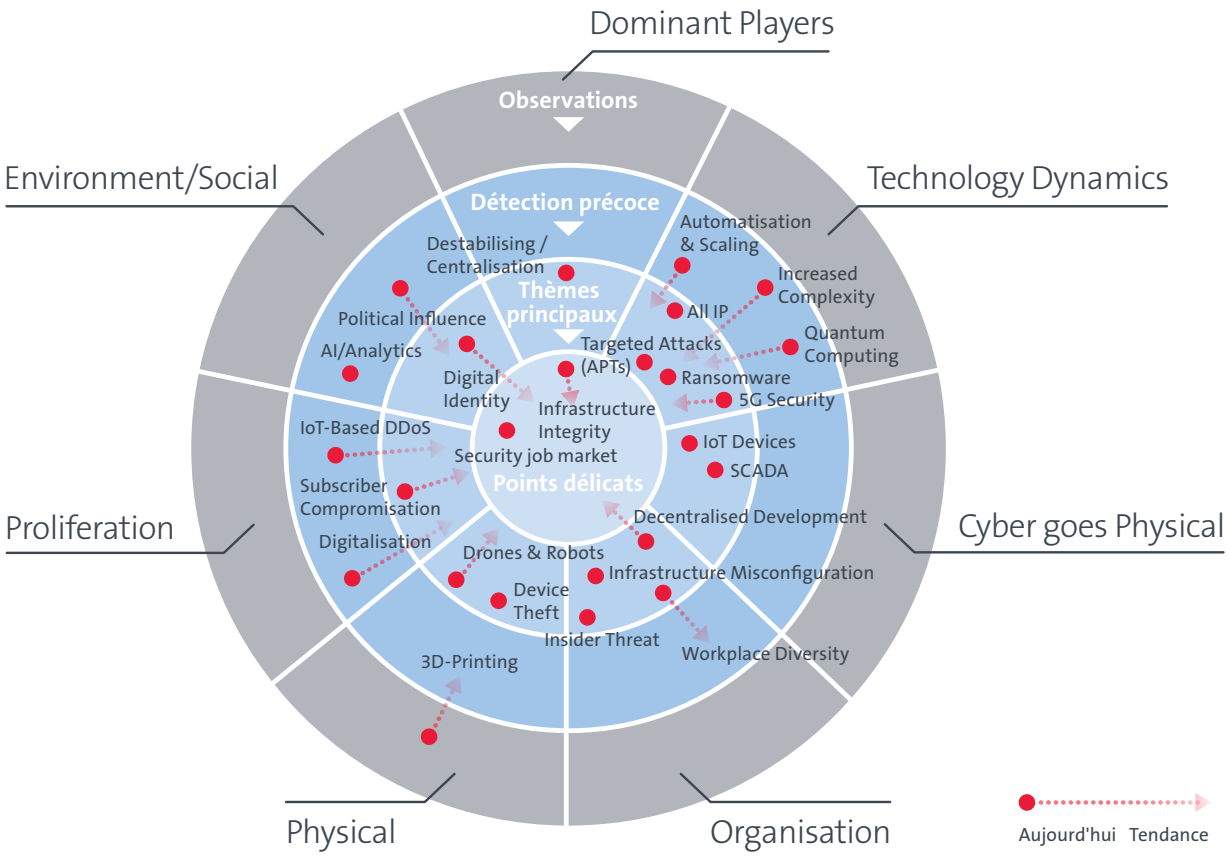
Nous sommes particulièrement heureux d'aborder ce thème. Costin Raiu de Kaspersky GReAT nous a fait le plaisir de répondre à une interview. Costin est un expert mondialement reconnu dans ce domaine, qui aime partager ses connaissances avec nous.

Ce rapport est le résultat d'un travail collectif réunissant plusieurs départements au sein de Swisscom.

Situation – radar des menaces

Les menaces trouvent leur origine dans le développement constant des nouvelles technologies, leur application et leur diffusion au sein de la société.

Les menaces potentielles doivent être détectées de façon précoce et systématiquement répertoriées. Pour représenter l'état des menaces et leur évolution, nous utilisons le radar familier auquel nous avons déjà fait référence dans des publications précédentes du Cyber Security Report de Swisscom.



Radar des menaces

Méthodologie

Le radar des menaces se compose de sept segments, délimitant les différents champs de menaces. Il est possible de rattacher les menaces associées à chaque segment dans l'un des quatre cercles concentriques. Les cercles présentent l'actualité de la menace et donc aussi le manque de précision lié à la menace. Plus une menace est proche du centre du cercle, plus elle est concrète et plus les contre-mesures sont importantes.

Nous considérons les cercles comme des:

- **Points délicats** pour les menaces qui sont déjà réelles et qui sont gérées avec une mobilisation relativement importante de ressources.

- **Thèmes principaux** pour les menaces qui sont déjà survenues individuellement et qui sont gérées avec une mobilisation normale de ressources. Il existe souvent des processus réglementés pour traiter efficacement de telles menaces.

- **Détection précoce** des menaces qui ne sont pas encore survenues ou qui ont actuellement très peu d'effet. Des projets ont été lancés afin de pouvoir rapidement faire face à l'avenir à l'importance croissante de ces menaces.

- **Observations** pour les menaces qui ne surviendront que dans quelques années. Il n'existe aucune mesure concrète pour gérer ces menaces.

Par ailleurs, les différentes menaces identifiées par ces points suivent une tendance. Celle-ci peut avoir une criticité en progression, en recul ou stable. La longueur du faisceau de tendance indique la rapidité escomptée de l'évolution de la criticité de la menace.

Menaces

Voici une brève description des sept segments du radar des menaces.

Dominant Players

Ce segment englobe les menaces résultant de dépendances aux éditeurs, services ou protocoles dominants.

Points délicats	*Infrastructure Integrity:* les principaux composants des infrastructures critiques peuvent comporter des failles intégrées par négligence ou sciemment, qui mettent en péril la sécurité du système.
Thèmes principaux	*Destabilising Centralisation:* la centralisation forte dans la structure d'Internet crée de gros risques. La défaillance d'un service peut avoir des conséquences à l'échelle mondiale, comme ce fut d'ailleurs le cas lors d'une défaillance d'Amazon Web Services (AWS).

Technology Dynamics

Menaces résultant de l'accélération de l'innovation technologique, offrant dès lors de nouvelles possibilités aux assaillants et créant aussi de nouvelles menaces du fait de l'évolution.

Thèmes principaux	*Targeted Attacks:* sont des attaques ciblées et complexes conçues pour atteindre un objectif spécifique. Cette menace est expliquée en détail dans les chapitres suivants du présent rapport. *All IP:* dans le contexte de l'introduction All IP à couverture globale, les risques augmentent en fonction de la technologie VoIP. *5G Security:* la 5G est une technologie de communication mobile encore jeune dont la mise en place est à l'origine de nombreuses opportunités ainsi que de risques encore inconnus. *Ransomware:* les données critiques sont cryptées en masse et sont ensuite décryptées (éventuellement) contre le versement d'une rançon.
Détection précoce	*Automatisation & Scaling:* l'automatisation renforcée des processus techniques d'exploitation aura des conséquences plus importantes en cas d'attaques efficaces ou de configurations erronées. *Increased Complexity:* la complexité des systèmes, en particulier au-delà des limites des technologies et des entreprises, ne cesse de croître. L'exposition aux risques augmente d'autant et la recherche d'erreurs devient plus difficile. *Quantum Computing:* les ordinateurs quantiques peuvent rendre les procédés cryptographiques actuels inutilisables, car ils peuvent les déjouer en très peu de temps.

Cyber goes Physical

Ce terme désigne les attaques utilisant les infrastructures dans le cyberespace, qui provoqueront de plus en plus de dommages dans le monde physique.

