Lettre n°49-Avril 2016-disponible sur omc.ceis.eu

Brève du mois

«From our standpoint, this is not a good thing.» *James R. Clapper, directeur de la NSA, au sujet du renforcement et de l'utilisation généralisée du chiffrement suite aux révélations Snowden*[1].

Table des matières

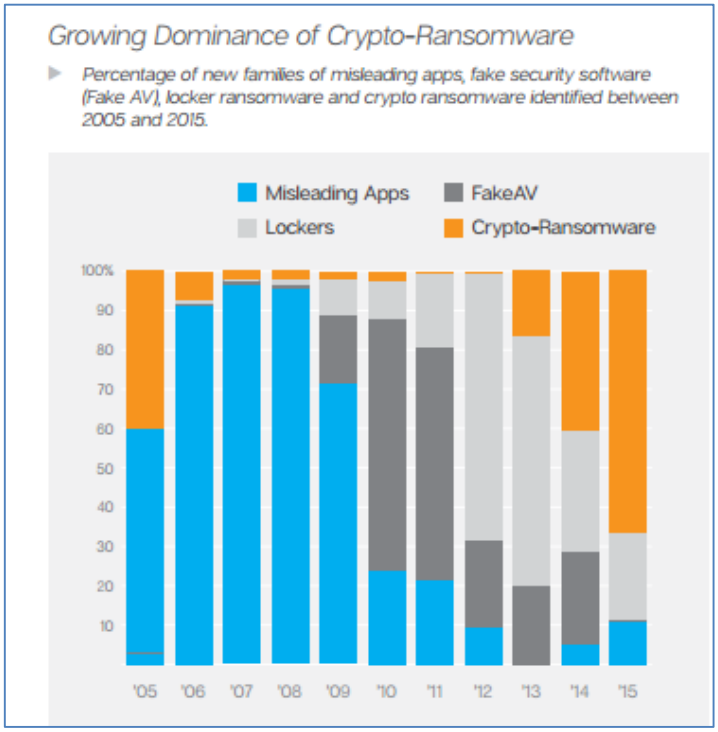
[1] http://www.csmonitor.com/USA/Politics/monitor_breakfast/2016/0425/New-encryption-technology-is-aiding-terrorists-intelligence-director-says

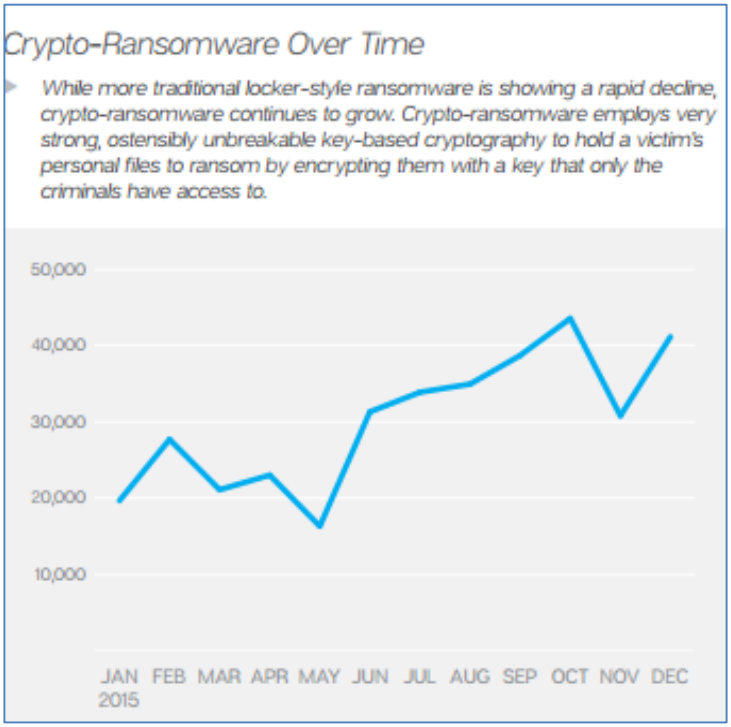
LES *RANSOMWARES* S'ATTAQUENT AUX SERVICES VITAUX

La multiplication des attaques par *ransomwares* contre des hôpitaux depuis le début de l'année 2016 montre que les cybercriminels n'hésitent désormais plus à s'attaquer aux services vitaux.

