Lettre n°52-Juillet 2016-disponible sur omc.ceis.eu

«We will use the power of sanctions, as we did against North Korea after its destructive attack against Sony Pictures. […] The President has made it clear that we will take action to protect our interests in cyberspace and we will do so at the time and place of our choosing» *Lisa O. Monaco, Assistante du Président pour la sécurité intérieure et le contreterrorisme, à ICCS 2016 .*

Table des matières

AFFAIRES SWIFT & HACKING TEAM : L'APT AU SERVICE DE LA CYBERCRIMINALITÉ ET DE L'HACKTIVISME

Les affaires SWIFT et Hacking Team ont fait la une de l'actualité liée à la cybersécurité en raison des dommages majeurs engendrés par ces attaques. En effet, dans le cadre de l'attaque SWIFT[1] qui a eu lieu en février 2016, près de 80 millions de dollars ont été dérobés à la banque du Bangladesh. Quant à l'entreprise Hacking Team, celle-ci s'est vue confrontée en juillet 2015 au vol et à la diffusion massive via son propre compte Twitter de près de 400 Go de données sensibles (e-mails, factures, enregistrements audio, codes sources de logiciels)[2]. Cette cyberattaque fut par la suite revendiquée en avril 2016 par un pirate isolé dénommé Phineas Phisher[3].

Bien qu'ayant visé des cibles différentes avec des motivations diamétralement opposées, ces deux cyberattaques peuvent néanmoins être analysées à l'aune d'une singularité commune, à savoir le recours à un modus operandi propre aux menaces APT (Advanced Persistent Threat).

L'APT, une menace au fonctionnement spécifique

D'après l'ouvrage de Cédric Pernet *« Sécurité et espionnage informatique : Connaissance de la menace APT (Advanced Persistent Threat) et du cyberespionnage »*, une offensive APT peut se définir comme étant *« une attaque informatique persistante ayant pour but une collecte d'informations sensibles d'une entreprise publique ou privée ciblée, par la compromission et le maintien de portes dérobées sur le système d'information »*[4]. Pour ce faire, l'APT repose sur un modus operandi aux caractéristiques spécifiques. Tout d'abord, ce genre de menace est généralement le fait d'un groupe ou d'un État disposant de larges ressources, de telles attaques nécessitant organisation et coordination. Enfin, ce type de menace possède une dimension temporelle non négligeable (« *persistent* ») dans la mesure où elle se déroule sur une durée conséquente (plusieurs semaines/mois voire plusieurs années). En effet, l'assaillant a besoin d'étudier en détail sa cible afin de pouvoir ultérieurement s'introduire et se maintenir furtivement dans son système d'information, et ceci pendant tout le temps nécessaire à la découverte et à l'extraction des informations ciblées. Le mode opératoire se décompose en cinq étapes distinctes :

1) **Phase de reconnaissance** : collecte des données relatives à la cible pouvant s'avérer utiles lors de l'attaque à venir.

2) **Compromission initiale** : attaque initiale envers le système d'information de la cible afin de compromettre une ou plusieurs machines.

---

[1] http://www.reuters.com/article/us-cyber-banking-swift-exclusive-idUSKCN0XM2DI

[2] http://www.numerama.com/magazine/33624-la-firme-d-espionnage-hacking-team-piratee-400-go-de-donnees-diffusees.html

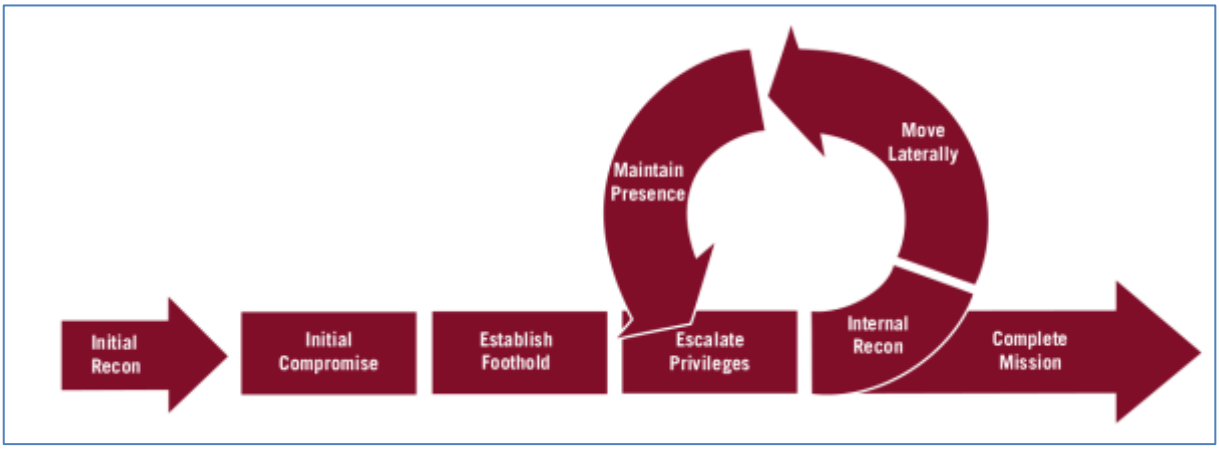
[3] http://pastebin.com/BFEpDVnZ

[4] Cédric Pernet : *« Sécurité et espionnage informatique : Connaissance de la menace APT (Advanced Persistent Threat) et du cyberespionnage », éditions Eyrolles.*

3) **Renforcement des accès** : mise en place de portes dérobées en différents points du réseau informatique de l'entreprise victime afin de disposer de plusieurs accès (dans l'hypothèse où l'un de ces accès serait découvert et désactivé par la cible ou un autre assaillant).

