Cyber Security 2018:

Intelligence artificielle, logiciels malveillants & crypto-monnaies

Auteur : Swisscom Security
Ce rapport est le fruit d'une étroite collaboration entre Swisscom Security et diverses unités opérationnelles.

Mai 2018

Table des matières

1. Introduction

Le Cyber Security Report de Swisscom entame sa deuxième année d'existence en 2018. Outre l'état des menaces, nous avons étudié deux questions qui préoccupent tout particulièrement la Security Community au sein de Swisscom, nos partenaires et nos clients, mais aussi la communauté internationale à l'heure actuelle.

Le premier thème étudié : l'utilisation de l'intelligence artificielle dans l'environnement Security. D'une part, nous observons son utilisation abusive dans le but de mener des attaques plus intelligentes. D'autre part, nous notons son utilisation la plus judicieuse, à savoir l'identification et l'élimination plus rapides et plus précises des attaques et des failles.

Deuxième thème : les logiciels malveillants que nous avons pu identifier sur notre réseau. Diffuser un malware demeure l'outil le plus puissant des pirates pour compromettre des services, dérober des données ou utiliser de manière abusive des systèmes de tiers à leur avantage. La plupart des attaques reposent sur des motivations financières, il n'est dès lors pas surprenant que les crypto-monnaies figurent en bonne place dans notre rapport.

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

Pour les lectrices et lecteurs pressés, nous avons rédigé une conclusion à la fin de chaque chapitre pour leur communiquer l'essentiel en bref. Par conséquent, nous avons renoncé dans cette édition au résumé global situé à la fin du rapport.

Swisscom a révélé en février dernier que des inconnus avaient accédé illégalement, à l'automne 2017, aux données de ses clients par l'intermédiaire d'un partenaire de distribution. Cet incident n'est pas traité dans le présent rapport. Ne ne souhaitons pas, à travers celui-ci, évoquer des incidents particuliers, mais plutôt indiquer les tendances générales qui se dessinent dans le cyberspace suisse. Nous avons renforcé les mesures de protection en interne afin d'éviter tout nouvel incident de ce type.

2. Situation – radar des menaces

Les menaces trouvent leurs origines dans le développement constant des nouvelles technologies, leur application et leur diffusion au sein de la société. Les menaces potentielles doivent être identifiées le plus tôt possible et enregistrées de manière systématique. Pour représenter l'état des menaces et leur évolution, nous utilisons un radar (cf. illustration 1).

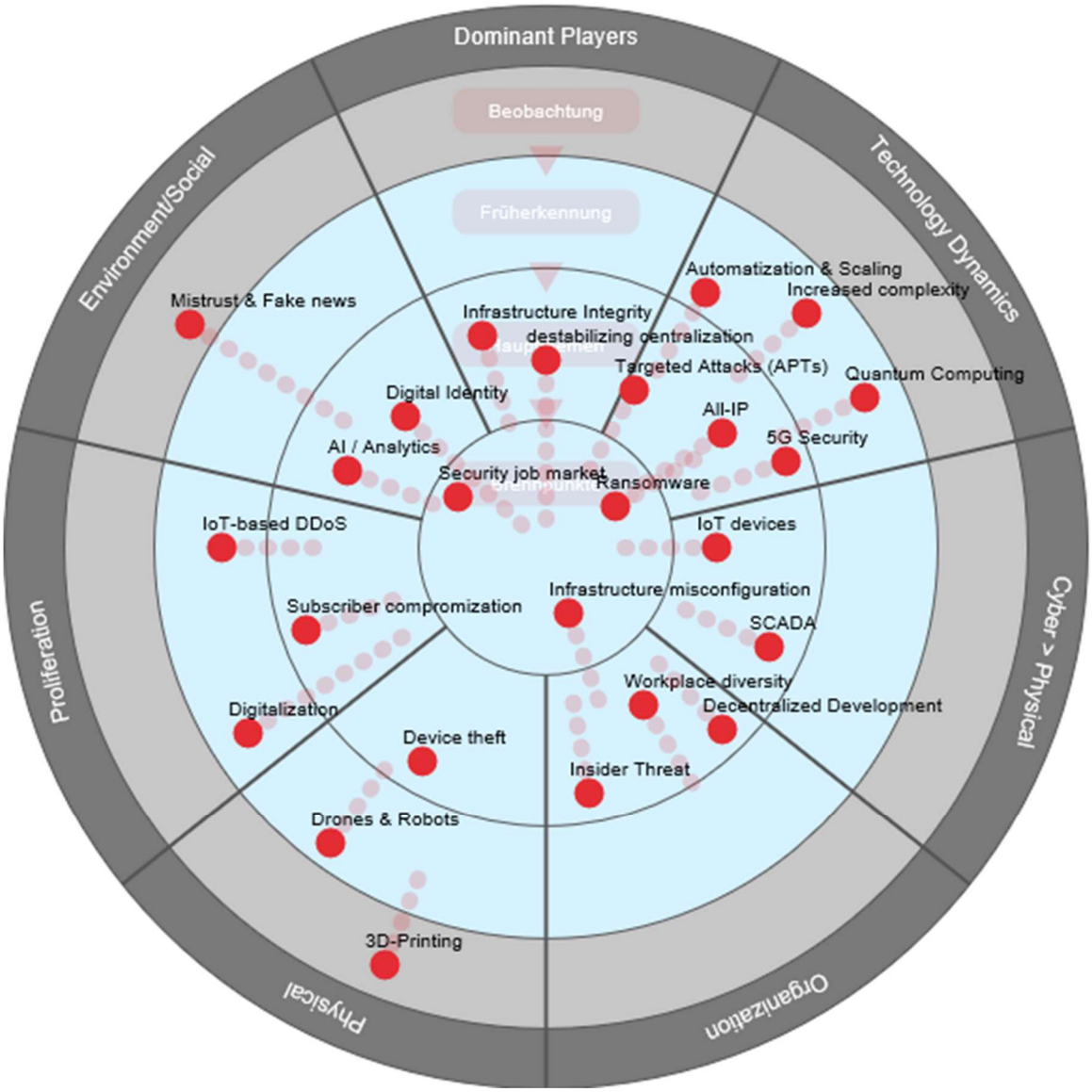

Illustration 1 : radar des menaces

2.1 Méthodologie

Le radar des menaces se compose de sept segments, délimitant les différents champs d'application des menaces. Il est possible de rattacher les menaces associées à chaque segment dans l'un des quatre anneaux concentriques. Les cercles présentent la pertinence de la menace et donc aussi le manque de précision lié à cette dernière. Plus une menace est proche du centre du radar, plus elle est concrète

et plus les contre-mesures sont importantes. Nous considérons les anneaux comme tels :

- **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.
- **Reconnaissances précoces** pour les menaces qui ne sont pas encore survenues ou qui montrent 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.