Une menace de plus en plus redoutable

Les attaques par *ransomwares* sont en nette progression depuis 2015. Selon le rapport *Internet Security Threat Report* publié par Symantec en avril 2016[2], le nombre de ces attaques aurait ainsi augmenté de 35% dans le monde et aurait plus que doublé en France. Même si l'on trouve trace de *ransomwares* dès 2005[3], l'autre nouveauté est depuis deux ans l'usage généralisé de «*crypto ransomwares* » qui chiffrent les fichiers présents sur un ordinateur afin de priver l'utilisateur de leur usage jusqu'au paiement de la rançon demandée. Cette technique, particulièrement incitative, est aujourd'hui utilisée par 60% des *ransomwares*[4].





Source : Security Threat Report 2016 de Symantec

Une menace de plus en plus redoutable

Les services publics deviennent progressivement une cible privilégiée de ces attaques. Quelques exemples récents :

[2]https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

[3]https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/

[4]https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

- Attaques contre des postes de police, notamment aux Etats-Unis (*ransomware* contre le poste de police de Durham en 2014, 5 petits départements policiers attaqués en 2015 dans le Maine, le Massachusetts et le Tennessee[5]) ;
- Attaques contre des collectivités locales et ministères, notamment en France et aux Etats-Unis. D'après un rapport du *Multi-State Information Sharing and Analysis Center*, organisme américain recensant les problèmes de cybersécurité liés au secteur public, 35 Etats ou collectivités américains ont subi une attaque par *ransomware* en 2014[6]. En France, on a observé une attaque début 2016 contre la direction générale de l'aviation civile[7] ;
- Attaques contre des écoles aux Etats-Unis. Principales cibles : les écoles élémentaires Swedesboro-Woolwich du district de New Jersey en mars 2015[8], l'école du district d'HorryCounty en Caroline du sud en mars 2016 (avec pour conséquence la paralysie de 60% des ordinateurs[9]), l'école d'Oxford dans le Mississippi en février 2016[10] ;
- Attaques contre les hôpitaux. Quelques 1 300 attaques informatiques contre des établissements de santé ont été signalées en 2015 en France selon le Fonctionnaire à la sécurité des systèmes d'information (FSSI) du ministère des affaires sociales[11]. Un hôpital de Boulogne sur Mer a ainsi récemment été la cible d'un *ransomware* et n'a dû son salut qu'à l'existence d'une sauvegarde récente des données[12].

Si l'on en croit le rapport de McAfee Labs *Prévisions 2016 en matière de menaces*[13], les campagnes de *ransomwares* devraient même s'intensifier dans les prochains mois et se *« tourner vers certains acteurs industriels, dont la finance et* ***les administrations publiques*** *»*. A noter que cette prévision est partagée par une étude du *Center for Internet Security*, pour qui les attaques par *ransomwares* devraient s'accroître considérablement en 2016[14].

Des infrastructures vulnérables

Des infrastructures sensibles comme les hôpitaux ne sont pas ciblées par hasard. Ils constituent tout d'abord une cible très attractive du fait du manque de sécurité de leurs infrastructures informatiques. Le rapport *The Current State of Healthcare Endpoint Security"*[15]du groupe de cybersécurité Duo Security met notamment en exergue le caractère vétuste des logiciels utilisés ainsi que le manque de formation du personnel aux problématiques de cybersécurité, ce qui rend les hôpitaux particulièrement vulnérables.