4) **Mouvements latéraux** : phase pendant laquelle l'attaquant parcourt le réseau de la cible et recherche les informations intéressantes à dérober.

5) **Exfiltration de données** : envoi des informations dérobées vers l'assaillant.



Déroulement type d'une offensive APT - Source : http://bl0g.cedricpernet.net/fr

Affaires SWIFT et Hacking Team : une méthodologie d'attaque indéniablement APT…

Ces deux affaires possèdent des caractéristiques propres aux menaces APT. L'une comme l'autre ont visé des cibles précises, à savoir l'entreprise Hacking Team, une société italienne commercialisant des logiciels d'espionnage et de surveillance[5] ; et le réseau SWIFT (Society For Worldwide Interbank Financial Telecommunication), un service de messagerie standardisé de transfert interbancaire utilisé par près de 10 800 institutions dans 205 pays[6]. La temporalité des attaques est également à relever, celle de Hacking Team ayant nécessité une centaine d'heures de travail et 6 semaines de présence sur les réseaux de l'entreprise selon son auteur[7]. Celle de SWIFT (dont la chronologie exacte demeure inconnue) s'est nécessairement étendue sur plus d'une semaine, les informations dérobées nécessitant des accès impossibles à obtenir rapidement (vol des identifiants et mots de passe des employés de la banque du Bangladesh permettant l'accès au réseau SWIFT)[8] ainsi que des moyens sophistiqués.

Qui plus est, les deux attaques ont scrupuleusement suivi la méthodologie détaillée auparavant. Dans le cas du piratage de la société Hacking Team, l'assaillant à l'origine de l'offensive (Phineas Phisher) a expliqué de

[5] http://surveillance.rsf.org/hacking-team/

[6] https://www.swift.com/node/16771

[7] https://motherboard.vice.com/read/the-vigilante-who-hacked-hacking-team-explains-how-he-did-it

[8] https://blog.cybelangel.com/le-systeme-bancaire-mondial-sous-tension-apres-une-serie-de-cyberattaques/?lang=fr)

manière exhaustive son modus operandi pour venir à bout de l'entreprise italienne dans une publication postée sur Pastebin en avril 2016[9]:

1) **Phase de reconnaissance** : Phineas explique qu'il a débuté son opération par l'analyse méthodique de l'environnement technique et social de l'entreprise : domaines et adresses IP, serveurs exposés, ports ouverts, organisation interne et employés ; ceci dans le but de développer une stratégie d'attaque efficace. Ses recherches furent peu fructueuses et il dut se résoudre à abandonner les méthodes classiques d'intrusion (à savoir les campagnes de spear-phishing et/ou l'achat d'accès internes sur le Dark Web) du fait de la spécialisation et de la structure de Hacking Team (employés rôdés aux emails piégés, structure de trop petite taille pour espérer acheter des accès clé-en-main sur le Dark Web)[10].

2) **Compromission initiale** : les méthodes classiques ayant échoué, l'assaillant s'est rabattu sur une méthode plus technique, la recherche d'une vulnérabilité zero-day, c'est-à-dire une faille n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif. Après deux semaines de rétro ingénierie, il a réussi à obtenir un *« accès à distance avec privilège administrateur ».*

3) **Renforcement des accès** : une fois présent sur le réseau de Hacking Team, Phineas Phisher a installé des logiciels lui permettant d'explorer le réseau de l'entreprise ainsi que d'installer une porte dérobée protégeant l'exploitation du zero-day.

4) **Mouvements latéraux** : l'attaquant a ensuite exploré le réseau afin de mettre la main sur des identifiants et mots de passe lui donnant accès aux ressources sensibles de la compagnie. Il parvint à trouver les identifiants des équipements de stockage dédiés à la sauvegarde dont l'accès était complètement ouvert. Après analyse des sauvegardes du serveur mail, Phineas Phisher a pu trouver le mot de passe de domaine d'un administrateur réseau de Hacking Team, ce qui lui donna un accès total au réseau de l'entreprise. Par la suite, il a pu espionner les administrateurs afin de trouver les informations recherchées, notamment les codes sources des produits d'espionnage de Hacking Team.

[9] http://pastebin.com/raw/0SNSvyjJ

[10] http://www.01net.com/actualites/hacking-team-comment-pirater-une-entreprise-en-6-etapes-968431.html

HACKINGTEAM	BESAdmin	bes32678!!!	
HACKINGTEAM	Administrator	uu8dd8ndd12!	
HACKINGTEAM	c.pozzi	P4ssword	<---- lol great sysadmin
HACKINGTEAM	m.romeo	ioLK/(90	
HACKINGTEAM	l.guerra	4luc@=.=	
HACKINGTEAM	d.martinez	W4tudul3sp	
HACKINGTEAM	g.russo	GCBr0s0705!	
HACKINGTEAM	a.scarafile	Cd4432996111	
HACKINGTEAM	r.viscardi	Ht2015!	
HACKINGTEAM	a.mino	A!e$$andra	
HACKINGTEAM	m.bettini	Ettore&Bella0314	
HACKINGTEAM	m.luppi	Blackou7	
HACKINGTEAM	s.gallucci	1S9i8m4o!	
HACKINGTEAM	d.milan	set!dob66	
HACKINGTEAM	w.furlan	Blu3.B3rry!	
HACKINGTEAM	d.romualdi	Rd13136f@#	
HACKINGTEAM	l.invernizzi	L0r3nz0123!	
HACKINGTEAM	e.ciceri	202571&2E	
HACKINGTEAM	e.rabe	erab@4HT!	