2.2 Menaces

2.2.1 Dominant players

Menaces résultant des dépendances aux éditeurs, services ou protocoles dominants.

Thèmes principaux	**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. **Destabilizing Centralization :** 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).

2.2.2 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.

Points délicats	**Ransomware :** les données critiques sont cryptées en masse et sont ensuite décryptées (éventuellement) contre le versement d'une rançon.

Thèmes principaux	**Targeted Attacks (APTs) :** des personnes-clés sont identifiées et attaquées de manière ciblée afin d'obtenir des informations pertinentes ou d'occasionner un maximum de dégâts. **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.
Détection précoce	**Automatization & 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.

2.2.3 Cyber goes physical

Les attaques utilisant les infrastructures dans le cyberespace 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.

2.2.4 Organization

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

Point délicat	**Infrastructure Misconfiguration :** exploitation de composants d'infrastructures mal configurés et/ou de failles identifiées et corrigées tardivement.
Thèmes principaux	**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. **Decentralized 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.

2.2.5 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.
Détection précoce	**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.

2.2.6 Proliferation

Menaces résultant des progrès en matière de disponibilité et d'accessibilité des médias informatiques et du savoir-faire. 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 Compromization :** 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. **Digitalization :** l'interconnexion de plus en plus forte entre le virtuel et le réel et la vie privée et professionnelle multiplie les vecteurs d'attaque.

2.2.7 Environmental / Social

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	**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. **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.
Observation	**Mistrust & Fake News :** la perte de confiance à l'encontre des instances étatiques ou sociales peut contribuer à réduire les échanges d'informations pour l'identification et la défense contre des attaques potentielles.

2.3 Conclusion

Le point que nous avons fait de la situation montre que l'état des menaces devient de plus en plus complexe. Les pirates profitent de la valeur croissante des actifs virtuels, ce qui augmente leur motivation à mener des attaques ciblées et intelligentes. Par ailleurs, les innovations technologiques et le rapprochement entre les mondes physique et virtuel ouvrent de nouvelles possibilités d'attaques. Les changements sociétaux se répercutent sur la confiance et sur la manière dont nous travaillons ensemble. Les assaillants peuvent exploiter ces deux facteurs pour leurs besoins.

Par rapport à l'année passée, nous pouvons constater que la plupart des menaces identifiées sont restées pertinentes, sans aucun changement. Certaines menaces, telles que **Destabilizing Centralization**, **5G Security**, **Insider Threat** et l'utilisation de **Ransomware** sont devenues critiques par rapport à 2017. Cette évolution peut s'expliquer par la diffusion plus généralisée des nouvelles technologies (p. ex. dans le cas de 5G Security) ou la multiplication des outils permettant de lancer des attaques (p. ex. dans le cas des rançongiciels).
Nous avons corrigé avec une tendance plus marquée l'hypothèse selon laquelle les menaces restent les mêmes sur les systèmes SCADA. A l'avenir, nous considérons que le problème va s'aggraver du fait d'une connexion toujours plus large des systèmes physiques à Internet.
Nous estimons que les autres menaces sont moins critiques. Ainsi, nous pensons que 3D-Printing et les attaques DDoS basées sur l'IoT ne seront pas aussi fréquentes dans la réalité que nous l'avions craint, mais qu'elles resteront pertinentes.

Nous avons intégré de nouvelles menaces à cette situation. Elles avaient déjà été identifiées l'année dernière, mais avaient été jugées moins critiques, contrairement aux autres menaces. Nous avons réévalué cette estimation. Désormais, de nouvelles

sources de risque sont apparues sur le radar : **Automatization & Scaling, Increased Complexity, Quantum Computing, Decentralized Development, AI / Analytics** et **Digital Identity**. Il est frappant de constater que la dynamique technologique liée à l'environnement de l'intelligence artificielle, qui se traduit d'un côté par des effets positifs sur la cybersécurité, influence d'un autre côté l'état des menaces et aide notamment les assaillants potentiels en leur fournissant des outils intelligents.

3. Intelligence artificielle et cybersécurité

Artificial Intelligence (AI)[1], Machine Learning (ML) et Deep Learning décrivent trois modèles connexes que nous délimitons comme suit :

Artificial Intelligence	L'intelligence artificielle définit l'intelligence simulée par les machines au moyen de la logique, de règles claires et d'arbres de décision.
Machine Learning	L'apprentissage automatique (ou « Machine Learning ») est un champ d'étude de l'AI, qui repose sur des techniques statistiques complexes dans le but de permettre aux machines d'exécuter de mieux en mieux des tâches grâce à l'expérience acquise.
Deep Learning	L'apprentissage profond (ou « Deep Learning ») est une subdivision du Machine Learning, qui permet à un logiciel de s'autoformer afin d'exécuter des tâches telles que la reconnaissance d'une langue et d'une image en mettant d'énormes volumes de données à disposition d'un réseau neuronal multiple.

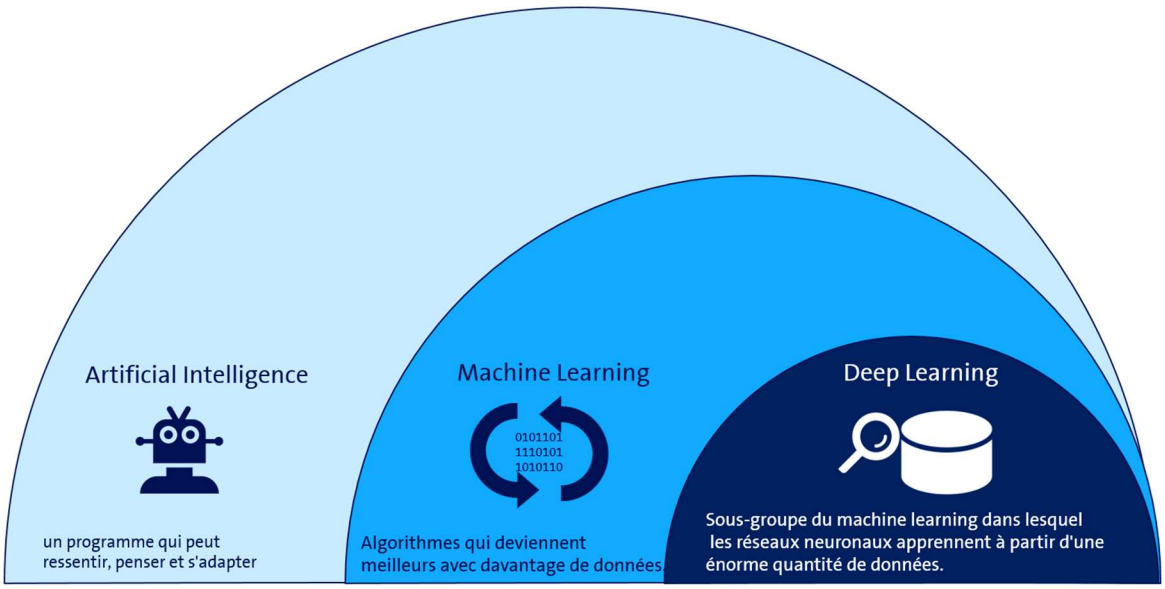

Illustration 2: Artificial Intelligence, Machine Learning et Deep Learning

3.1 Interview avec Laure Willemin, Head of AI chez Swisscom

Laure Willemin et son équipe développent et exploitent des systèmes logiciels résilients et évolutifs en tirant profit des nouvelles technologies apparues dans les secteurs AI, ML et Deep Learning, notamment les outils Enabler Sentiment Analysis, Key Phrase Extraction, Named Entity Recognition. Notre collègue de chez Swisscom