---

[5]http://www.governing.com/columns/tech-talk/gov-ransomware-police-cybsersecurity.html

[6]*Ibid.*

[7]http://www.industrie-techno.com/un-rancongiciel-contamine-la-messagerie-de-la-direction-generale-de-l-aviation-civile.42057

[8]http://www.networkworld.com/article/2901527/microsoft-subnet/crypto-ransomware-attack-hit-new-jersey-school-district-locked-up-entire-network.html

[9]http://money.cnn.com/2016/04/04/technology/ransomware-cybercrime/

[10]http://www.localmemphis.com/news/local-news/oxford-school-computers-hacked-with-ransomware

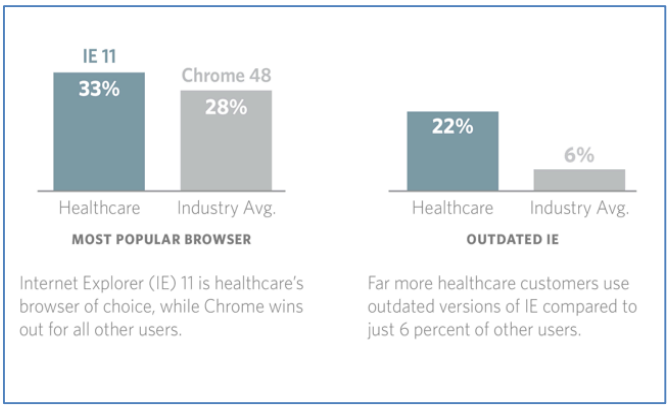
[11]http://www.ticsante.com/Plus-de-1300-attaques-informatiques-contre-des-etablissements-de-sante-signalees-en-2015-%28ministere%29-NS_2945.html

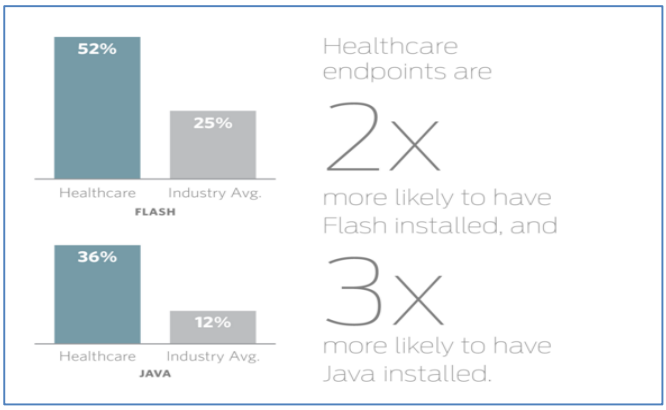
[12]http://www.lemagit.fr/actualites/4500279795/Rancongiciel-des-hopitaux-sauves-par-leurs-sauvegardes

[13]http://www.mcafee.com/fr/resources/reports/rp-threats-predictions-2016.pdf

[14]http://www.icomm.co.uk/it-support/it-support-news/Ransomware-security-threats-to-public-sector-will.aspx

[15]https://duo.com/blog/the-current-state-of-healthcare-endpoint-security





Source : The Current State of Healthcare Endpoint Security de Duo Security

Une autre étude réalisée par *l'Independent Security Evaluation*[16] émet un constat similaire. Les dispositifs de sécurité des hôpitaux ne seraient en réalité efficaces que contre des attaques non ciblées et peu sophistiquées. Il s'agirait en fait surtout de se protéger contre des intrusions informatiques traditionnelles. Le rapport dénonce ainsi le fait que la priorité soit donnée à la protection de la confidentialité des dossiers médicaux au détriment de leur sécurité.

Autre caractéristique majeure partagée par les services hospitaliers, et plus généralement par les services publics : l'urgence de trouver une solution pour faire face aux conséquences de l'attaque. En mars dernier, le MedStarHealth a dû revenir au « papier » lorsque cela était possible et suspendre certains services avec pour conséquences des rendez-vous non pris, des examens non réalisés et des opérations retardées[17]. Dans ce cas, céder au chantage et payer est forcément tentant, d'autant que les cybercriminels offrent des réductions lorsque le paiement intervient rapidement et se montrent souvent raisonnables dans leurs demandes, préférant réaliser de nombreuses « petites » opérations plutôt que de tenter le casse du siècle. Qu'il y ait ou non paiement de la rançon, les conséquences financières de l'attaque restent de toutes façons très lourdes pour la victime puisqu'il faut remettre en état le réseau et renforcer sa sécurité[18].