Source : 01net

5) **Exfiltration des données** : enfin, Phineas a pu voler les documents confidentiels de l'entreprise, pour ensuite les diffuser sur le propre compte Twitter de la société.

Source : motherboard

On trouve une méthodologie similaire dans le cas de l'attaque SWIFT, dont les assaillants restent encore inconnus :

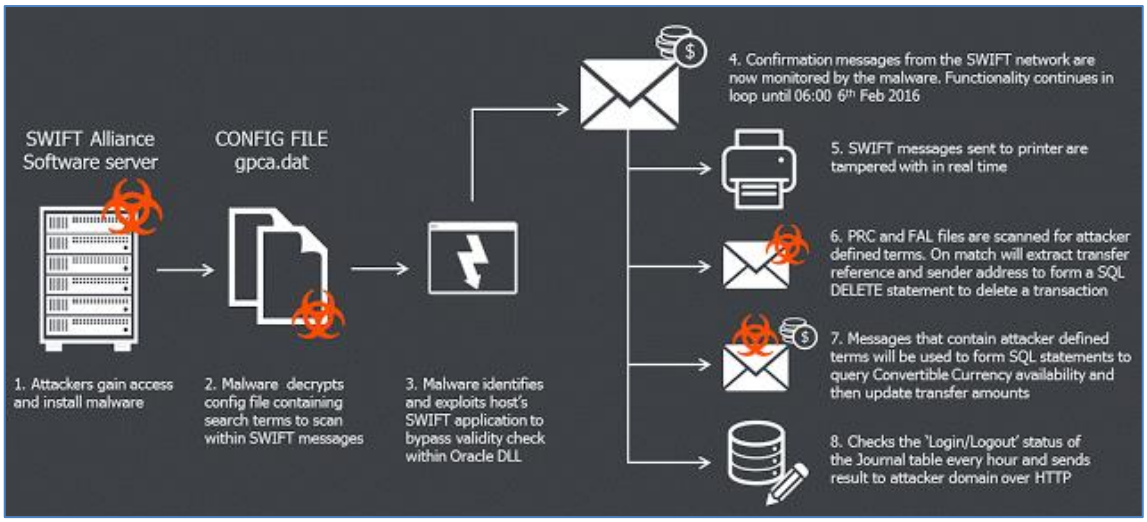
1) **Phase de reconnaissance** : étude de l'environnement de la Banque du Bangladesh pour connaître les points d'entrée possibles.

2) **Compromission initiale** : la compromission initiale a pu être réalisée du fait du manque de sécurité des réseaux de la Banque du Bangladesh. D'après l'un des enquêteurs détachés par le Forensic Training Institute of Bangladesh pour enquêter sur le piratage, la Banque du Bangladesh était une cible facile dans la mesure où elle ne disposait pas de pare-feu et utilisait des commutateurs bas de gamme pour connecter les systèmes informatiques de la banque à SWIFT[11]. La compromission a pu venir d'une des vulnérabilités susmentionnées.

[11] http://www.reuters.com/article/us-usa-fed-bangladesh-idUSKCN0XI1UO

3) **Renforcement des accès et mouvements latéraux** : l'attaquant a par la suite pu explorer le réseau de la Banque du Bangladesh et y installer un logiciel espion, peut-être un simple RAT[12] afin d'apprendre précisément comment les employés transféraient les fonds[13]. Cela aura tout d'abord permis d'obtenir les codes d'accès SWIFT en espionnant les employés, puis de détourner le logiciel client Swift appelé Access Alliance, selon la firme spécialisée en cybersécurité BAE System[14].

4) **« Exfiltration des données » :** une fois les réseaux étudiés et le malware opérationnel, l'attaquant a pu dérober près de 80 millions de dollars à la Banque de Bangladesh via le piratage du réseau SWIFT. D'après BAE System, l'assaillant a ainsi pu déclencher des ordres via le malware evtdiag.exe[15], et masquer ceux-ci en interceptant les messages entrants confirmant les ordres passés par les pirates ou en manipulant les soldes sur des enregistrements.



Fonctionnement malware SWIFT - Source : BAE Systems

…. Employée à des desseins bien différents

Au-delà du caractère technique des offensives APT, celles-ci se caractérisent surtout par leur finalité, à savoir le vol d'informations confidentielles. De ce fait, elles sont souvent opérées par des États désireux de mettre en place des stratégies d'espionnage industriel ou de déstabilisation. On peut citer comme exemple

---

[12] *Remote Access Tool* : Outil d'administration à distance, permettant la prise de contrôle à distance d'un ordinateur. Ce type de logiciel permet généralement de voir tel quel l'affichage de l'utilisateur.

[13] http://www.zdnet.com/article/malware-was-at-the-root-of-80-million-bangladesh-bank-heist/

[14] http://www.reuters.com/article/us-cyber-banking-swift-exclusive-idUSKCN0XM2DI?feedType=RSS&feedName=technologyNews&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+reuters%2FtechnologyNews+%28Reuters+Technology+News%29&utm_content=Netvibes

[15] http://baesystemsai.blogspot.fr/2016/04/two-bytes-to-951m.html

l'attaque NetTraveler perpétrée en 2013 visant à la surveillance d'acteurs influents, et qui aura conduit à l'espionnage de près de 350 diplomates ou ambassadeurs originaires de près de 40 États différents.