[1] Même si on parle d' «intelligence artificielle» (IA) dans l'espace linguistique francophone, la désignation anglaise a été adoptée dans les technologies de l'information et est donc utilisée ici.

aime se confronter aux défis technologiques complexes et les relève depuis plus de 15 ans en tant que développeuse, ingénieure système et architecte système.

Laure, l'intelligence artificielle est-elle juste une opportunité pour Swisscom et notre société ou doit-elle aussi être considérée comme une menace pour la sécurité ?
Nous n'envisageons pas l'AI comme une menace. Grâce aux nouvelles technologies, nous pouvons aider à mieux comprendre de gros volumes de données et soutenir les efforts de notre entreprise en matière de sécurité. Les nouvelles technologies conduisent souvent à des incertitudes et des malentendus. Elles peuvent également faire l'objet d'une utilisation abusive. Toutefois, les effets positifs l'emportent largement.

Quelles sont les malentendus les plus fréquents auxquels tu as été confrontée jusqu'à présent au sujet de l'intelligence artificielle et du Machine Learning ?
En premier lieu, des attentes trop importantes concernant ce qu'il est possible de faire grâce à l'AI. Les données forment la partie critique d'un système effectif. Souvent, ces données ne sont pas structurées et les systèmes qui les traitent doivent être entraînés, avant de pouvoir les exploiter utilement. Grâce aux nouvelles technologies, nous pouvons faire du bon travail lors de la création des modèles de données et nous enregistrons également des progrès dans le traitement de quantités de données moindres. L'excellente qualité des données est donc le critère essentiel au succès des applications AI.

Considéres-tu l'AI et ML comme des éléments perturbateurs dans le paysage industriel suisse ? Quels sont, à ton avis, les plus grands changements à venir ?
L'intelligence artificielle ne saurait être considérée comme un élément perturbateur, mais plutôt comme un moyen incontournable pour le maintien de la compétitivité, même à l'avenir. Grâce à l'AI, l'industrie suisse sera en mesure d'automatiser les processus et les tâches répétitifs, ainsi que d'employer du personnel qualifié pour les travaux plus complexes, réclamant plus de créativité. Parallèlement, l'AI va aider les individus à prendre de meilleures décisions plus rapidement, par exemple avec l'analyse en temps réel des données.

Dans quelle mesure penses-tu que l'AI, ML et le Deep Learning contribuent à l'évolution de la cybersécurité ?
La technologie AI la plus récente peut servir à analyser d'énormes volumes de données et à détecter plus facilement les anomalies. Ainsi, les incidents de sécurité peuvent être identifiés plus tôt, voire avant de se transformer en problème. La technologie AI ne remplace pas les systèmes ou les experts actuels, mais réduit les efforts souvent manuels, réduit le temps de réponse et améliore par la même occasion la sécurité globale d'une entreprise.

Sur quel projet travailles-tu actuellement ?

Nous développons une nouvelle plateforme de dialogue entre nos clients et nous. Swisscom gère chaque année près de 20 millions d'interactions avec des clients. Ce nombre est en constante progression, car nombreux sont les clients qui passent en général d'un canal à l'autre. Un service de haute qualité sur tous les canaux est donc indispensable à une excellente expérience client. Le client ne doit pas être obligé de redonner ses renseignements à chaque fois qu'il change de canal. Voilà pourquoi Swisscom bâtit une nouvelle plateforme basée sur l'AI ayant pour but de coordonner les différents canaux d'interaction et d'offrir aux clients la meilleure des assistances.

3.2 Applications de l'AI et du ML dans la cybersécurité

Comme nous l'avons montré en faisant le point de la situation pour 2018, plusieurs tendances convergent actuellement vers le développement et la mise en place de solutions AI & ML pour les mesures de cybersécurité.

- Des volumes de données toujours plus importants et des applications AI & ML : il s'agit de les évaluer, sachant qu'ils peuvent être utilisés abusivement pour mener, par exemple, des attaques ciblées plus efficacement.
- Le transfert de valeurs toujours plus substantielles dans l'espace virtuel renforce donc la motivation des organisations criminelles en ce qui concerne l'usage des nouvelles technologies pour dérober ou compromettre ces valeurs.
- En croissance constante et rapide, le besoin en experts en cybersécurité provoque d'ores et déjà des difficultés, à savoir former suffisamment de talents de haut niveau, les faire venir dans les entreprises, les faire évoluer et les conserver. Cette situation va encore nettement s'aggraver dans les années à venir.

3.2.1 Security Operations Center

L'un des piliers d'une stratégie mature de cybersécurité est la capacité de détecter qu'une attaque a eu lieu. Cette tâche est du ressort du Security Operation Center (SOC).

Une mission importante des analystes du SOC consiste à différencier les événements pertinents des événements qui ne le sont pas (encore appelés des « false positives ») et à traiter uniquement les événements pertinents (« true positives ») comme des incidents ou des incidents de sécurité. Ces analystes remplissent d'ores et déjà cette mission, notamment grâce à des outils basés sur des règles. Toutefois, la qualité de ces outils dépend entièrement des règles définies au préalable. Leur point faible est qu'ils sont incapables de réagir rapidement aux changements et aux incidents imprévisibles et inhabituels. Face au volume croissant des données et aux attaques plus intelligentes, les outils basés sur des règles ne suffisent plus à protéger les entreprises et leurs clients contre les pirates.

Des systèmes intelligents dotés de capacités d'auto-apprentissage constituent la clé de voûte pour développer la capacité d'empêcher de telles attaques ou, tout du moins, de les identifier précocement et de les repousser. Qui plus est, ces systèmes

ne peuvent pas se limiter à détecter les menaces de manière indépendante, ils doivent aussi savoir rechercher activement les faiblesses dans une configuration système et proposer des mesures correctives ou les mettre en œuvre directement.