Les *ransomwares* les plus en vogue

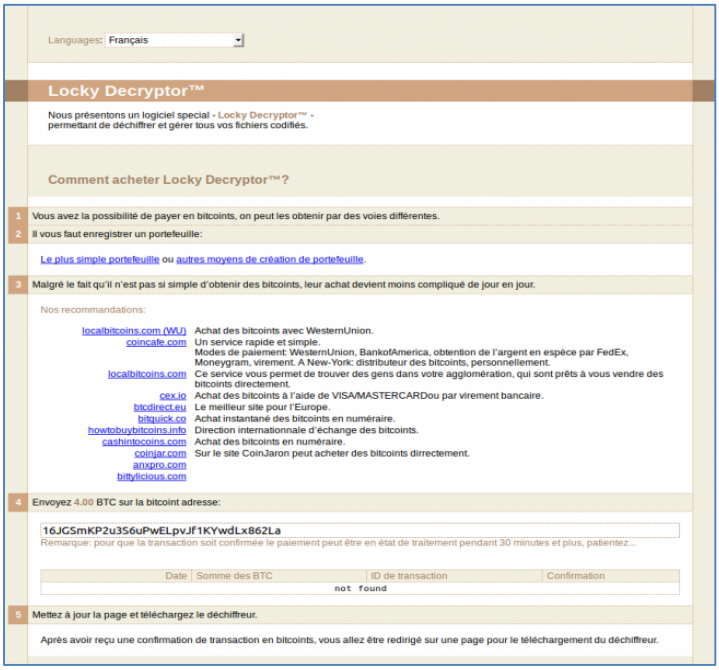
Les attaques visant les acteurs publics se caractérisent notamment par l'emploi de nouveaux *ransomwares* aux effets particulièrement dévastateurs. Exemple : Locky, en plein essor depuis début 2016. Ce *malware* permet notamment de chiffrer les données présentes dans un serveur (et non seulement d'un unique ordinateur) et même de supprimer les sauvegardes internes (*shadow copies*) effectuées par Windows. La contamination d'un réseau par Locky se fait par l'ouverture, depuis un utilisateur, d'un email contenant une pièce-jointe infestée[19], ce qui correspond au vecteur traditionnel d'infection par *ransomware*.

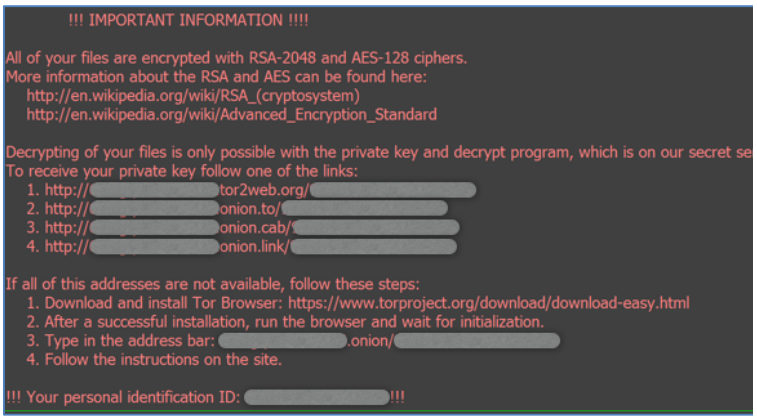
[16]https://securityevaluators.com/hospitalhack/securing_hospitals.pdf

[17]http://www.baltimoresun.com/health/bs-md-medstar-hack-recovery-20160331-story.html