Thèmes principaux	*IoT Devices:* les appareils insuffisamment protégés peuvent être compromis et sabotés. Ils peuvent ainsi voir leurs propres fonctions, par exemple leur disponibilité ou l'intégrité des données, restreintes. *SCADA:* des systèmes de contrôle mal ou pas du tout protégés continuent d'être utilisés dans les installations de certaines infrastructures critiques.

Organisation

Menaces résultant des changements dans l'organisation ou exploitant les failles qui y sont présentes.

Thèmes principaux	*Infrastructure Misconfiguration:* exploitation de composants d'infrastructures mal configurés et/ou de failles identifiées et corrigées tardivement. *Workplace Diversity:* outre les nombreux avantages qu'apportent les nouveaux modèles de travail, leur mise en œuvre incontrôlée, p. ex. «Bring your own Device» (BYOD) ou l'utilisation accrue des postes de travail distants, entraîne une exposition accrue aux risques. *Insider Threat:* manipulation, exploitation abusive ou vente d'informations de partenaires ou de collaborateurs, par négligence ou de manière préméditée. *Decentralised Development:* les départements de développement classiques disparaissent, alors que le développement des applications se rapproche des Business Units avec des cycles de release de plus en plus courts.

Physical

Menaces émanant de l'environnement physique et visant généralement des objectifs physiques.

Thèmes principaux	*Device Theft:* le vol, notamment de certains composants des infrastructures critiques ou, à l'avenir, de plus en plus d'appareils IoT peut donner lieu à des pertes de données ou perturber la disponibilité des services. *Drones and Robots:* la reconnaissance ou les attaques à de grandes distances deviennent plus simples et moins coûteuses.
Observation	*3D-Printing:* la fabrication de clés, par exemple, ou d'autres appareils physiques est plus avantageuse et plus simple grâce à l'amélioration de la qualité des imprimantes 3D.

Proliferation

Les menaces résultant des progrès en matière de disponibilité et d'accessibilité des médias informatiques et de savoir-faire relèvent du segment de la prolifération. D'une part, parce que l'accessibilité multiplie les points d'attaque et d'autre part, parce que la disponibilité des outils d'attaque augmente.

Thèmes principaux	*Subscriber Compromisation:* les logiciels malveillants attaquent les données des utilisateurs ou sont utilisés pour attaquer les infrastructures de télécommunication ou d'informatique.
Détection précoce	*IoT-Based DDoS:* une croissance forte associée à une faible protection des appareils IoT augmente le nombre des «candidats à la prise de contrôle» pour les botnets. *Digitalisation:* l'interconnexion de plus en plus forte entre le virtuel et le réel et la vie privée et professionnelle multiplie les vecteurs d'attaque.

Environmental / Social

Il s'agit de menaces résultant des changements politiques et sociaux ou devenant plus aisées ou plus payantes grâce à ces changements.

Point délicat	*Security job market:* les besoins en professionnels de sécurité peuvent difficilement être couverts, ce qui se traduit par une pénurie d'expertise dans les interventions contre les attaques qui deviennent de plus en plus complexes et intelligentes.
Thèmes principaux	*Digital Identity:* les identités numériques individuelles certifiées peuvent être utilisées abusivement ou volées dans le but de conclure des contrats au nom de tiers, par exemple.
Détection précoce	*AI / Analytics:* grâce à l'AI, des données en plus grand nombre et de meilleurs modèles d'analyse peuvent être utilisés abusivement afin d'influencer le comportement des individus. Les décisions sont de plus en plus laissées à des systèmes autonomes. *Political Influence:* les tendances politiques peuvent influencer les décisions technologiques ou économiques, par exemple dans le choix des fournisseurs de technologie. Il peut en résulter de nouveaux risques.

Conclusion

L'état des menaces demeure complexe. Les pirates profitent de la valeur croissante des actifs virtuels, ce qui augmente leur motivation à mener des attaques ciblées. Par ailleurs, les innovations technologiques et le rapprochement entre les mondes physique et virtuel ouvrent de nouvelles possibilités d'attaques. Toutefois, il devient également évident qu'une menace n'est pas fixe, mais qu'elle est sujette à des fluctuations et à des tendances.

Par rapport à la situation de l'année dernière, nous pouvons constater que l'état des menaces dans leur ensemble est stable. Bien que les menaces individuelles diminuent cette année, comme c'est le cas pour *l'Infrastructure Misconfiguration* et la *Workplace Diversity,* la plupart subsistent et ne changent que très peu.

Pour les deux menaces à la baisse, nous pensons que le «soulagement» réside non pas dans l'intérêt réduit des assaillants potentiels, mais dans la maturité accrue des infrastructures affectées. La Workplace Diversity, par exemple, est gérée activement par de plus en plus d'entreprises, des outils Mobile Device Management (MDM) sont utilisés et des directives pour l'utilisation de Bring Your Own Devices (BYOD) sont élaborées et appliquées.

Les menaces via les systèmes *SCADA* (systèmes de contrôle industriels) et les *appareils IoT* (Internet des objets) restent au centre des préoccupations, mais nous ne voyons aucun changement à court terme. La pénétration de l'Internet des objets n'est pas encore assez forte pour aggraver davantage la situation.

Les drones, par contre, se répandent de plus en plus, avec les conséquences négatives qui en découlent, dont certaines ont également été rapportées dans les médias. Nous constatons donc actuellement une forte tendance à l'aggravation de l'état des menaces.

L'état des menaces demeure complexe. Les pirates profitent de la valeur croissante des actifs virtuels, ce qui augmente leur motivation à mener des attaques ciblées.

Entretien avec Costin Raiu

(responsable de l'équipe GReAT chez Kaspersky)

Nous avons eu l'occasion de poser à Costin Raiu six questions qui portent sur les APT et d'obtenir un aperçu de ses expériences et observations en tant qu'expert en la matière.

1. Costin Raiu, quelles sont les principales caractéristiques d'une menace persistante avancée (APT)?

De notre point de vue, il s'agit de tout ce qui rend un logiciel malveillant ou une attaque plus avancé:

- L'*utilisation d'un exploit Zero Day,* comme avec Sofacy, aussi connu sous le nom d'APT28, Pawn Storm ou FancyBear. C'est probablement le champion toutes catégories pour ce qui est du nombre d'exploits Zero Day découverts.
- Une *plate-forme modulaire très complexe* pour réaliser diverses fonctions, comme Regin et ProjectSauron.
- L'*utilisation de techniques sophistiquées d'infection, de persistance ou d'exfiltration.* A titre d'exemple, RedOctober a utilisé un mécanisme de persistance très intelligent sous la forme d'un plugin Office et Adobe Reader, qui a la capacité d'exécuter du code caché dans des documents spécialement conçus à cet effet; cette sophistication recouvre également diverses techniques de bootkit.

La *réplication lente* couplée à la *persistance au niveau du réseau,* l'*infection du matériel réseau professionnel,* comme les routeurs centraux, et les *attaques de la chaîne d'approvisionnement* comptent également au nombre des caractéristiques des APT.

Duqu2, SYNful Knock ou Shadowpad ainsi que la version corrompue de CCleaner en sont de parfaits exemples, qui permettent de comprendre comment ces attaques ont été menées.

Cette liste est loin d'être exhaustive. S'y ajoutent notamment les attaques sur les fonctionnalités matérielles, l'infection du BIOS, les attaques destructives contre le matériel avec Stuxnet, l'un des exemples les plus frappants, ou les logiciels malveillants multi-plateformes.

2. Quels sont les changements les plus importants que vous observez dans les activités APT et quels sont les domaines les plus touchés par ces changements?