3.2.2 Phisherman

Chez Swisscom, nous misons déjà sur l'apprentissage automatique pour lutter contre les menaces en matière de sécurité. L'hameçonnage représente une menace qui plane quotidiennement sur nos activités et nos clients. Dans le cas du phishing, les criminels tentent d'accéder aux données de l'utilisateur, telles que mots de passe et renseignements sur les cartes de crédit, par le biais de faux e-mails, par exemple.
La pierre angulaire en matière de prévention contre le phishing consiste à identifier correctement et rapidement les e-mails frauduleux et à les différencier des vrais e-mails. Les attaques de phishing sont de plus en plus ciblées et professionnelles, si bien que même les utilisateurs précautionneux et compétents sur le plan technique ne sont pas toujours en mesure de les reconnaître comme telles.
L'apprentissage automatique offre alors une véritable valeur ajoutée. Phisherman, notre application de prévention des attaques par hameçonnage, utilise des techniques avancées d'apprentissage automatique pour identifier et qualifier les tentatives de phishing.

L'illustration suivante est un extrait à jour de Phisherman, associé à une comparaison des tendances de 2016 et 2017.
La légende « Top phished companies » signifie que des assaillants ont tenté de se faire passer pour l'entreprise citée auprès d'autres personnes. Le plus souvent, cette tentative prend la forme de faux e-mails. Il ressort clairement que les entreprises américaines et leurs clients étaient les premiers concernés en 2016, alors que de plus en plus d'entreprises suisses ont été touchées en 2017. Même si la « première place» reste attribuée à Apple et que Swisscom occupe le cinquième rang durant ces deux années, UBS et Postfinance ont été particulièrement affectées en 2017.

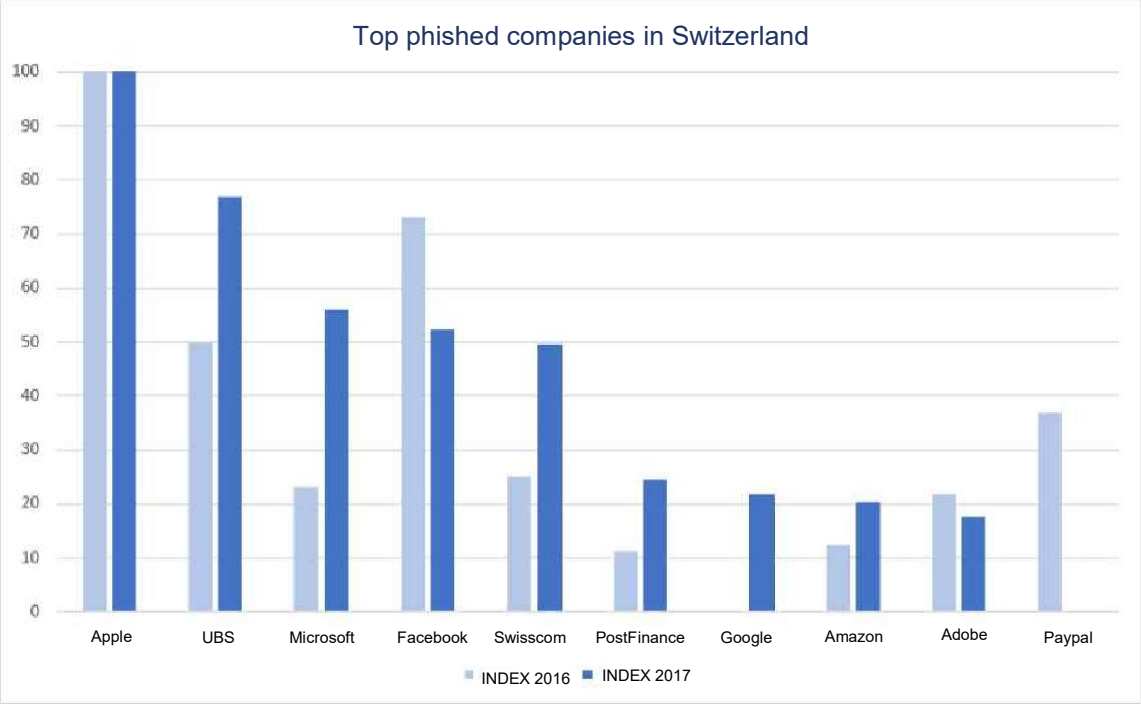

Illustration 3 : Top phished companies en Suisse, évaluation 2016/17 par Swisscom Phisherman

Il est possible de déduire de cette évolution que les attaques de phishing sont devenues plus ciblées, plus intelligentes et, également, plus régionales. Plus les pirates sont proches de l'environnement réel des personnes concernées, plus il leur est facile de les tromper et d'en tirer profit.

3.3 Conclusion

L'adoption d'applications AI va devenir un facteur déterminant dans le domaine de la cybersécurité à court et moyen termes. D'ailleurs, comme indiqué, les volumes de données en croissance constante ne peuvent plus raisonnablement être évalués par les systèmes de support actuels dont disposent les analystes dans le domaine de la sécurité. De plus, les attaques sont de plus en plus intelligentes et ciblées. Même si les applications AI sont nécessaires pour faire la distinction entre les événements critiques et les autres, ces systèmes doivent pour le moment être uniquement utilisés en soutien. La responsabilité de la prise de décision doit rester du ressort des spécialistes aussi longtemps que l'AI n'aura pas fait ses preuves dans la pratique quotidienne sur une période plus longue.

4. Menaces sur le réseau Swisscom

Avec plusieurs millions d'accès Internet et en tant que fournisseur d'infrastructures d'informatique et de télécommunication destinées aux grandes entreprises, Swisscom est confrontée quotidiennement aux menaces les plus variées sur une très grande échelle. Ces menaces visent soit directement les clients, soit les infrastructures propres à Swisscom.

Pour pouvoir dresser l'état des lieux de ces menaces, nous avons évalué sur une période de six mois les données extraites de DNS sinkholes (cf. glossaire) et les données du passive DNS. L'analyse d'identification a principalement permis d'étudier les accès DNS pour attribuer des menaces au sein du réseau Swisscom à ce segment de clientèle. La pertinence de cette méthode d'analyse est limitée, car l'identification dépend du fait que le domaine est connu ou pas et qu'il a été enregistré dans les données du sinkhole.

Les conclusions présentées ici ne constituent qu'une vue d'ensemble des principaux résultats obtenus :

L'évaluation des menaces identifiées montre une nette prédominance du trafic Malware Call-Home (Command and Control), alors que les attaques par amplification DNS et les logiciels publicitaires ont toujours une incidence plus faible. L'autre prédominance qui se dessine concerne la communication avec des infrastructures de crypto-mining.