[18]http://www.tripwire.com/state-of-security/regulatory-compliance/hipaa/how-hospitals-are-at-risk-of-ransomware-attacks/

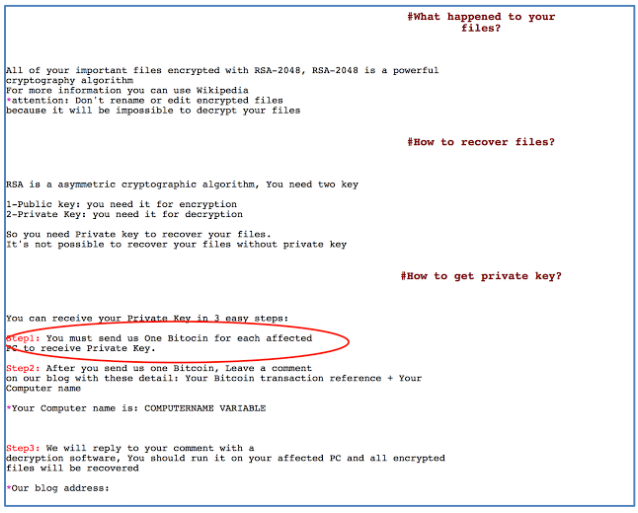
[19]https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/26000/PD26383/en_US/McAfee_Labs_Threat_Advisory-Ransomware-Locky.pdf

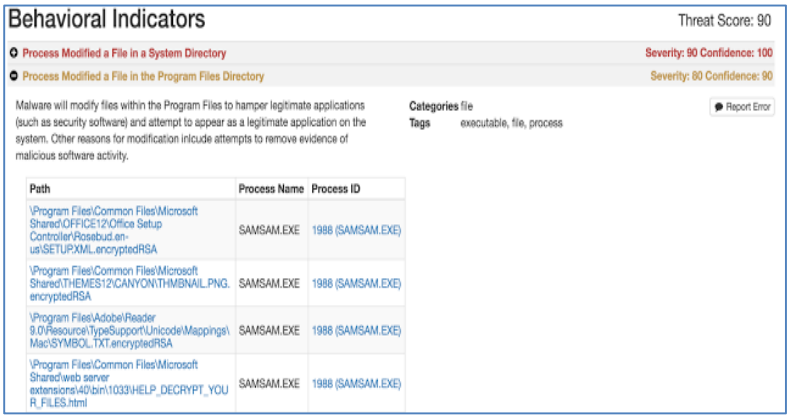




Source : McAfee Labs[20]

Un autre *ransomware* touchant actuellement les administrations publiques est SamSam, qui affecte quasi-exclusivement les hôpitaux à ce jour. L'une de ses caractéristiques majeures est de s'étendre à l'ensemble du SI auquel la machine infectée est reliée et ce, sans nécessiter que les machines concernées soient connectées à Internet[21]. La spécificité de ce *ransomware* réside donc dans le fait qu'il s'attaque directement à des vulnérabilités de serveurs web (présentes au sein de serveurs JBoss) plutôt que d'employer le vecteur utilisateur (infection par pièce jointe présente dans un email)[22] comme le fait Locky.





Source : Talos[23]

[20] https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/26000/PD26383/en_US/McAfee_Labs_Threat_Advisory-Ransomware-Locky.pdf

[21] http://www.healthcareitnews.com/news/two-new-ransomware-strains-discovered-can-spread-even-when-offline

[22] http://blog.talosintel.com/2016/03/samsam-ransomware.html

[23] http://blog.talosintel.com/2016/03/samsam-ransomware.html

Quelles solutions ?

Malgré la menace majeure que représentent ces *ransomwares*, il est possible de s'en prémunir ou, en cas d'infection avérée, de rétablir rapidement la situation en adoptant certaines bonnes pratiques.

Il est tout d'abord impératif de disposer d'un système de sauvegarde efficace reposant sur deux types de sauvegardes :

- des sauvegardes en temps réel pour éviter toute perte de données (dans le cas où l'établissement ne peut pas se permettre de perdre les données d'une seule journée) ;
- des sauvegardes journalières sur des cassettes magnétiques qui doivent être décorrélées du SI.