Nous suivons actuellement plus de 100 groupes et opérations APT. Nous avons commencé à suivre les groupes APT sur une base régulière en 2010, après l'histoire de Stuxnet, et quand il est devenu clair que c'était une tendance, nous avons décidé de continuer. Dès que nous avons eu connaissance d'une centaine de groupes et d'opérations APT, à savoir en 2015, nous avons lancé notre service de reporting APT privé aussitôt ou à peu de choses de près.

Nous observons également de plus en plus de groupes APT s'engageant dans des attaques sans fichier. Du coup, il est plus difficile de détecter les infections, car aucun fichier malveillant ne se trouve sur le système. De plus, nous voyons un nombre croissant de groupes adopter des outils publics tels qu'Empire Powershell, Metasploit, Cobalt Strike ou Mimikatz. Il est donc difficile de les distinguer.

3. Vous avez été amené à analyser de nombreuses APT. Quelle a été la plus intéressante?

Duqu2, probablement. Tout d'abord, nous avons pensé que Duqu2 était spéciale parce qu'elle ciblait Kaspersky Lab. L'idée d'une APT ciblant spécifiquement une société de sécurité est plutôt audacieuse, car rien ne laisse supposer que l'intrusion ne sera pas détectée. D'autre part, Duqu2 était assez particulière dans la mesure où, en tant que menace «memory-only», elle n'existait durant son exécution que dans la mémoire de plusieurs systèmes informatiques, sans artefacts sur les disques. Ces circonstances ont beaucoup compliqué sa détection. Enfin, recourir à un exploit 0 Day dans Windows pour contourner les produits Kaspersky nous a semblé très intéressant et a abouti à plusieurs améliorations de nos produits en vue de détecter un tel comportement à l'avenir.

4. Quelles sont les erreurs typiques commises par les organisations lorsqu'elles se préparent à une attaque APT et, le cas échéant, comment réagissent-elles?

La plupart des organisations se concentrent sur la prévention de tout accès à leurs ressources internes mené par un assaillant externe, mais peu prennent des mesures pour détecter cet assaillant une fois qu'il a accédé au réseau interne. Comme je l'ai appris au cours de nos recherches, les pirates passent la plupart de leur temps à opérer des mouvements latéraux et des exfiltrations. Les organisations devraient donc se concentrer sur ces phases. De plus, la mise en œuvre des mesures d'atténuation du TOP35[1] du DSD australien contre les APT est insuffisante.

[1] https://acsc.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm

5. Quelles sont les erreurs typiques que commettent les pirates pendant leurs opérations? Selon vous, où chercher l'avantage dont les organisations pourraient bénéficier face à leurs adversaires?

Il nous arrive souvent de nous rendre compte d'erreurs en matière d'OPSEC, telles que les échecs VPN, les chemins PDB oubliés dans les binaires ou les horodatages de compilation, qui laissent la porte ouverte aux pirates.

6. Quelles sont les ressources les plus importantes pour se préparer à des intrusions APT à grande échelle?

Pour les entreprises, il est essentiel d'avoir accès à un système de renseignement privé sur les menaces, de disposer d'un Security Operation Center pleinement fonctionnel, de mettre en œuvre un filtrage réseau, ainsi que de détecter les mouvements latéraux et les mécanismes d'exfiltration. En outre, les organisations doivent savoir et comprendre à la perfection de quelle manière travaillent les assaillants. Par exemple, connaître les outils qu'ils utilisent et la façon dont ils opèrent pendant les phases d'attaque. Dans leur grande majorité, ils se servent de Mimikatz, Powershells et Webshells.

A propos de Costin Raiu

Costin Raiu est spécialisé dans l'analyse des menaces persistantes avancées (APT) et des attaques malveillantes complexes. Il dirige l'équipe Global Research and Analysis Team (GReAT) de Kaspersky, qui a notamment étudié les opérations de Stuxnet, Duqu, Flame et EquationGroup. Costin a plus de 19 ans d'expérience dans les technologies antivirus et la recherche dans le secteur de la sécurité. Il est membre du Virus Bulletin Technical Advisory Board, membre de la Computer AntiVirus Researchers' Organisation (CARO) et rapporteur pour la Wildlist Organisation International. Avant de rejoindre Kaspersky Lab, Costin a travaillé pour GeCad en tant que chercheur en chef et au sein du RAV Antivirus Development Group en tant qu'expert en sécurité des données.

Composantes de l’attaque ciblée

Les médias rapportent souvent que des entreprises sont infectées par un malware ou qu'un malware a été utilisé pour voler des données à une entreprise.

Les médias rapportent souvent que des entreprises sont infectées par un malware ou qu'un malware a été utilisé pour voler des données à une entreprise. Pour comprendre les attaques ciblées, nous devons comprendre que ce n'est pas le malware qui commet les attaques, mais les entreprises qui sont attaquées par des personnes. Dans le cyberespace, on les désigne souvent par le terme «acteurs» (Threat Actors / Cyber Operators) et ils sont les principaux éléments à l'origine de l'attaque. Les acteurs à l'origine des attaques ciblées n'effectuent pas ces dernières sans discernement, mais ont un objectif stratégique, des motivations extrêmement variées et des techniques diversifiées servant de composantes supplémentaires d'une attaque ciblée et identifiées ultérieurement.

Threat Actor Landscape

La mission, l'objectif stratégique, a des intentions complètement différentes selon l'acteur et chaque acteur dispose de capacités très diverses pour les mettre en pratique. Pour une meilleure orientation et évaluation du potentiel et de la motivation des différents acteurs, nous les répartissons dans les groupes suivants:

Les menaces persistantes avancées et l'attaque ciblée

La menace persistante avancée (APT) appartient à la catégorie reine des cyberacteurs. L'exécution des attaques ciblées d'une APT repose sur une mission conçue pour obtenir un avantage stratégique afin d'atteindre des objectifs politiques ou d'influencer positivement les développements technologiques. Dans ce contexte, les APT sont supposées provenir d'un gouvernement ou de son représentant. La particularité de l'APT consiste en ce que les attaques qui lui sont associées sont considérées comme «parrainées par l'Etat», ce qui signifie explicitement que les acteurs sont acceptés par ce dernier et représentent donc des pirates «légaux» (ou du moins protégés par l'Etat). La légalité étatique, la traçabilité difficile et la mise en œuvre relativement sans risque ont conduit de plus en plus d'Etats à étendre leurs cybercapacités et leurs attaques APT.[2]

[2] https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf

Outre les APT «légales», il existe un autre groupe marginal qui peut être considéré comme les pionniers d'Etats ou de gouvernements n'ayant pas encore développé les capacités nécessaires pour mener eux-mêmes des attaques avancées telles que celles d'une APT. En tous cas, depuis les révélations de l'hacktiviste Phineas Phisher sur la société Hacking Team, il est devenu clair que ce groupe marginal poursuit des objectifs financiers et stratégiques clairs.[3]

Les cybercriminels et l'attaque ciblée

Les cybercriminels sont avant tout opportunistes et utilisent tous les moyens d'attaque disponibles (p. ex., un exploit contre Microsoft Office qui a été publié) contre un large éventail de cibles. S'ils obtiennent un nouveau moyen d'attaque, ils l'utilisent, afin de profiter d'autant d'attaques que possible. Outre les attaques opportunistes, il existe aussi des attaques ciblées et bien organisées qui visent à voler un grand nombre de données ou d'autres valeurs d'une cible spécifique au moyen d'une seule attaque qui peut être converti en argent. Pour cela, les assaillants ont besoin de beaucoup de temps («Dwell Time») dans le système de la cible. De tels criminels organisés n'ont souvent rien à envier à de nombreuses APT en termes de capacités techniques. La différence décisive réside toutefois dans les objectifs stratégiques de ces acteurs.