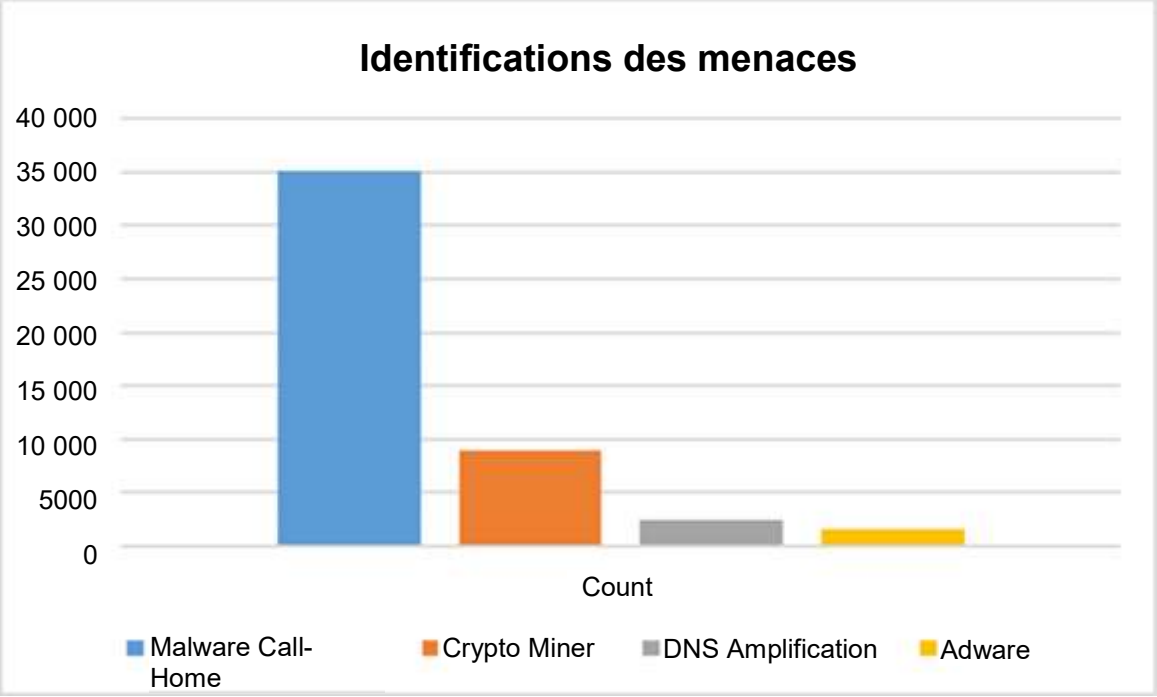

Illustration 4 : identifications des menaces

4.1 Malware Call-Home

Nous désignons le trafic de réseau CnC (Command and Control) typique sous l'appellation Malware Call-Home. « Command and Control » fait référence à la communication d'un système infecté (p. ex. un bot) avec le système sous le contrôle d'un assaillant. Pour conserver le contrôle sur le système infecté et exécuter des actions telles que des attaques DDoS, l'envoi de spams ou l'infection d'autres systèmes, l'assaillant a besoin de ce canal. Les virus Conficker, Ramnit et Gamut sont en particulier présents sur le réseau destiné aux utilisateurs de Swisscom. Comme aucun composant Command and Control n'est en général utilisé dans les attaques par ransomware, l'identification des rançongiciels au moyen de requêtes DNS s'avère extrêmement difficile. Le rançongiciel WannaCry constitue une exception, car il peut être identifié via le domaine Kill-Switch.

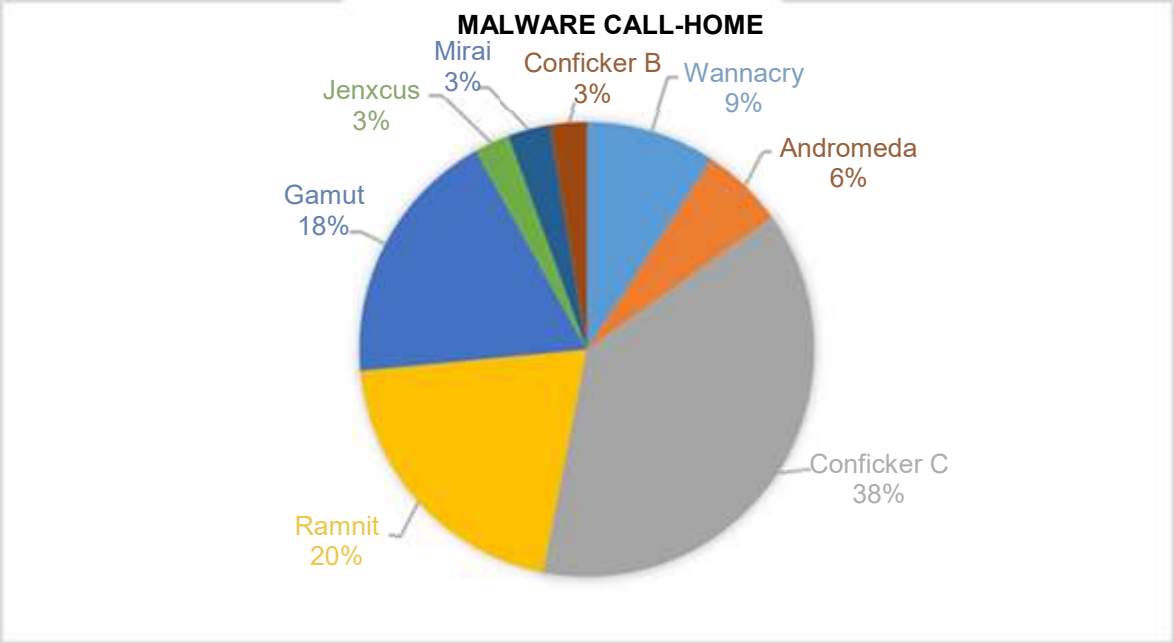

Illustration 5 : Malware Call-Home

Ces résultats représentent les accès détectés à des infrastructures déjà bloquées par des sinkholes DNS (ou « gouffres » DNS).

Conficker, également connu sous le nom Downadup, est apparu dès 2008 dans différentes variantes et a infecté des millions de systèmes Windows. Ce malware exploitait une faiblesse au niveau du Server Service de Microsoft Windows et utilisait un type d'attaque par dictionnaire dans ses versions B et C ainsi qu'une exécution abusive de Windows Autorun pour s'autopropager. La version C est la famille de logiciels malveillants la plus répandue en Suisse. Un groupe de travail (Conficker Working Group) a été expressément constitué pour stopper Conficker. Ce groupe de travail a été en mesure d'arrêter la propagation de Conficker. Les pirates qui se dissimulaient derrière Conficker restent encore inconnus à ce jour.

Ramnit est un « malware toolkit » de conception modulaire, qui bénéficie d'une immense popularité auprès des cyber-criminels depuis 2010. Ce logiciel malveillant est en mesure d'espionner le comportement de navigation sur le web des systèmes victimes, puis de lire et récupérer les données d'accès saisies, par exemple. Ce toolkit déploie plusieurs méthodes pour rester de manière permanente sur un système infecté. Il infecte entre autres les fichiers .exe, .dll, .htm et .html. Il se duplique sur tous les disques durs connectés (même les appareils connectés via USB sont infectés). Les infections Ramnit continuent à être très répandues en Suisse.