Une bonne gestion des droits est en outre nécessaire afin d'éviter que les supports de sauvegarde soient eux-mêmes atteints par le *ransomware*.

Certaines structures infectées ont ainsi pu se remettre d'attaques par *ransomwares* grâce à ces types de sauvegarde. L'hôpital méthodiste d'Henderson dans le Kentucky a par exemple pu recouvrer le contrôle intégral de son système 5 jours après l'attaque et ce, sans payer de rançon[24], tout comme le MedStarHealth qui a lui aussi refusé de payer une rançon de 19 000 dollars et a recouvré 90% des fonctionnalités de son système d'information 4 jours après le début de l'infection par le *ransomware*[25].

La formation du personnel est également prépondérante, notamment pour faire face à des *ransomwares* privilégiant le vecteur utilisateur comme Locky. Ce dernier se présentant souvent sous la forme d'un mail accompagné d'une fausse facture destiné au service comptabilité, une sensibilisation du personnel est essentielle pour limiter l'erreur humaine.

De façon plus globale, une amélioration du niveau de sécurité des réseaux et systèmes d'information des organisations publiques est absolument essentielle pour s'adapter à ces nouvelles menaces. Une amélioration qui passe notamment par le déploiement de solutions de sécurité reposant non seulement sur la détection de signatures, mais également sur des modules heuristiques (grâce à une analyse du trafic réseau).

[24] http://www.lemagit.fr/actualites/4500279795/Rancongiciel-des-hopitaux-sauves-par-leurs-sauvegardes

[25] http://www.nbcnews.com/news/us-news/medstar-hospitals-recovering-after-ransomware-hack-n548121

ISRAEL : L'INFLUENCE DU SYSTEME MILITAIRE SUR L'INDUSTRIE CYBER

L'Armée de défense d'Israël, plus connue sous le nom de Tsahal, a été créée le 16 mai 1948. Avec un budget de plus de 60 milliards de shekel (environ 14 milliards d'euros) alloués à la défense en 2016[26], Israël est le 16ème pays en valeur absolue mais il est le cinquième pays en termes de dépenses militaires par rapport au budget national (6,4% en Israël contre 4,4% aux USA, pays qui a le plus fort budget alloué à la défense). Ce chiffre est significatif de la place du monde militaire dans le fonctionnement de la société israélienne. Si la part exacte de ce budget allouée aux unités cyber n'est pas connue, les officiers spécialisés réclamaient, en 2015, au moins 8% de ce budget pour leurs unités[27]. C'est également en 2015 que Tsahal a décidé de se réorganiser et de créer un corps d'armée entièrement consacré à la lutte cybernétique[28] qui aura le même statut que les armées de Terre, de l'Air et de la Marine.

Au-delà des capacités de Tsahal, il est intéressant d'analyser le fonctionnement du lien armée-Nation dans le domaine « cyber » et d'évaluer les conséquences que celui-ci peut avoir sur l'industrie numérique israélienne, notamment dans le domaine de la cybersécurité.

Les conséquences du service militaire obligatoire

D'une durée de 36 mois, le service militaire en Israël est obligatoire après le lycée pour tous les citoyens ayant atteint l'âge de la majorité civile et déclarés aptes. Ce système a de nombreuses conséquences sur l'industrie numérique israélienne.

L'armée pourra tout d'abord tester chaque élève durant 3 ans en vue d'un éventuel recrutement, ce qui est particulièrement intéressant pour les unités cyber qui demandent plus de savoir-faire académiques que les unités combattantes. Ce repérage de talents démarre en réalité encore plus tôt. L'Unité 8200, également appelée Israeli SIGINT National Unit (ISNU), qui est l'unité de renseignement responsable du renseignement d'origine électromagnétique et du décryptage de codes de l'armée israélienne, a en effet mis en place un système qui permet de détecter les élèves les plus brillants au sein des lycées dès l'âge de 15 ans[29]. Une fois repérés, ces élèves se voient alors proposer des cours du soir dans le but de perfectionner leur niveau dans les matières scientifiques, technologiques et informatiques dans leurs propres lycées. Une deuxième sélection est alors effectuée pendant ces cours de soutien afin d'envoyer les meilleurs de ces élèves à l'université. Lors de leur arrivée au service militaire, ils sont donc déjà formés et compétents sur les questions numériques.