Source : *Securelist*

L'offensive Titan Rain menée contre les États-Unis[16] (espionnage d'agences gouvernementales) ainsi que l'attaque GhostNet mise en place contre divers acteurs influents[17] (près d'un millier d'ordinateurs infectés dans le monde entier), que l'on soupçonne toutes deux d'être des opérations chinoises, correspondent à des attaques de type APT visant un objectif de renseignement. Or, les affaires Hacking Team et SWIFT diffèrent totalement des attaques APT classiques quant à leur finalité.

En effet, le pirate à l'origine de l'attaque à l'encontre de Hacking Team a certes cherché à dérober des données sensibles et à les divulguer au plus grand nombre, mais il l'a fait dans un but purement idéologique sans servir les intérêts d'un Etat. Il l'explique lui-même dans sa publication sur Pastebin[18] : « *le hacking donne à l'opprimé une chance de se battre et de gagner. C'est la beauté et l'asymétrie du hacking : avec 100 heures de travail, une personne peut détruire des années de travail d'une entreprise qui réalise plusieurs millions de chiffre d'affaires.* ». Son action a donc été réalisée dans un but hacktiviste, lui-même se

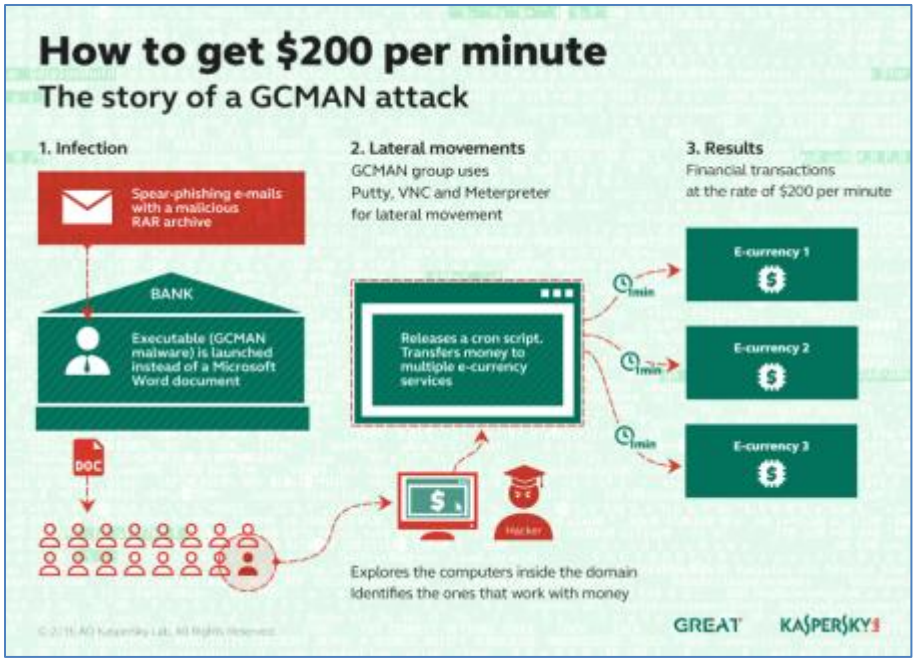
[16] https://threatpost.com/titan-rain/91835/

[17] http://www.slate.fr/story/3617/les-hackers-nationalistes-passent-%C3%A0-lattaque

[18] http://pastebin.com/raw/0SNSvyjJ

définissant comme un *« anarchiste révolutionnaire »*, luttant contre les produits proposés par Hacking Team qui permettent selon lui à des États autoritaires de surveiller et de contrôler des populations[19]. Le cas Hacking Team met en lumière un nouvel usage des méthodologies d'attaque APT, utilisées désormais dans un but hacktiviste de revendication et de dénonciation alors que, traditionnellement, les moyens techniques déployés par les hacktivistes sont moins sophistiqués (defacement, DDoS). L'affaire Hacking Team est par conséquent novatrice dans le domaine de l'attaque de type hacktiviste.

Le cas de SWIFT est encore différent, dans la mesure où la motivation de l'attaquant n'est ni le vol d'informations, ni l'hacktivisme, mais la recherche du gain financier via le détournement de fonds. Cette attaque revêt un caractère unique de par sa technicité et son organisation pour une motivation de type cybercriminelle. D'après le responsable de l'intelligence des menaces cybernétiques de BAE System, c'est la « *première fois qu'un criminel va jusqu'à ce niveau de personnalisation pour s'adapter à l'environnement auquel il fait face.* »[20]. L'assaillant demeure encore à ce jour inconnu, mais des similitudes dans le mode opératoire utilisé pour infiltrer la Banque centrale du Bangladesh et celui employé à l'encontre d'autres banques début 2015 orientent l'enquête vers des groupes cybercriminels tels que Carbanak, GCMan ou Metel. Ces derniers ont en effet déjà usé d'une stratégie de type APT afin de subtiliser des millions d'euros à diverses banques[21].



Source : Securelist

Le cas Carbanak, dans lequel près d'un milliard d'euros ont été dérobés, est très proche de celui de l'affaire SWIFT dans la mesure où le système SWIFT a également été piraté afin de permettre le détournement de fonds[22].