Les terroristes et l'attaque ciblée

Alors que la société craint que les terroristes n'attaquent des systèmes critiques, pas un seul cas n'a été signalé où les terroristes ont poursuivi et atteint leurs objectifs stratégiques grâce à des cyberattaques ciblées. Au contraire, a propos des craintes exprimées à ce jour, le Cambridge Centre for Risk Studies n'a observé aucun groupe terroriste non étatique ayant développé la capacité de mener des cyberattaques avancées et ciblées qui pourraient causer des dommages physiques.[4] Dans le même temps, le World Wide Threat Assessment 2018 de la US Intelligence Community évalue que le cyberespace est principalement utilisé par les terroristes à des fins médiatiques.[5]

Nous continuons de penser qu'il existe un danger de cyberterrorisme et qu'il jouera un rôle plus important à l'avenir.

Les hacktivistes et l'attaque ciblée

Les hacktivistes mènent généralement des attaques ciblées par motivation politique pour exprimer leur protestation. Ils se rassemblent dans le monde entier au sein de groupes de personnes partageant les mêmes idées pour coordonner et cibler les attaques, ou ils mènent ces dernières en solitaires. Les compétences varient considérablement d'un hacktiviste à un autre. Il s'agit d'atteindre le plus rapidement possible l'objectif stratégique décisif et d'attirer l'attention des médias. Jusqu'à présent, il a été observé que ces acteurs menaient principalement des opérations Smash and Grab afin de faire connaître leur réussite aussi rapidement que possible.

[3] https://arstechnica.com/information-technology/2016/04/how-hacking-team-got-hacked-phineas-phisher/
[4] https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/180620-slides-evan.pdf
[5] https://www.wilsoncenter.org/article/world-wide-threat-assessment

Targeting

Les objectifs (targets) des attaques ciblées ne sont pas choisis au hasard, mais en fonction d'une relation spécifique entre la cible et l'assaillant.

Target of Interest

Plus la cible de l'attaque répond aux besoins de l'assaillant, plus son importance augmente et plus elle devient la cible d'intérêt (Target of Interest - TOI) pour les acteurs. Les principaux aspects qui décrivent ce besoin sont la caractéristique spécifique de la cible, l'effort requis et les coûts associés à l'exécution de l'attaque, ainsi que les risques qui peuvent survenir pour l'assaillant.

Target of Opportunity

La cible d'opportunité (Target of Opportunity - TOO) est d'importance secondaire. Ces objectifs répondent à un besoin secondaire des acteurs et sont compromis afin d'être utilisés comme point de départ pour atteindre la cible d'intérêt réelle. Il est également possible, cependant, que la cible ait été sensible (vulnérable) à une Capability à un moment donné et qu'elle ait été compromise. Cela peut parfois conduire à ce que la cible d'opportunité devienne la cible d'intérêt si les acteurs découvrent plus tard que la victime représente une valeur supérieure à celle qui avait été détectée initialement.[6]

Plus la cible de l'attaque répond aux besoins de l'assaillant, plus son importance augmente et plus elle devient la cible d'intérêt (Target of Interest - TOI) pour les acteurs.

[6] www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

Exécution de l’attaque

Il existe de nombreuses méthodes pour décrire l'exécution d'une cyberattaque. Nous avons choisi le framework ATT&CK du MITRE, dont les données sont basées sur des attaques exécutées dans le monde réel. ATT&CK est une méthode similaire à la Cyber Killchain[7] pour décrire les cyberattaques[8]. Alors que la Cyber Killchain est plutôt une description d'ensemble, le framework ATT&CK détaille les activités de plus de 80 (groupes de) Threat Actors. ATT&CK contient principalement les techniques de menaces persistantes avancées dans les différentes phases d'attaque, décrites par les tactiques, techniques et procédures (TTP)[9] de ces acteurs.

Notre analyse des données s'est déroulée sur plusieurs semaines via ATT&CK Enterprise[10] (ci-après ATT&CK), le dernier accès ayant eu lieu en janvier 2019. Le framework ATT&CK est continuellement étendu et mis à jour. Les données du framework et l'expérience de l'équipe GReAT de Costin Raiu permettent cependant des évaluations très précises, tant qualitatives que quantitatives.

En janvier 2019, ATT&CK comptait

Nous avons compilé dans les chapitres suivants les principaux enseignements de haut niveau tirés du framework ATT&CK, selon nous, en mettant clairement l'accent sur la menace persistante avancée.

[7] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
[8] https://www.mitre.org/publications/technical-papers/mitre-attack-design-and-philosophy
[9] https://apps.dtic.mil/dtic/tr/fulltext/u2/1004650.pdf
[10] https://attack.mitre.org/matrices/enterprise/

Les phases d'attaque

Par tactiques (Tactics), ATT&CK entend les différentes phases d'attaque qu'un Threat Actor doit traverser pour atteindre son objectif stratégique. Dans ce contexte, on parle aussi d'objectifs tactiques. ATT&CK définit les tactiques suivantes:

Initial Access	La phase d'accès initiale est le point de départ de toutes les phases ultérieures de l'attaque. Elle inclut le contact initial avec la cible de l'attaque et la compromission du patient zéro.
Persistence	Les points de persistance au sein du réseau cible continuent d'assurer l'accès au réseau. Plus la cible (Target of Interest) est importante, plus l'effort requis pour la persistance d'une intrusion à long terme est important.
Privilege Escalation	L'escalade de privilèges est souvent nécessaire pour installer des logiciels malveillants ou des points de persistance. Des privilèges accrus sont parfois nécessaires pour s'étendre à d'autres systèmes ou pour avoir accès à des objectifs stratégiques (p. ex. des données).
Discovery	L'exploration au sein du réseau cible est nécessaire pour localiser les données, les systèmes et les utilisateurs pertinents pour la mission.
Lateral Movement	Il s'agit de la propagation au sein du réseau, vers les données pertinentes pour la mission. Ces mouvements latéraux incluent souvent la phase d'exécution et l'installation d'autres points de persistance.
Collection	Les données pertinentes pour la mission sont recueillies.
Exfiltration	Il s'agit de la phase finale pour mener à bien la mission et elle comprend l'exfiltration des données pertinentes.

Les phases suivantes se déroulent parallèlement à ces phases et dépendent de la réalisation des objectifs de chacune d'elles:

Execution

L'exécution de codes malveillants sur un système local ou distant a lieu principalement lors des phases d'accès initial et de mouvement latéral. Sans exécution de code sous le contrôle de l'assaillant, la phase suivante ne pourrait pas être atteinte. L'exécution est donc l'une des conditions préalables les plus importantes pour le développement ultérieur de l'attaque et de la propagation dans le réseau cible.

Defense Evasion

Le contournement des mécanismes de défense et de détection – comme la désactivation du pare-feu au niveau du Endpoint ou la suppression des données du journal – est l'un des objectifs tactiques que l'auteur utilise dans chacune des autres phases de sa mission pour dissimuler sa présence ou contourner les mécanismes de détection.

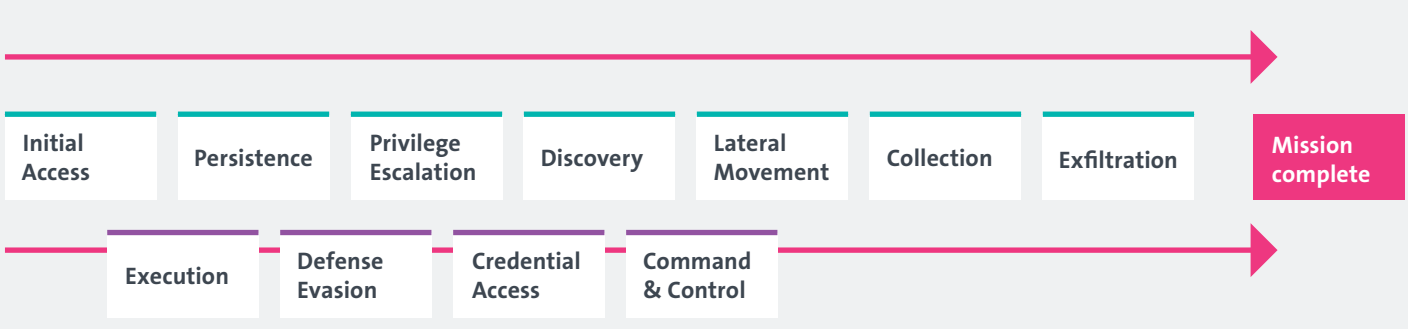
Credential Access

Les données d'accès jouent un rôle clé pour les assaillants. D'une part, elles permettent des intrusions et des mouvements inaperçus au sein du réseau cible. D'autre part, elles donnent accès aux données que les assaillants veulent obtenir. De plus, en les réutilisant, les assaillants sont en mesure d'effectuer leur attaque en économisant les ressources, puisqu'aucun exploit ne doit être écrit, acquis, ni autrement utilisé.