Dans le même objectif, Israël a également développé la possibilité pour les lycéens de suivre un cursus spécialisé en « cyber » (au même titre qu'une filière littéraire, scientifique ou encore technologique en France). Cette filière est disponible dans plus de 10 lycées du pays. Le but affirmé de ce dispositif est de former des jeunes personnes capables d'avoir des compétences de plus en plus avancées avant même le début de leur service militaire.

[26] http://fr.timesofisrael.com/le-budget-de-la-defense-pour-2016-seleve-a-60-milliards-de-shekels/

[27] http://www.jpost.com/Israel-News/New-Tech/Cyber-Chief-8-percent-of-ministry-budgets-should-go-to-cyber-security-395101

[28] http://www.i24news.tv/fr/actu/israel/diplomatie-defense/79932-150727-israel-exercice-militaire-d-urgence-dans-tout-le-pays

[29] http://benillouche.blogspot.fr/2013/10/lunite-secrete-8200-ou-le-nsa-israelien.html

Si le service militaire obligatoire provoque une porosité entre le monde militaire et le monde civil avant même le début du service militaire, des connexions apparaissent également pendant celui-ci : certains soldats ont l'opportunité d'obtenir un *Bachelor's Degree* en *Computer Sciences* au cours de leur service militaire dans une unité cyber. Ils obtiennent alors un diplôme du *College of Management AcademicStudies*, l'université la plus ancienne et la plus importante d'Israël, qui possède des liens étroits avec Tsahal. Cette université offre également la possibilité d'effectuer ce *Bachelor* avant de débuter son service militaire. La date de début du service est alors reportée. Il est intéressant de relever que dans le cas où l'entrée au service militaire est reportée dans le but d'obtenir ce diplôme, l'armée a la possibilité de financer elle-même les études de ces futurs soldats via des systèmes de bourse.

L'Unité 8200, un incubateur militaire

De nombreux soldats qui font partie de l'Unité 8200 ont ensuite tendance à prolonger leur service militaire de quelques années de façon à optimiser leur compétence et leur expérience[30]. C'est donc à leur sortie du monde militaire que ces formations pointues vont avoir un impact sur le monde civil et entrepreneurial.

Cet impact va être double. Au plan humain, il se traduit par un transfert de compétences humaines du monde militaire au monde civil. De nombreuses entreprises qui sont à la pointe au plan numérique ont ainsi été créées par des anciens de l'unité 8200 telles que Waze, CheckPoint, Forecast, Palo Alto Network ou encore NICES System (voir graphique ci-dessous)[31].

Les soldats qui sortent des unités spécialisées de l'armée expliquent que la création de leur start-up débute en réalité alors qu'ils sont encore dans l'unité 8200, au point qu'ils considèrent eux-mêmes cette unité comme un véritable « incubateur ».