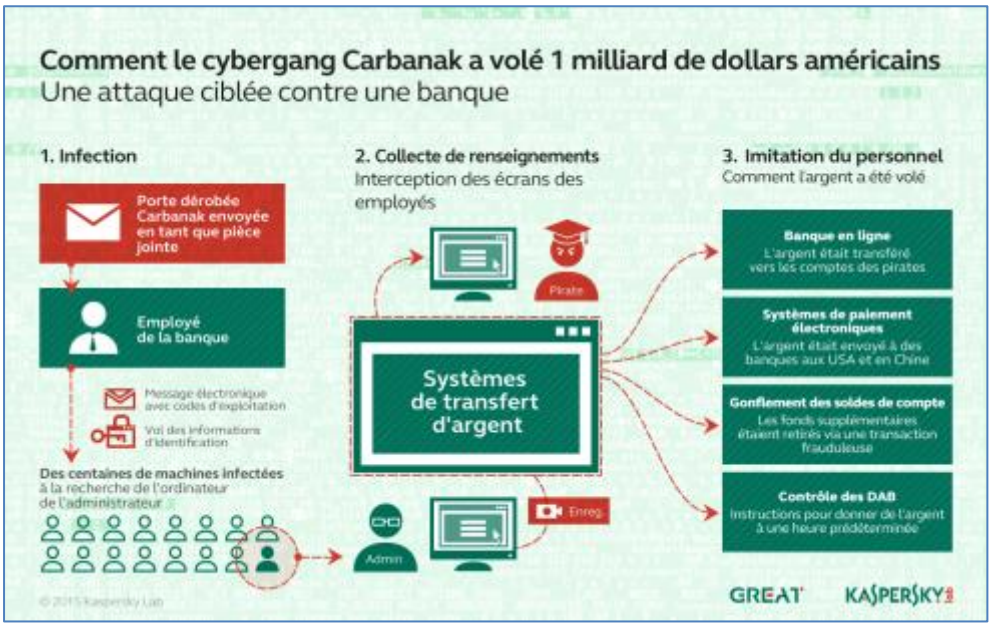
---

[19] https://motherboard.vice.com/read/the-vigilante-who-hacked-hacking-team-explains-how-he-did-it

[20] http://www.silicon.fr/malware-menace-echanges-bancaires-swift-145735.html

[21] https://securelist.com/blog/research/73638/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/

[22] http://www.01net.com/actualites/cyberbraquage-comment-les-pirates-ont-reussi-a-voler-un-milliard-de-dollars-645788.html



Source : Kaspersky

Au vu des similitudes entre ces deux affaires, il n'est pas improbable qu'un groupe cybercriminel comme Carbanak soit à l'origine de l'affaire SWIFT[23]. Là encore, ce mode opératoire est novateur dans le cadre des attaques cybercriminelles, et tend à se propager (une tentative d'attaque SWIFT similaire ayant depuis été détectée contre une banque vietnamienne)[24].

Les affaires SWIFT et Hacking Team sont donc précurseurs dans le domaine de l'hacktivisme et de la cybercriminalité. Bien qu'elles suivent à la lettre le mode opératoire de type APT, leur motivation respective est en effet bien différente de celles traditionnellement propres à ce genre d'offensives. Habituellement employé par des Etats à des fins de renseignement, le modus operandi APT semble désormais s'appliquer aux opérations hacktivistes et cybercriminelles. Ce genre d'évolution est à surveiller, dans la mesure où il pourrait se démocratiser et représenter un risque conséquent pour des acteurs majeurs de l'économie - à savoir les entreprises et les banques, qui plus est dans un contexte de dématérialisation croissante des process (évolution amenant de nouveaux enjeux en terme de cybersécurité). Les administrations publiques ne sont pas à l'abri non plus dans la mesure où elles sont régulièrement la cible d'attaques hacktivistes (vol de données à l'encontre des gouvernements turc[25], syrien[26], philippin[27] et kenyan[28] en 2016). Ces attaques pourraient donc également gagner en technicité à l'avenir. Le fait que des pirates soient parvenus à pénétrer dans les systèmes d'information de nombreuses banques (organismes pourtant généralement bien protégés contre les risques cybernétiques "traditionnels") accentue ce constat. Si les systèmes de défense des banques peuvent être compromis par des groupes cybercriminels, il n'est pas impossible que ces derniers aient les moyens de le faire pour des administrations publiques majeures.

---

[23] http://www.bloomberg.com/news/articles/2016-03-14/don-t-blame-the-fed-bangladesh-seen-responsible-for-bank-heist

[24] http://www.bloomberg.com/news/articles/2016-05-15/vietnam-s-tien-phong-bank-targeted-by-swift-hack-reuters-says

[25] http://news.softpedia.com/news/details-of-almost-50-million-turkish-citizens-leaked-online-502549.shtml

[26] http://news.softpedia.com/news/syrian-government-hacked-43-gb-of-data-spilled-online-by-hacktivists-502765.shtml

[27] http://blog.trendmicro.com/trendlabs-security-intelligence/55m-registered-voters-risk-philippine-commission-elections-hacked/

[28] http://news.softpedia.com/news/anonymous-hackers-leak-1tb-of-documents-from-kenya-s-ministry-of-foreign-affairs-503518.shtml

RUSSIE : LE LONG CHEMIN VERS L'INDEPENDANCE INFORMATIQUE

Le 17 décembre 2010, Vladimir Poutine, alors premier ministre, signe le décret n°2299-r ordonnant aux autorités et aux agences dépendantes du budget fédéral russe de se tourner activement vers des solutions open-source pour leurs besoins informatiques. Il initie un mouvement qui va s'intensifier au cours des années qui vont suivre, s'accélérant avec la montée des tensions avec l'Occident.