Gamut est un spam botnet (robot d'envoi de spams), qui infecte les systèmes Windows dans le but d'envoyer des spams. Selon une analyse récente, Gamut et le réseau de bots Necurs sont responsables de 97% de tous les spams envoyés au cours du dernier trimestre 2017.

4.1.1 WannaCry

Même si les répercussions de WannaCry sur notre réseau sont moins importantes, nous désirons tout de même en parler du fait des caractéristiques particulières de ce rançongiciel. Les ransomwares identifiés à ce jour se caractérisaient par le fait qu'ils accédaient aux systèmes qu'ils ciblaient au moyen de spams, de sites Internet infectés ou de réseaux bots, puis y demeurait pour dérober de l'argent à ses victimes. Ce ransomware jouit en particulier d'une grande popularité auprès des cyber-criminels. Les principales raisons que nous envisageons sont détaillées dans le tableau suivant.

Low Entry Barrier	Une professionnalisation croissante des rançongiciels sous forme d'offres de service, grâce à laquelle même les criminels sans connaissances en programmation ni savoir-faire technique ont désormais la possibilité de lancer des attaques par ransomware.
Transferts anonymes d'argent	Du fait de la multiplication des crypto-monnaies anonymes, comme Monero, les cyber-criminels peuvent agir dans le monde entier et extorquer de l'argent numérique à leurs victimes sur toute la planète, sans être identifiés ni traçables.
Impuissance des victimes	Les particuliers et les PME qui ne disposent d'aucune stratégie de sauvegarde pour leurs données envisagent le versement de l'argent extorqué comme la seule solution pour récupérer leurs données.

Avec WannaCry, l'infection automatisée par un ransomware a atteint une toute nouvelle dimension. La campagne WannaCry identifiée en mai 2017 s'est appuyée sur l'exploit ETERNALBLUE, précédemment connu et indûment extirpé de l'arsenal

de la NSA. En l'espace de quelques jours, plus de 230 000 systèmes dans plus de 150 pays ont été infectés automatiquement. Des infrastructures critiques, comme le service public de santé britannique ou la compagnie ferroviaire allemande Deutsche Bahn, ont été touchées[2].

Illustration 6 : infection par WannaCry

La Suisse a été et est encore concernée par la campagne WannaCry. Toutefois, ses infrastructures critiques n'ont pas été touchées contrairement à de nombreux autres pays. Sur le plan mondial, cette attaque montre parfaitement que l'exploitation d'une seule faille peut provoquer une pandémie via des mécanismes latéraux de propagation, que les frontières des réseaux, comme le périmètre et le réseau interne, peuvent se fondre, mettant en lumière la vulnérabilité de nos systèmes interconnectés et de notre ère numérique.

[2] https://www.heise.de/newsticker/meldung/Ransomware-WannaCry-befaellt-Rechner-der-Deutschen-Bahn-3713426.html

4.2 Crypto-mining

Même si les crypto-monnaies continuent de gagner en popularité dans le cadre des attaques par ransomware, une nouvelle tendance a fait son apparition parmi les menaces identifiées sur le réseau de Swisscom : l'extraction[3] des crypto-monnaies. En tant que menace identifiée, cette opération s'entend selon nous comme l'extraction (mining) non autorisée de crypto-monnaies par le biais de l'installation non autorisée d'extracteurs (miners), par exemple par ...

Insiders	La gratuité de l'extraction réalisée à l'aide des ressources (puissance de calcul) et aux frais de l'entreprise (électricité) rend le mining très attirant aux yeux des salariés des entreprises. Les collaborateurs disposant de droits particuliers (p. ex. administrateurs, power-users) peuvent en tirer profit[4].
Malware	Contrairement aux attaques par ransomware qui donnent lieu à un paiement unique, les extracteurs assurent des revenus réguliers et sont donc nettement plus lucratifs pour les cyber-criminels.
Drive-By Mining	Drive-By Mining s'exécute directement dans le navigateur par le biais des langages de script et utilise la puissance CPU des visiteurs du site Internet.

Une évaluation générale de nos données DNS passives montre quels pools sont exploités de manière active pour l'extraction des crypto-monnaies.

[3] Dans le cas du «mining» (en français, «extraction»), la puissance de calcul est utilisée pour confirmer les transactions en crypto-monnaies. Les mineurs sont motivés sur le plan financier.
[4] https://www.rferl.org/a/russia-sarov-nuclear-facility-workers-arrested-using-supercomputer-mine-bitcoin/29030004.html

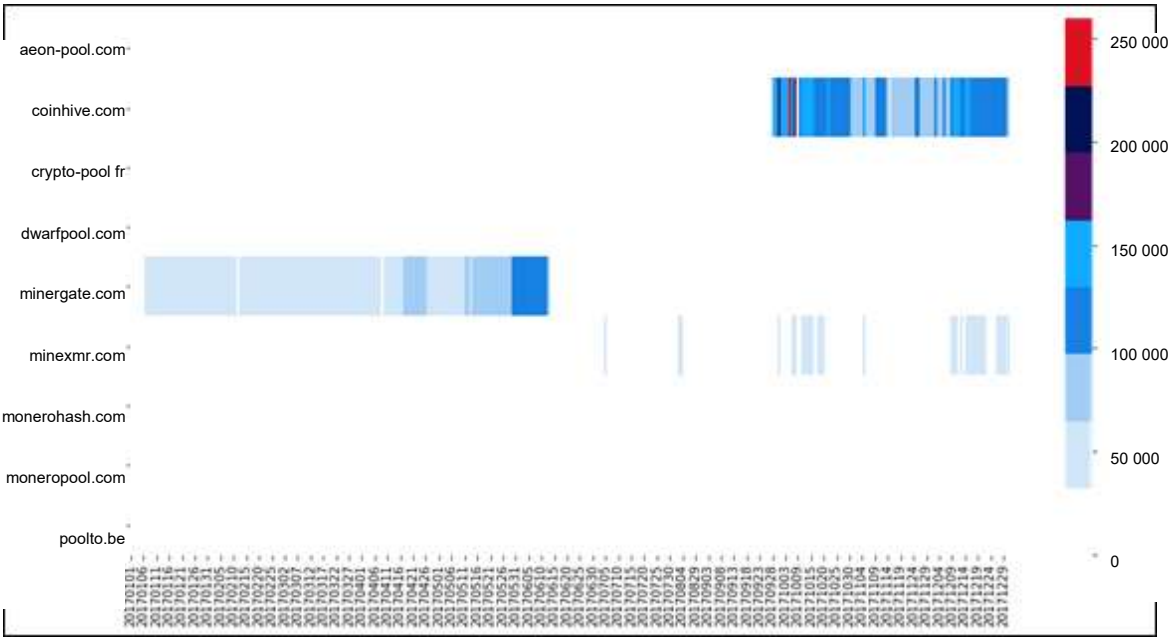

Illustration 7 : utilisation du pool d'extraction (Mining Pool)

Les entrées blanches se situent en dessous de 50 000 appels par jour. Il convient de mentionner tout particulièrement les pools minergate.com et coinhive.com. L'utilisation de ces pools ne laisse en général pas présager une intention malveillante. Pourtant, les cyber-criminels ont commencé depuis longtemps à équiper leurs logiciels malveillants avec un crypto-miner et accèdent ainsi à des pools d'extraction éprouvés dans le cadre de ce modèle lucratif à des fins de monétisation des ordinateurs infectés.