Companies with founders who have been through the 8200		
Argus Cyber Security	Co-founders Ofer Ben-Noon, Oron Lavi and Yaron Galula	$4 million in funding
Adallom	Co-founders Assaf Rappaport, Ami Luttwak and Roy Reznik	$49.5 million in funding
Palo Alto Networks	Founder Nir Zuk	Company went public on July 20, 2012 ($260.4 million IPO)
NSO	Founder Shalev Hulio	Company acquired by Francisco Partners for $120 million on March 19, 2014
CyberArk	Founder Udi Mokady	Company went public on September 24, 2014 ($85.8 million IPO)
Imperva	Co-founder Shlomo Kramer	Company went public on November 9, 2011 ($90 million IPO)
Check Point Software Technologies	Co-founder Gil Shwed	Company went public on June 28, 1996 ($67 million IPO)
Hyperwise Security	Co-founders Aviv Gafni and Ben Omelchenko	Company acquired by Check Point Software Technologies (terms not disclosed)
FST Biometrics	Founder Major General Aharon Zeevi Farkash	$5 million in funding
Radware		Company went public on October 8, 1999
Other companies with 8200 alums		
BioCatch	Lev Kadyshevitch, Head of Research	$14 million in funding
CybeReason	Lior Div, CEO	$4.6 million in funding
Sequoia Capital	Gili Raanan, Partner	

Exemple d'entreprises cyber israéliennes qui ont un lien avec l'Unité 8200 –

[30] http://www.jewishjournal.com/israel/article/israeli_officers_learn_to_fight_cyber_war

[31] http://techcrunch.com/2015/03/20/from-the-8200-to-silicon-valley/

Source : https://next.ft.com/content/acab9d3a-c32a-11e5-808f-8231cd71622e

Ce transfert s'opère également au plan technologique. De nombreuses technologies qui sont aujourd'hui présentes dans le monde civil ont ainsi été initiées lors du service militaire des créateurs de l'entreprise comme par exemple l'application Waze[32].

Le soutien à l'industrie

Cette expertise cyber acquise tout au long du service et de la carrière militaire des militaires a donc un réel impact sur la création même de start-up et le développement des technologies. A cela s'ajoute enfin des initiatives communes aux mondes militaire et civil, comme le programme d'accélération créé par des anciens de l'Unité 8200 ou bien encore le centre CyberSpark.

Des anciens de l'Unité 8200 ont en effet mis en place un programme de 5 mois qui encadre les start-ups qui n'en sont encore qu'à un stade précoce de leur maturation via un programme nommé 8200 EISP[33]. Triés parmi plus de 200 candidats, les 20 entrepreneurs sélectionnés pour avoir accès au programme reçoivent des conseils de la part d'anciens soldats de l'Unité. Ce programme qui se déroule sur une courte période se termine par la présentation des technologies développées devant plusieurs centaines d'investisseurs potentiels.

Autre programme clé : le CyberSpark. Inauguré en 2014, ce parc industriel regroupe l'Université Ben Gourion ainsi que les complexes professionnels adjacents. Pour soutenir son développement, l'Etat a décidé de financer 20% de la masse salariale des entreprises qui s'y installeront et 30% de la masse salariale des sociétés étrangères qui y installeront leur centre de recherche et développement[34], preuve s'il en était besoin de l'implication de l'Etat Israélien dans le développement des capacités numériques du pays[35]. CyberSpark va également voir arriver de nombreuses bases de l'armée actuellement situées à Tel-Aviv, au point que 30 000 militaires devraient investir ce complexe. A noter, enfin, que Tsahal offre une prime aux militaires de carrière qui s'installeront dans le Néguev pour une durée d'au moins 5 ans[36].

[32] https://www.battery.com/powered/the-secretive-israeli-army-unit-that-recruits-like-harvard-and-churns-out-high-profile-startups/

[33] http://www.eisp.org.il/en/home

[34] http://www.lefigaro.fr/international/2016/01/25/01003-20160125ARTFIG00285-beersheba-la-future-cybercapitale-d-israel.php

[35] http://in.bgu.ac.il/en/cyber/Pages/Innovation-Arena.aspx

[36] http://www.lefigaro.fr/international/2016/01/25/01003-20160125ARTFIG00285-beersheba-la-future-cybercapitale-d-israel.php

La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique**, sous le numéro de marché 1502492543. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la Défense et des Anciens combattants
Direction Générale des Relations Internationales et de la Stratégie
14 rue Saint-Dominique - 75700 – Paris SP 07

CEIS
280 Boulevard Saint-Germain - 75007 - Paris
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com