Command & Control

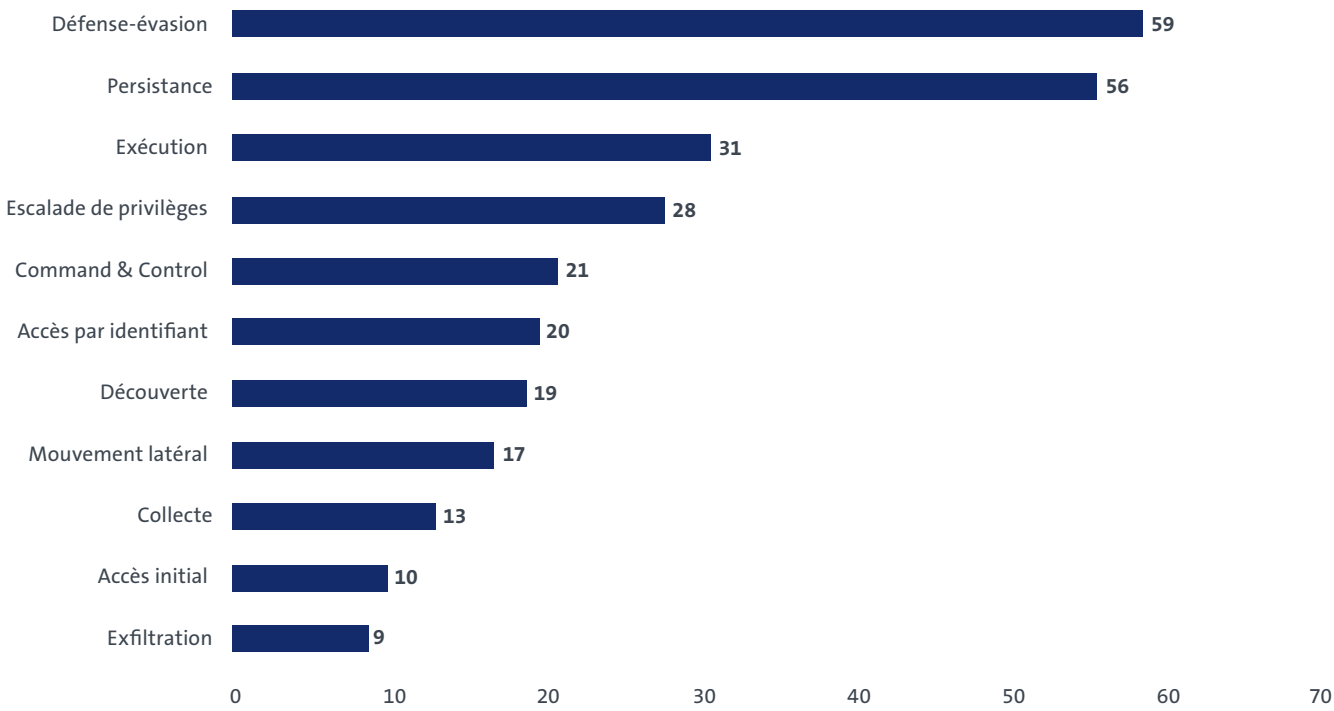
Le canal Command & Control est le moyen de communication de l'assaillant pour garder l'infrastructure cible compromise sous contrôle. S'il le perd, l'attaque sera interrompue. Les assaillants ciblés établissent souvent plusieurs canaux de commandement et de contrôle.

L'illustration suivante montre la relation entre les phases:



Techniques des acteurs

Afin d'atteindre ou de passer par une phase spécifique, les acteurs du framework ATT&CK[11] utilisent une grande variété de modes opératoires spécifiques, également appelées techniques. Chaque phase peut contenir plusieurs techniques et les techniques peuvent être présentes dans plusieurs phases. ATT&CK contient 224 de ces techniques, qui sont réparties sur les différentes phases comme suit:



Le diagramme à barres donne un aperçu du modus operandi des acteurs et montre clairement dans quelles phases ces derniers ont le plus et le moins de capacités. Ainsi, si l'on considère les phases sous l'angle du nombre de techniques disponibles, l'analyse montre que les acteurs peuvent accéder à un très large spectre pour tirer parti des mécanismes de défense dans les différentes phases de l'attaque via défense-évasion et disposent d'autant de techniques pour assurer un accès durable dans la phase de persistance.

Extrait de l'interview de Costin Raiu, qui confirme cette affirmation:

Quelles sont les ressources les plus importantes pour se préparer à des intrusions APT à grande échelle?

Les organisations doivent savoir et comprendre à la perfection de quelle manière travaillent les assaillants. Par exemple, connaître les outils qu'ils utilisent et la façon dont ils opèrent pendant les phases d'attaque. Dans leur grande majorité, ils se servent de Mimikatz, Powershells et Webshells.

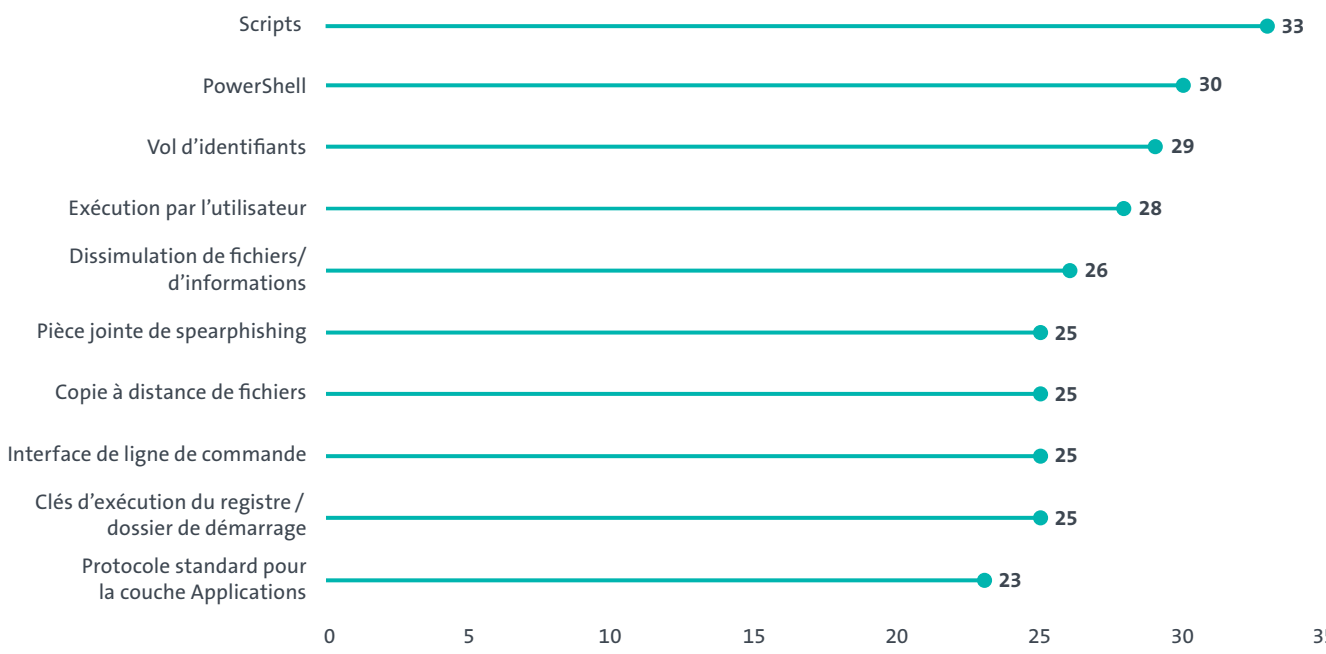
[11] https://attack.mitre.org/

Techniques les plus utilisées par les acteurs
Une évaluation des groupes APT et de leurs techniques montre une nette tendance aux fileless attacks (comprendre «attaques sans fichier»), ce qui est également confirmé par Costin Raiu.