La prolifération d'installations d'extraction concerne aussi bien les stations clientes, les serveurs que les navigateurs.

4.2.1 Coinhive

Coinhive est très en vogue auprès des pirates souhaitant extraire des crypto-monnaies par Drive-By Mining. Comme Coinhive s'exécute directement dans le navigateur de la victime et utilise la puissance CPU des visiteurs du site Internet via un script Java pour extraire la cryto-monnaie Monero, il est facile à utiliser et ne coûte rien aux cyber-criminels en termes de frais d'exploitation. Pour obtenir les plus gros versements possibles, les cyber-criminels ciblent les sites Internet les plus fréquentés. Les sites Internet gouvernementaux sont ainsi devenus des cibles depuis longtemps déjà. Le script Java d'extraction Coinhive leur a été intégré et est utilisé abusivement pour des attaques Drive-By Mining[5].

[5] https://twitter.com/Scott_Helme/status/962684239975272450

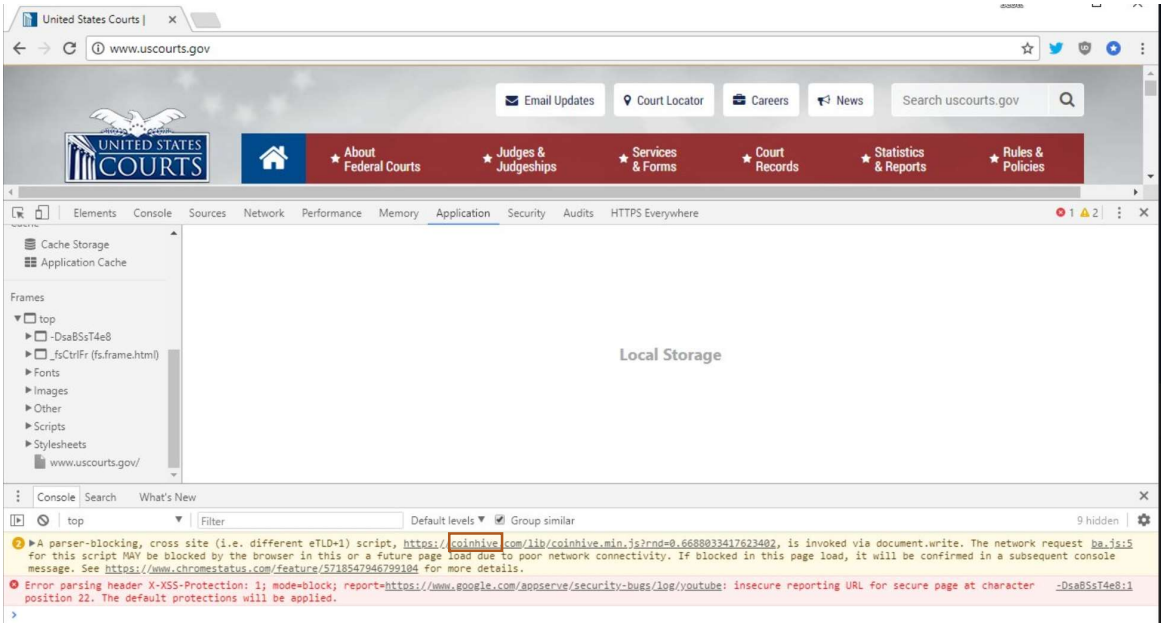

Illustration 8 : site Internet « United States Courts» infecté par le script Java Coinhive

Dans le cadre d'une analyse actuelle, nous avons utilisé le site web publicwww.com pour identifier les sites Internet qui chargent le script Java Coinhive.

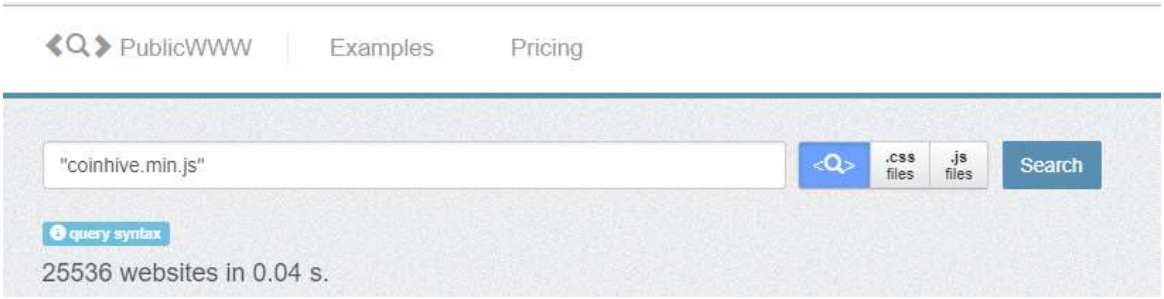

Illustration 9 : Coinhive sur publicwww.com

Au total, plus de 25 500 sites Internet qui exécutent des recherches de sites web via des opérations Coinhive Drive-By-Mining sur les terminaux ont été identifiés. Nombre de ces sites Internet ont été identifiés comme compromis[6].

4.3 Conclusion

Au travers des infections Conficker, Gamut, Ramnit et WannaCry, diverses familles de logiciels malveillants sont présentes à des fins différentes chez les clients au sein du réseau Swisscom. Les infections par Conficker nous révèlent que parmi les systèmes infectés, de nombreux utilisent encore des systèmes d'exploitation Legacy, qui restent vulnérables face aux faiblesses exploitées par Conficker. Les infections

[6] https://badpackets.net/cryptojacking-malware-coinhive-found-on-30000-websites/

par Gamut et Ramnit montrent que des cyber-criminels ont pris le contrôle d'un grand nombre de systèmes appartenant à des clients suisses et qu'ils les utilisent abusivement à leur propre avantage. Même si la Suisse a été moins touchée par WannaCry, nous devons nous attendre à ce que le risque d'un autre « contrôle extérieur » au moyen d'une cyber-arme avec des effets planétaires augmente en raison de la numérisation croissante (cf. le radar des menaces).