En dehors du domaine des services, où les solutions locales sont majoritaires, les importations représentent 80% du marché du logiciel en Russie et proviennent majoritairement des Etats-Unis. Le constat n'est pas plus reluisant du côté du matériel informatique, dont la quasi-totalité est issue de l'importation. Cette situation de dépendance se fait particulièrement sentir lorsque le 8 mars 2013, le BIS (Bureau of Industry and Securities, US Department of Commerce) ajoute l'entreprise russe T-Platforms à sa liste d'organisation qui « agissent de façon contraire à la sécurité nationale ou aux intérêts extérieurs des Etats-Unis ». Une telle décision implique en effet que toute exportation à destination des entités présentes sur la liste soit soumise à une autorisation, rarement accordée, du BIS. Pour T-Platforms, fabriquant russe de supercalculateur, l'impact de cette décision a été lourd[29] car l'entreprise importait nombre des composants de ses supercalculateurs, notamment les microprocesseurs, à des sociétés américaines.

Confortée aujourd'hui dans son choix par les conséquences de la montée des tensions avec l'Occident, la Russie poursuit tous azimuts une politique d'affranchissement à l'égard des solutions informatiques américaines, multipliant les initiatives de soutien aux entreprises locales et les coopérations avec ses partenaires des BRICS.

Initiatives politiques et conséquences des sanctions

Une volonté politique intérieure forte

La première offensive russe à l'encontre des logiciels payants date de fin 2007[30]. Le gouvernement annonce que d'ici fin 2009, les écoles devront avoir migré vers des solutions logicielles entièrement gratuites, et lance des projets pilotes dans plusieurs régions. Cette décision repose alors davantage sur une question financière que sur un principe de souveraineté : la Russie souhaite rejoindre l'Organisation Mondiale du Commerce, mais ses écoles emploient alors majoritairement des versions piratées de Windows. Le choix du système d'exploitation se porte alors sans surprise sur une distribution russe de Linux, Alt-Linux.

C'est en 2010 qu'émerge une première stratégie globale de recherche d'autonomie. Le décret présente un plan de transition à destination des institutions fédérales en 25 points, assortis de dates limites correspondantes. Le plan prévoit en outre la création d'un centre fédéral de support et d'une bibliothèque nationale d'applications open source pour accompagner la transition. Pour Alexei Smirnov, directeur général d'Alt-Linux, plus la Russie s'investira dans l'open-source, plus elle sera en mesure de l'influencer.

---

[29] http://primeurmagazine.com/weekly/AE-PR-02-14-32.html

[30] http://news.bbc.co.uk/2/hi/technology/7034828.stm

Une loi adoptée définitivement le 29 juin 2015 a créé un registre des logiciels domestiques[31]. Depuis son entrée en vigueur le 1er janvier 2016, seules les sociétés appartenant à ce registre peuvent prendre part à un marché public de fourniture de biens ou de services. En d'autres termes, la loi interdit l'usage par des autorités fédérales de logiciels étrangers s'il existe des alternatives nationales[32]. Il est admis qu'une institution puisse autoriser des entités étrangères à participer, sous condition d'en justifier la nécessité et en offrant la préférence aux solutions incluant des logiciels libres[33]. Cette loi établit trois catégories de logiciels :

- Les applications B2B, les solutions de sécurité informatique et les services web basés en Russie ;
- Les systèmes d'exploitation d'ordinateurs de bureau, de mobiles et de serveurs, les systèmes de gestion de bases de données, d'infrastructures Cloud et les suites logicielles de bureautique ;
- Les logiciels spécifiques à certaines industries, notamment de fabrication, d'énergie, de construction, de santé, de finance et de transport.

Le plan fixe un objectif ambitieux : en 2025, 50% des logiciels des catégories 2 et 3 devront être domestiques. Un objectif encore plus élevé pour la catégorie 1 où les logiciels domestiques devront représenter jusqu'à 90 % des services web.

D'après le journal russe Vedomosti, le président russe aurait même demandé en mars 2016 que le champ d'application de ces dispositions soit prochainement élargi aux contrats de fourniture des entreprises publiques[34].

L'effet des sanctions

Si le mouvement de transition avait démarré bien avant la perspective des sanctions occidentales, celles-ci ont eu pour effet d'inciter, voire de contraindre, à l'abandon des solutions informatiques occidentales.

La récession économique du pays, renforcée notamment par la forte baisse du cours du pétrole, a provoqué une chute du rouble qui a rendu les produits occidentaux d'autant plus onéreux. Face à cette problématique, la majorité des entreprises occidentales ont fait le choix d'adapter leurs prix en conséquence sur ce marché.

Cependant, la crainte de nouvelles sanctions a également incité nombre d'entreprises locales à initier cette transition afin de minimiser les risques potentiels de sanctions à leur encontre. Ainsi, le secteur bancaire et celui de l'énergie ont été les premiers à répondre à l'appel à la « souveraineté digitale » de Vladimir Poutine.

Le secteur de la défense a évidemment été particulièrement visé par les sanctions, et doit ainsi plus que jamais se reposer sur des alternatives locales. L'entreprise United Aircraft Corp., sur la liste des sanctions européennes depuis septembre 2014[35], est ainsi contrainte de travailler au remplacement des logiciels d'avionique Siemens qui équipent ses avions.

---

[31] http://asozd2.duma.gov.ru/main.nsf/%28SpravkaNew%29?OpenAgent&RN=764677-6&02 (en russe)

[32] https://themoscowtimes.com/articles/russia-restricts-use-of-foreign-software-in-battle-for-information-sovereignty-50861

[33] http://www.duanemorris.com/alerts/russia_steps_implement_import_substitution_plan_for_software_0715.html

[34] http://fortune.com/2016/03/31/russia-foreign-software/

[35] http://en.cfts.org.ua/news/eu_imposes_sanctions_on_major_russian_aircraft_corporation_that_assembles_an_148

Lorsque le 1er septembre 2015, la loi imposant aux entreprises d'héberger les données personnelles sur des serveurs localisés en Russie est entrée en vigueur, la dépréciation du rouble a encore une fois joué en faveur de ce mouvement, rendant plus attractifs les datacenters russes.