L'illustration suivante montre le top 10 des techniques les plus fréquemment utilisées parmi les 80 acteurs d'ATT&CK:

Quels sont les changements les plus importants que vous observez dans les activités APT et quels sont les domaines les plus touchés par ces changements?

Nous observons également de plus en plus de groupes APT s'engageant dans des attaques sans fichier. Du coup, il est plus difficile de détecter les infections, car aucun fichier malveillant ne se trouve sur le système.



Les 10 meilleures techniques peuvent être regroupées sous les deux thèmes «Living off the Land» et «Méthodes éprouvées».

Living off the Land

De plus en plus de groupes APT utilisent des scripts qui sont désormais intégrés par défaut dans les systèmes d'exploitation Windows, comme les interfaces Powershell et Command-Line, pour exécuter leur code malveillant. Ceci, sans que les solutions White Listing des applications ne le détectent et qu'aucune trace significative ne soit laissée sur le système.

En tant que mécanisme de persistance, les clés d'exécution du registre et les entrées dans le dossier de démarrage de Windows restent les techniques les plus populaires parmi les acteurs.

Des méthodes éprouvées mènent au but

Tous les acteurs n'ont pas les ressources nécessaires pour développer les «Zero Day Exploits». Un grand nombre d'acteurs continuent de s'appuyer sur les pièces jointes de spear phishing (Spear Phishing Attachments) et l'exécution par l'utilisateur (User Execution) pour que ce dernier exécute le code malveillant.

Les acteurs APT utilisent des moyens simples pour atteindre leur but. Le vol d'identifiants (Credential Dumping) obtenue, puis utilise des données d'accès valides pour se déplacer à l'intérieur de l'infrastructure et en assurer l'accès.

Le chargement et le stockage supplémentaires de codes sous le contrôle de l'assaillant, la simple copie de fichiers (Remote File Copy) via des protocoles légitimes (Standard Application Layer Protocol) et l'application de codage et de cryptage (Obfuscated Files or Information) restent les techniques les plus populaires pour l'exfiltration des données.

Logiciel des acteurs

Le logiciel utilisé par les acteurs met en œuvre les techniques nécessaires pour une phase d'attaque. Pour cela, les acteurs s'appuient sur différentes catégories de logiciels qui représentent un outil, un utilitaire ou un malware au sein d'ATT&CK.[12]

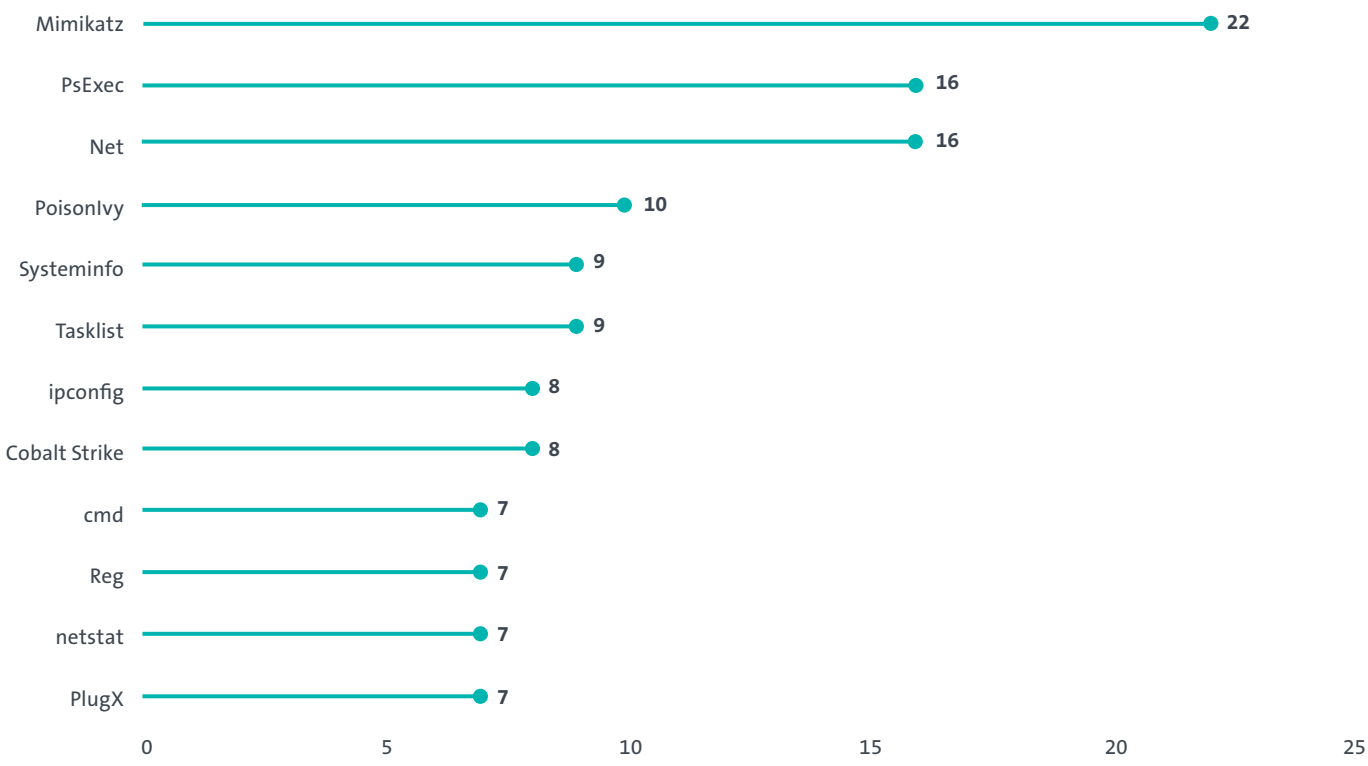
[12] https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philosophy.pdf

Logiciels les plus utilisés par les acteurs
Une analyse des groupes APT et des logiciels qu'ils utilisent montre que les outils et logiciels du commerce déjà fournis par le système d'exploitation sont les plus couramment utilisés. Ce constat va de pair avec l'expérience de Costin Raiu.

L'illustration suivante montre le top 10 des logiciels les plus fréquemment utilisés par les 80 acteurs d'ATT&CK.

Quels sont les changements les plus importants que vous observez dans les activités APT et quels sont les domaines les plus touchés par ces changements?

Nous voyons un nombre croissant de groupes adopter des outils publics tels qu'Empire Powershell, Metasploit, Cobalt Strike ou Mimikatz. Il est donc difficile de les distinguer.



Contre-mesures et effets

Les contre-mesures contre les attaques ciblées se fondent sur une protection de base, reposant sur des mesures préventives telles que l'application des correctifs actuels, la mise en œuvre de l'authentification à deux facteurs, les connexions Internet par proxy uniquement, etc. Ces mesures sont parfois suffisantes pour orienter l'intérêt des acteurs non étatiques vers d'autres objectifs.