L'évaluation des pools d'extraction pour les crypto-monnaies a révélé un grand nombre d'accès possibles par Drive-By Crypto-mining. Le modèle lucratif et l'anonymat en vigueur avec les crypto-monnaies rendent cette nouvelle technologie très alléchante, en particulier pour les cyber-criminels. En plus de l'installation d'extracteurs par des personnes de l'intérieur (insiders) ou de virus Drive-By Mining comme Coinhive, même les entreprises pourraient se résoudre à utiliser leurs ressources disponibles pour exploiter l'extraction.

En tant que fournisseur de services Internet, Swisscom garantit un accès Internet sûr, sans heurt et sans barrière à ses clients et à la société. Tout en défendant un Internet ouvert en Suisse[7], nous sommes tenus de protéger nos clients et de ne pas compromettre l'ouverture du réseau.

Pour assurer une protection contre les logiciels malveillants, nous avons déjà mis en œuvre divers mécanismes établis, notamment :

Spam traps	Les spam traps sont des adresses e-mail ne correspondant à aucun utilisateur, qui ont été créées dans le but d'identifier les e-mails illégitimes tels que pourriels, hameçonnage ou attaques de malware. Swisscom exploite des milliers de comptes de messagerie de ce type, dont le contenu est analysé de manière automatique pour accroître la sécurité des filtres de protection.
Internet Guard	Internet Guard de Swisscom fonctionne sur la base de listes noires fournies par des opérateurs tiers ainsi que nos propres listes noires, qui sont transférées sur nos serveurs DNS, puis bloquées. En recourant à l'infrastructure DNS d'Internet Guard, les clients Swisscom sont protégés contre les sites Internet identifiés comme malveillants.
Annonces des clients	Les sites frauduleux (p.ex. hameçonnage ou tentative de fraude), les sites comportant un logiciel malveillant (virus, cheval de Troie, etc.) et les sites qui exploitent une faille de sécurité des

[7] https://www.asut.ch/asut/media/id/154/type/document/ai_code_de_conduite_avec_asut_201603.pdf

appareils peuvent être signalés directement par e-mail à l'adresse : spamreport@bluewin.ch.

Tout client déjà infecté par un malware est maintenu dans une Sandbox – un réseau isolé en quarantaine. Lorsqu'il tente de se connecter, ce client accède à une page d'information sur la mesure appliquée et la raison d'être de cette mesure, ainsi qu'à des informations d'assistance supplémentaires. Swisscom TV et la téléphonie ne sont pas concernés par ce blocage. Il reste possible d'établir des connexions ayant pour but d'aider le client à résoudre le problème, par exemple à l'aide de logiciels antivirus, de mises à jour logicielles, etc.

5. Glossaire

0-Day / Zero-Day Exploit	Exploit connu avant ou lors de la première divulgation d'une faille de sécurité. En d'autres termes, un exploit est disponible avant que l'éditeur du logiciel concerné ne dispose d'un patch de sécurité.
API	Application Programming Interface (interface de programmation d'applications). Interface permettant aux programmes d'échanger directement des données sur la base d'un langage commun (de machine à machine).
Backdoor	Porte dérobée permettant d'accéder à un ordinateur en contournant la protection d'accès.
Botnet	Réseau avec un grand nombre d'ordinateurs compromis, dont le contrôle central est assuré par un botmaster.
Defacement	Introduction de contenus indésirables sur un site Internet piraté.
DoS, DDoS	Denial of Service (DoS). Un système est paralysé par un grand nombre de requêtes. Distributed Denial of Service (DDoS). L'attaque DoS (attaque par déni de service) est lancée simultanément à partir d'un grand nombre de systèmes répartis (p. ex. un botnet). Il n'est plus possible de bloquer l'agresseur.
DNS Sinkhole	Ces « gouffres DNS » sont principalement utilisés pour diriger vers une autre adresse IP un domaine identifié comme malveillant via DNS.
Exploit	Programme, code ou séquences d'instructions permettant d'exploiter les failles d'un logiciel.
Exploit Mitigation	Terme générique désignant les techniques utilisées pour empêcher ou rendre plus difficile l'exploitation des failles des systèmes.
ICS	Industry Control System. Désignation générale des systèmes de contrôle industriel, voir SCADA.
TIC	Abréviation correspondant aux technologies de l'information et de la communication, pour le secteur de l'informatique et des télécommunications.
Jamming	Brouillage intentionnel de la radiocommunication.
Kill switch	Logiciel caché, qui peut également réagir à un ordre provenant de l'extérieur et qui perturbe le fonctionnement d'un système ou le rend inutilisable.
Malware	Logiciel malveillant qui exécute des fonctions dommageables et non souhaitées.
Money Mule	Des criminels incitent des personnes à percevoir de l'argent de « clients » et à le transférer, par le biais d'un service de transfert, après déduction d'une commission. La personne

	(money mule) croit travailler pour une organisation légitime.
Monero	La crypto-monnaie Monero présente des avantages particuliers pour les cyber-criminels, notamment la non-traçabilité des transactions et l'algorithme CryptoNight, qui donne la préférence aux CPU et GPU des ordinateurs et des serveurs. Pour ce dernier, Monero se distingue largement de Bitcoin en ce qui concerne l'extraction, pour laquelle des matériels spéciaux et chers s'avèrent maintenant nécessaires.
OSINT	Open Source Intelligence. Collecte d'informations en utilisant exclusivement des sources accessibles au public.
Patch Mise à jour de sécurité	Remplacement du code programme d'un logiciel défaillant afin d'éliminer des failles de sécurité.
Phishing	Avec le phishing, les utilisateurs sont incités à divulguer des données sensibles par des astuces (le plus souvent par des e-mails contenant des messages trompeurs).
SCADA	Supervisory Control And Data Acquisition System. Systèmes de surveillance et de contrôle de processus techniques (p. ex processus industriels).
Faiblesse	Faille ou vulnérabilité matérielle ou logicielle, par laquelle les pirates peuvent avoir accès à un système.
SDR	Software Defined Radio. Emetteurs et récepteurs haute fréquence universels qui assurent le traitement des signaux par logiciel et qui sont par conséquent adaptables par l'utilisateur à différents protocoles et applications.
SmartGrid	Réseau électrique intelligent. SmartGrid comprend l'interconnexion et la gestion des producteurs d'électricité, des systèmes de stockage, des consommateurs d'électricité ainsi que des réseaux de transmission et de distribution d'énergie.
SmartHome	Habitat intelligent. Terme générique désignant la gestion en réseau et partiellement automatisée de l'énergie, de la maintenance et de la sécurité dans les appartements et les maisons.
Social Media	Sites Internet sur lesquels les utilisateurs échangent des informations par le biais de profils établis par leurs soins (p. ex. Facebook, Twitter, LinkedIn, Xing).
Spearphishing	Attaque par hameçonnage ciblée et personnalisée, p. ex. pour obtenir les données d'accès de personnes-clés.
Spoofing	Tentatives de tromperie dans les réseaux en vue de masquer son identité.