Notons cependant que la récession n'a pas eu que des effets positifs pour le marché intérieur du logiciel, celui-ci s'étant contracté de 18% en 2015. Pour assurer leur pérennité, les éditeurs russes ont aujourd'hui besoin d'exporter leurs solutions en profitant justement d'un rouble faible. Une démarche activement soutenue par le gouvernement.

Le développement à l'international

Pour parvenir à son objectif, le gouvernement multiplie les accords, et le pays peut effectivement compter sur le soutien des autres BRICS dans sa démarche d'indépendance face aux solutions américaines.

En août 2014, le ministre russe des communications annonçait par exemple avoir signé un accord avec la Chine prévoyant une augmentation des importations chinoises de logiciels russes en contrepartie d'une augmentation des importations russes de serveurs chinois[36].

Le ministère des Télécoms et des Médias indiquait également en 2015 avoir engagé des discussions avec les BRICS, qui se sont montrés intéressés par le développement conjoint de solutions logicielles d'importance critique, afin de s'affranchir du monopole américain[37].

Les initiatives et produits souverains majeurs

Les systèmes d'exploitation

Du côté des systèmes d'exploitation, la Russie mise avant tout sur des distributions[38] locales de Linux.

Faisant suite au plan de 2010, la Russie a fait développer par la société RusBitTech une distribution Linux appelée Astra Linux pour ses forces armées et ses agences de renseignement. Le système d'exploitation est certifié pour permettre le traitement d'informations classées du plus haut niveau. La société propose en outre gratuitement une version « communauté » de son système d'exploitation, mais le code source de la solution est fermé.

Rosatom (Agence fédérale de l'énergie atomique) et RJD (Compagnie des chemins de fer russe) ont de leur côté décidé à l'été 2014 du développement conjoint d'une distribution Linux baptisée Synergy, afin d'équiper leurs systèmes informatiques les plus sensibles (notamment ceux des centrales nucléaires et des systèmes de gestion des trains[39]).

---

[36] https://www.rt.com/business/181080-china-russia-technology-swap/

[37] http://minsvyaz.ru/en/events/33237/

[38] Le terme distribution fait ici référence aux différents systèmes d'exploitation assemblés autour d'un noyau Linux.

[39] http://www.vedomosti.ru/technology/articles/2014/08/25/reaktory-i-poezda-perejdut-na-linux (en russe)

Le plan de 2015[40], qui prévoyait le développement de logiciels domestiques lorsqu'aucune solution russe similaire n'existe, a en outre conduit à la sélection de deux systèmes d'exploitation :

- Alt-Linux, distribution russe de Linux. Il s'agit de la distribution qui avait été choisie pour équiper les écoles du pays ;
- ReactOS[41], un système d'exploitation conçu pour être compatible avec les applications et drivers développés pour Windows. Cette compatibilité permettrait de s'affranchir du système d'exploitation tout en permettant une migration progressive vers des solutions locales. L'équipe de ReactOS collabore notamment avec le projet *Wine*[42] dont elle partage l'objectif. Le système est actuellement considéré comme étant en phase alpha[43], mais permet déjà de faire fonctionner de nombreuses applications Windows (Adobe Reader, OpenOffice, etc.).

Enfin, le volet « mobilité » n'a pas été oublié. Si iOS et Android représentent ensemble 90% du marché des smartphones en Russie, le gouvernement souhaite voir cette part tomber à 50% d'ici 2025. Pour ce faire, la Russie souhaite le développement d'une version localisée du système d'exploitation SailFish où des services russes remplaceraient les services américains[44]. On notera à ce propos que la FAS[45] (Federal Antimonopoly Service), l'autorité russe en charge de la concurrence, est actuellement en conflit juridique[46] avec Google, qui impose aux constructeurs souhaitant intégrer Android à leurs smartphones d'y préinstaller la suite de logiciel Google Apps. L'institution russe considère qu'il s'agit de pratiques anti-concurrentielles, une position d'ailleurs partagée par la Commission Européenne qui avait initié une procédure similaire plusieurs mois auparavant[47]. Cette situation est très similaire au différend qui avait opposé la Commission Européenne à Microsoft et qui avait conduit à une amende record de 899M€ en 2008[48].

Les processeurs

Le 19 juin 2014, le Ministère du Commerce et de l'Industrie a annoncé son intention de cesser de s'équiper en processeurs américains (Intel et AMD) et de ne se fournir qu'en processeurs Baikal. Des processeurs[49] conçus par la société russe T-Platforms (spécialisée dans les supercalculateurs), avec le soutien du conglomérat Rostec et le cofinancement du géant technologique publique Rosnano.

Deux processeurs sont aujourd'hui développés par T-Platforms :

---

[40] http://minsvyaz.ru/en/events/32967/

[41] https://www.reactos.org/

[42] Wine est un projet visant à faire fonctionner des applications Windows sur les distributions Linux.