Dans les chapitres précédents, nous avons examiné les aspects fondamentaux des Threat Actors, qui se reflètent dans les objectifs stratégiques (Intent), la surface d'attaque (Opportunity) et les techniques (Capability). Ce sont précisément ces aspects qui doivent être pris en compte afin d'élaborer des contre-mesures appropriées ayant l'impact le plus efficace. La défense la plus efficace consisterait probablement à éliminer l'objectif stratégique (Intent). Les gouvernements ou les entreprises qui ne conservent pas de données ne deviennent pas la cible d'un acteur étatique qui fait de l'espionnage et qui veut tirer un avantage des données volées. Toutefois, cette défense ne peut être mise en œuvre que dans de très rares cas. Si l'on examine la surface d'attaque disponible, on constate qu'elle a augmenté plutôt que diminué au cours des dernières années. La numérisation croissante, le stockage de données dans le cloud et tout ce qui s'y rattache ainsi que les dispositifs «always-on» et IoT contribuent à créer une surface d'attaque d'une taille exorbitante pour les entreprises, la société et les individus.

Nous devons donc baser nos contre-mesures sur les capacités et les techniques des Threat Actors, ce qui se termine souvent par une course au coude à coude et semble extrêmement complexe à première vue étant donné la multitude des techniques.

En y regardant de plus près, il apparaît toutefois que la plupart des techniques et des logiciels utilisés peuvent être identifiés par des méthodes de détection qui suivent l'activité du système.

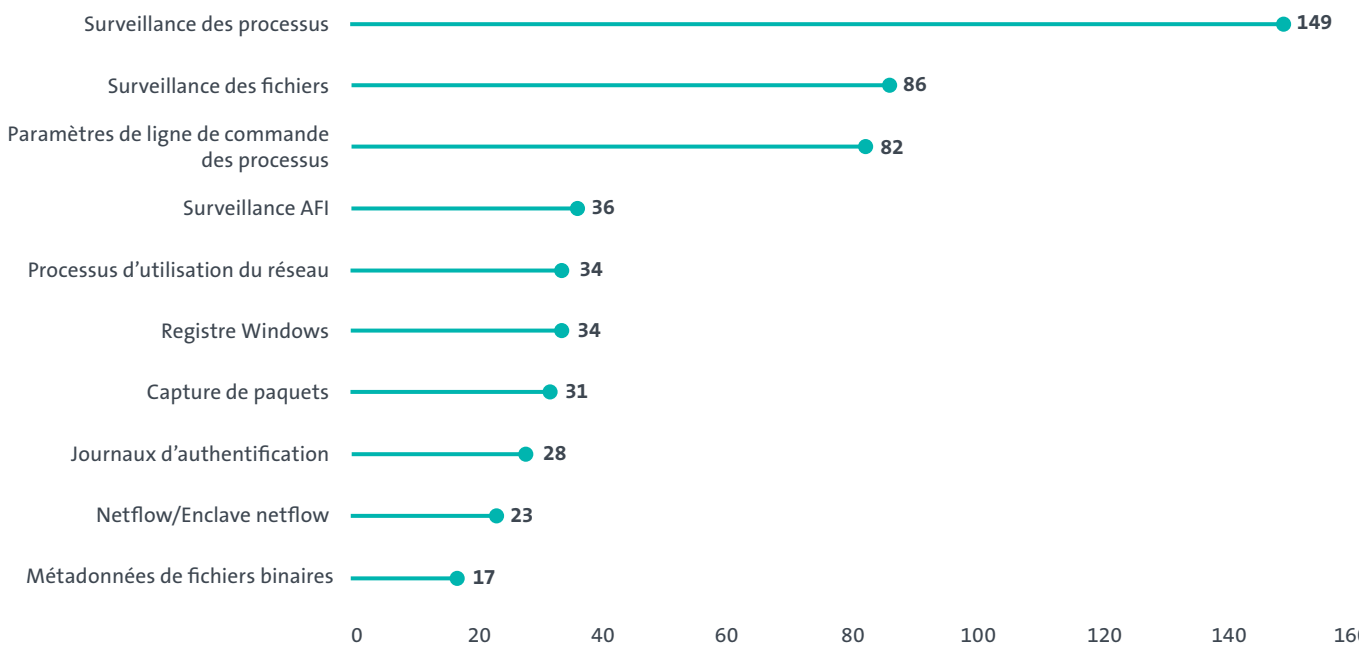
Méthodes de détection les plus complètes

Notre analyse montre qu'une grande partie des techniques des acteurs peut être identifiée par le suivi des processus et des opérations de fichiers. Il faut comprendre que ces méthodes de détection sont les plus prometteuses pour pouvoir suivre les activités d'un attaquant après l'accès initial.

L'illustration suivante des 10 principales méthodes de détection le démontre une fois de plus:

Quelles sont les erreurs typiques commises par les organisations lorsqu'elles se préparent à une attaque APT et, le cas échéant, comment réagissent-elles?

La plupart des organisations se concentrent sur la prévention de tout accès à leurs ressources internes mené par un assaillant externe, mais peu prennent des mesures pour détecter cet assaillant une fois qu'il a accédé au réseau interne.



Les méthodes de détection des activités de processus identifient une grande partie des techniques existantes des acteurs. Les activités des utilisateurs et du réseau fournissent un contexte supplémentaire.

Activités du système

L'exécution du code sous le contrôle des acteurs est une condition préalable à la réalisation de l'objectif stratégique de ces derniers. Pour suivre leur schéma d'attaque, et notamment pour détecter leurs techniques, la surveillance des processus, des fichiers et des changements survenant dans le registre Windows constitue la méthode la plus efficace. Même si cette forme de détection apporte la plus grande valeur ajoutée, il faut s'attendre à un volume de données très élevé et à des ajustements. Les opérations de fichiers et de registre, les connexions réseau et les processus doivent être bien compris.

Activités des utilisateurs et du réseau

Outre la surveillance des activités du système, les données réseau et les journaux d'authentification des utilisateurs fournissent une visibilité sur une grande partie des techniques des acteurs.

Que fait Swisscom?

La probabilité des attaques ciblées ne cesse d'augmenter et les moyens technologiques actuellement disponibles sont souvent insuffisants pour faire face aux compétences des cyberacteurs professionnels. Pour ces raisons, Swisscom s'appuie sur un modèle de sécurité basé sur le risque qui promeut une solide culture de la sécurité au sein de l'entreprise via la formation des collaborateurs, qui intègre la communauté dans la culture de la sécurité, p. ex. à travers le programme Bug Bounty[13], et qui implique des mesures de sécurité préventives fondamentales telles que la White Listing et le patching d'applications ou la limitation du trafic réseau et des pièces jointes aux e-mails. La prévention n'est qu'un domaine parmi d'autres qui, en fin de compte, échouera face à des acteurs très motivés. Il est donc nécessaire de se montrer proactif et de comprendre les tactiques, techniques et procédures des acteurs, puis d'intégrer les connaissances acquises dans la détection. Nous appelons cette approche Threat Intelligence comme base de détection et nous la concrétisons, par exemple, en simulant une attaque ciblée par Red Teaming, en cartographiant la recherche de menaces non découvertes sur notre réseau par Threat Hunting et en échangeant régulièrement des informations avec d'autres entreprises du même secteur, dans des groupes de partage.

Red Teaming

Les assaillants ayant toujours une longueur d'avance, nous devenons nous-mêmes des assaillants. Swisscom a décidé en 2015 d'innover et a été la première entreprise suisse à créer une Red Team officielle. La Red Team se compose d'un petit groupe de collaborateurs qui mènent autant que possible de véritables attaques contre l'infrastructure et les services de Swisscom. Ce sont des hackers éthiques, c'est-à-dire des hackers avec de bonnes intentions, qui mènent des attaques ciblées contre Swisscom, mais PAS contre les applications et données des clients finaux.