[43] https://en.wikipedia.org/wiki/ReactOS

[44] http://www.theverge.com/2015/5/19/8624901/russia-mobile-os-sailfish-jolla-tizen

[45] http://en.fas.gov.ru/

[46] http://arstechnica.com/tech-policy/2016/08/google-loses-appeal-russia-android-ruling/

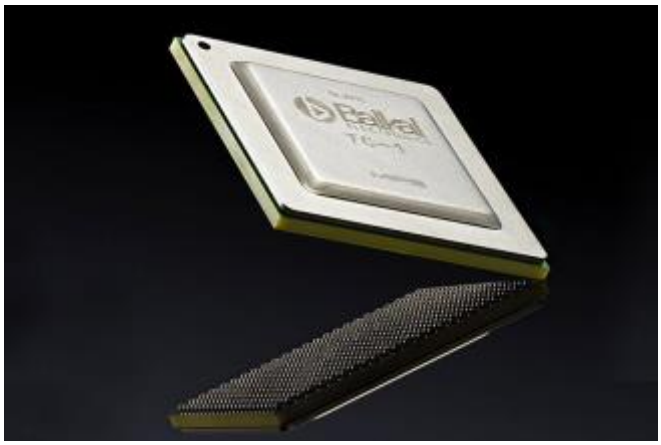
[47] http://europa.eu/rapid/press-release_IP-16-1492_fr.htm

[48] http://www.lemondeinformatique.fr/actualites/lire-bruxelles-inflige-a-microsoft-une-nouvelle-amende-record-de-899-meteuro-25459.html

[49] http://www.baikalelectronics.com/products/ (en russe)

- Les processeurs Baikal M et M/S sont basés sur une architecture développée par l'entreprise anglaise ARM[50]. Il s'agit d'une architecture de puce employée par d'autres fondeurs au sein de processeurs de serveurs (AMD) et de smartphones (Qualcomm, Samsung) ;
- Les processeurs Baikal T1 sont basés sur une puce MIPS[51], développés par la société californienne éponyme. Les puces MIPS se retrouvent généralement dans le domaine des systèmes embarqués et les équipements réseaux, mais on la retrouve également dans certains supercalculateurs chinois.

L'indépendance matérielle que procurent les processeurs Baikal reste cependant toute relative : bien que reposant sur une conception domestique, ils emploient une architecture étrangère (MIPS ou ARM) et sont fabriqués à Taiwan par TSMC, le plus grand producteur mondial de semi-conducteurs[52]. Pour autant, cette approche permet de familiariser les ingénieurs russes avec des architectures, constituant un premier pas avant la conception d'un processeur doté d'une véritable puce "maison". On notera au passage que T-Platforms fait le choix de processeurs basés sur des architectures connues pour leur efficience énergétique, ce qui ouvre la voie au développement futur de puces souveraines pour la mobilité.



Processeur Baikal TC-1, basé sur architecture MIPS

[50] Contrairement à ses concurrents, l'entreprise ARM ne vend pas à proprement parler de processeurs : elle met au point des architectures de puces qu'elle vend sous forme de licence en tant que propriété intellectuelle.

[51] MIPS Technologies est une société basée en Californie et rachetée en 2013 par la société britannique Imagination Technologies

[52] http://www.gartner.com/newsroom/id/3027717

La deuxième offensive russe en matière de processeurs est conduite par la société MCST, créée en 1992 mais partant des travaux de l'ère soviétique[53], qui fournit depuis cette date la défense et les administrations russes. Elle tente depuis quelques années d'élargir sa cible, et parvient aujourd'hui à vendre « aux organisations pour lesquelles la sécurité constitue un critère important »[54]. MCST conçoit en effet des systèmes informatiques complets, ce qui inclut une architecture maison pour laquelle une distribution Linux a été développée, dans l'objectif de pouvoir assurer à ses clients que ses produits ne possèdent pas de « capacités non déclarées », c'est à dire, en d'autres termes, que ceux-ci sont exempts de portes dérobées. Les processeurs Elbrus-4C peuvent être comparés aux processeurs *Atom* d'Intel datant de 2010 en termes de performance[55], mais la génération suivante dont la production a démarré à Taïwan, devrait être du niveau des processeurs de type i7 d'Intel[56].

Pour l'heure, les ordinateurs dotés de composants russes restent cependant beaucoup plus onéreux que leurs équivalents étrangers du fait du faible volume de production. La production micro-électronique russe reste en effet limitée, même si les progrès réalisés ces dernières années montrent une forte volonté politique.

De façon plus générale, il est clair que les initiatives gouvernementales sont encore loin d'avoir véritablement changé la donne en termes d'usage au niveau national. La transition est en outre loin d'être achevée au sein même de l'administration. Une enquête parlementaire[57] rendue publique le 9 août 2016 a révélé que la majorité des agences nationales continuent d'avoir recours à des produits Microsoft. L'enquête a notamment fait émerger des contrats avec l'entreprise américaine pour un montant totalisant 12 millions de dollars[58]. Au-delà même de la problématique du développement des alternatives (1 186 logiciels figurent actuellement dans le registre national), force est de constater que ce type de migration se heurte aussi à l'aversion au changement de la part des utilisateurs et à l'impératif de productivité des organisations concernées.

---

[53] http://www.mcst.ru/istorija_predprijatija (en russe)

[54] https://www.youtube.com/watch?v=f3lBJt478l8, propos de Konstantin Truskkin, directeur marketing de MCST

[55] http://www.tomshardware.com/news/mcst-elbrus-4c-x86-programs,29077.html

[56] http://www.mcst.ru/novyj-8yadernyj-mikroprocessor-elbrus-8c (en russe)

[57] http://rbth.ru/science_and_tech/2016/08/09/why-do-russian-officials-still-prefer-to-use-microsoft_619419

[58] Les achats combinés des administrations russes en 2014 auprès de SAP, Oracle, IBM et Microsoft représentaient 300 millions de dollars.

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