Quels sont leurs objectifs?

- Trouver les vulnérabilités et identifier leur impact avant les autres.
- Tester la Blue Team et aider l'entreprise à développer des contre-mesures et à améliorer les processus.
- Apprendre des incidents survenus dans d'autres entreprises et tester s'ils auraient pu se produire chez Swisscom.

La probabilité des attaques ciblées ne cesse d'augmenter et les moyens technologiques actuellement disponibles sont souvent insuffisants pour faire face aux compétences des cyberacteurs professionnels.

[13] https://www.swisscom.ch/en/about/company/portrait/network/security/bug-bounty.html

Threat Hunting

Le Threat Hunting vise à détecter des menaces qui ne l'avaient pas été auparavant. Il ne remplace pas un Security Operation Center (SOC) opérationnel, mais utilise des méthodes partiellement automatisées, ainsi que manuelles, pour détecter les comportements et les schémas d'attaque qui ne peuvent l'être par les mécanismes de protection existants. Cette technique fournit, par exemple, de nouvelles méthodes de détection. L'équipe CSIRT de Swisscom organise régulièrement des sessions de Threat Hunting pour détecter les menaces au sein du réseau Swisscom. Le framework ATT&CK sert souvent de référence pour comprendre les tactiques et les techniques des différents acteurs. Dans ce contexte, CSIRT publie régulièrement de nouvelles méthodes de détection pour SIGMA[14] et YARA[15], et les rend accessibles à la communauté. SIGMA est un format de signature générique et ouvert qui permet de décrire une fois les données de journal pertinentes en tant que (méthode de) détection et de les utiliser pour une multitude de SIEM et de systèmes de journal. SIGMA est l'un des rares outils qui peut décrire des attaques avec les tactiques et techniques ATT&CK, et rend la détection directement utilisable par les autres. Avec YARA, il est possible de créer ses propres signatures et détections, qui peuvent être utilisées aussi bien pour les fichiers que pour les scans mémoire. L'équipe CSIRT de Swisscom crée régulièrement des règles YARA relatives aux outils utilisés par les assaillants, qu'elle partage avec des communautés publiques telles que la base de signatures de Florian Roth[16] ou d'autres communautés fermées.

Comme indiqué dans les chapitres précédents, il est important de comprendre que les attaques ne sont pas menées par des systèmes, mais par des personnes, et qu'il faut des personnes pour y répondre. C'est pourquoi Swisscom dispose de plusieurs Security Operation Center (SOC) afin d'enquêter systématiquement sur les possibles activités des agresseurs. Les analystes de l'équipe CSIRT de Swisscom deviennent opérationnels dès que l'activité détectée indique des attaques plus ciblées sur l'infrastructure informatique de Swisscom.

Groupes de partage et communauté

En plus de partager les détections basées sur SIGMA et YARA, les collaborateurs de l'équipe CSIRT de Swisscom sont des membres actifs de nombreux groupes de confiance qui œuvrent à la coopération opérationnelle quotidienne des équipes CSIRT, SOC et Threat Intelligence. L'objectif de ces groupes de confiance est de réunir des personnes qui rencontrent les mêmes problèmes au quotidien et de simplifier l'échange. Swisscom diffuse régulièrement des informations sur les observations actuelles, les menaces ainsi que les indicateurs de logiciels malveillants et d'attaques au sein de ces groupes de partage et communautés.

Protection complète de l'entreprise grâce à une détection précoce et à une action professionnelle en cas d'attaques de cybersécurité – disponible en tant que service

Des quantités gigantesques d'informations d'entreprise et personnelles sont désormais disponibles sur différentes sources de données (réseaux, applications, terminaux, médias sociaux, cloud, Darknet, etc.). Face à une mise en réseau et à une numérisation qui ne cessent de progresser, les menaces sont de plus en plus multiformes. Il est essentiel de détecter à temps les incidents liés à la sécurité.

Un Threat Detection & Response professionnel exige des processus et des outils spécifiques, de nombreuses années d'expérience ainsi que des collaborateurs hautement spécialisés. Une entreprise ne peut plus, à elle seule, comprendre les attaques de cybersécurité en

[14] https://github.com/Neo23x0/sigma/

[15] https://yara.readthedocs.org

[16] https://github.com/Neo23x0/signature-base

constante évolution et réagir en conséquence. Un partenaire expérimenté doit apporter son soutien. Depuis des années, Swisscom protège avec succès son infrastructure réseau, ses données clients et produits ainsi qu'elle-même contre les cybermenaces. Elle utilise cette expérience pour minimiser les cyber-risques avec ses clients. Une bonne visualisation des données permet une détection précoce des incidents de sécurité potentiels. Une analyse en temps réel et une réponse appropriée à un incident de sécurité améliorent le niveau de sécurité et l'utilisation des ressources au sein de l'entreprise.

Avec Threat Detection & Response, les entreprises clientes peuvent choisir entre quatre variantes de services, en fonction de l'étendue du soutien que doit leur apporter Swisscom en matière de cybersécurité. En voici un bref aperçu:

Security Analytics as a Service: les clients reçoivent une vue d'ensemble via le tableau de bord sur les incidents de sécurité potentiels à partir des données de journal définies par l'entreprise.

Security Operation Center (SOC) as a Service: outre les solutions Security Analytics, les clients reçoivent des analyses avec des recommandations d'action concrètes et un accès direct aux spécialistes du SOC de Swisscom. Depuis plus de 10 ans, nous offrons des services de SOC aux entreprises suisses dans le pays et à l'étranger. Nos analystes SOC peuvent interpréter les événements et incidents de sécurité avec compétence et rapidité.

Computer Security Incident Response Team (CSIRT as a Service): les experts de Swisscom peuvent être appelés pour analyser et traiter les incidents de sécurité critiques et gérer le processus Security Incident Management. Ces experts expérimentés aident les clients à recueillir les preuves et les assistent dans la communication avec les clients et les partenaires.

Threat Intelligence as a Service: les clients sont informés de manière proactive de l'apparition d'informations commerciales et personnelles sensibles de leur entreprise sur les réseaux publics et fermés (p. ex. Darknet).[17]

Conclusion

Les attaques ciblées, en particulier par des APT ayant des objectifs stratégiques gouvernementaux, ne pourront pas être empêchées dans la plupart des cas. Le monde de plus en plus numérisé attire un nombre croissant d'acteurs dans le cyberespace. Par conséquent, nous devons nous attendre de plus en plus à devenir une cible d'intérêt (Target of Interest) ou du moins une cible d'opportunité (Target of Opportunity) à un moment donné. Les acteurs disposent d'une grande variété de techniques dans les différentes phases d'attaque, pour lesquelles ils recourent toujours davantage à des outils disponibles sur le marché et à des méthodes «Living off the Land». Les APT appartiennent à la catégorie reine des cyber-acteurs, mais plutôt que de développer des «Zero Day Exploits» pour chaque opération, ils utilisent des méthodes éprouvées avec lesquelles les humains demeurent une cible intéressante pour contourner les mécanismes de sécurité et exécuter un code malveillant.

On dit souvent que les assaillants n'ont besoin de réussir qu'une seule fois pour parvenir à leurs fins. Comme notre analyse l'a montré, on peut argumenter au contraire que si l'on étend nos mesures de détection en vue d'identifier leurs techniques, les assaillants n'ont qu'à faire une seule erreur pour être détectés. L'accent mis sur la détection de la phase d'exécution constitue ici une approche prometteuse. Avec les APT en particulier, il faut comprendre l'ensemble du schéma d'intrusion pour que l'attaque soit arrêtée.

[17] Pour plus d'informations et de coordonnées à ce sujet: www.swisscom.ch/detection