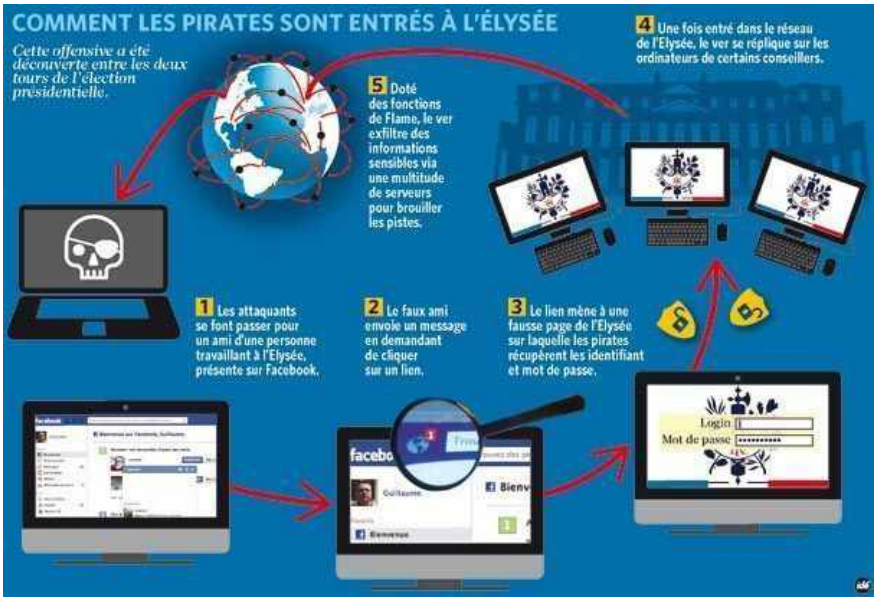
Cyberguerre: comment les Américains ont piraté l'Élysée

Par Charles Haquet et Emmanuel Paquette (L'Express) - publié le 20/11/2012 à 15:31

EXCLUSIF. En mai, l'équipe de Nicolas Sarkozy a été victime d'une opération d'espionnage informatique hypersophistiquée. Les sources de L'Express concordent : le coup vient de... l'ami américain. Révélations sur une attaque qui s'inscrit dans une bataille planétaire.



CYBERGUERRE - Les intrus qui se sont introduits dans les réseaux informatiques de l'Elysée en mai dernier ont subtilisé des notes secrètes et des plans stratégiques à partir des ordinateurs de proches conseillers de Nicolas Sarkozy.

DR

C'est l'un des hold-up les plus audacieux réalisés contre l'Etat français. En mai dernier, quelques jours avant le second tour de l'élection présidentielle, des pirates ont réussi à s'introduire dans les réseaux informatiques de l'Elysée. Révélée par le quotidien régional Le Télégramme, cette intrusion avait alors été soigneusement étouffée par le Château. Une omerta qui, jusqu'à présent, n'avait pas été brisée. Aucune information n'avait filtré sur la nature des agresseurs, ou même sur le préjudice subi. Pourtant, l'affaire est grave, d'autant qu'elle constituerait une cyberattaque sans précédent entre pays alliés.

L'Express peut révéler que les intrus ont non seulement réussi à pénétrer au coeur même du pouvoir politique français, mais qu'ils ont pu fouiller les ordinateurs des proches conseillers de Nicolas Sarkozy. Des notes secrètes ont été récupérées sur des disques durs, mais aussi des plans stratégiques. Du vrai travail de pro, digne du dernier James Bond, Skyfall. Et, comme souvent dans ce type d'attaque, une négligence humaine est à l'origine de la catastrophe.

L'ordinateur du secrétaire général de l'Elysée pillé

Tout a commencé sur Facebook. Les assaillants ont d'abord identifié, sur le réseau social, le profil de personnes travaillant au palais présidentiel. Se faisant passer pour des amis, ils les ont ensuite invitées, par un message électronique, à se connecter sur l'intranet du Château. Sauf que ce lien menait à une fausse page Web - une réplique de celle de l'Elysée. Les victimes n'y ont vu que du feu ; et lorsque est apparu, à l'écran, un message leur demandant leur identifiant et leur mot de passe, elles les ont donnés en toute bonne foi. Une technique bien connue des hackers, qui leur a permis de récupérer les clefs numériques pour s'inviter en toute quiétude dans le saint des saints.

Une fois à l'intérieur, les pirates ont installé un logiciel espion qui s'est

La réaction de l'ambassade des Etats-Unis à Paris

Nous réfutons catégoriquement les allégations de sources non-identifiées, parues dans un article de l'Express, selon lesquelles le gouvernement des Etats-Unis d'Amérique aurait participé à une cyberattaque contre le gouvernement français. La France est l'un de nos meilleurs alliés. Notre coopération est remarquable dans les domaines du renseignement, du maintien de l'ordre et de la cyberdéfense. Elle n'a jamais été aussi bonne et demeure essentielle pour mener à bien notre lutte commune contre la menace extrémiste.

Mitchell Moss, porte-parole de l'ambassade des Etats-Unis à Paris

propagé d'un ordinateur à l'autre. Très élaboré, ce "ver" n'a infecté que quelques machines. Et pas n'importe lesquelles : celles des conseillers les plus influents du gouvernement... et du secrétaire général, Xavier Musca. Nicolas Sarkozy y a, lui, échappé. Et pour cause, il ne possédait pas de PC. Malheureusement pour les assaillants, le code malveillant a laissé des empreintes. "Telles des marionnettes actionnées par des fils invisibles, les machines infectées communiquent avec leur maître pour prendre leurs ordres, décrypte un expert, Olivier Caleff, responsable sécurité du Cert-Devoteam, une société de sécurité informatique. Lorsque l'on essaie de remonter ces fils sur Internet, on arrive souvent sur des serveurs situés à l'étranger."

C'est ce travail de fourmi qu'ont mené les enquêteurs français. Le degré de sophistication de l'attaque était tel que les suspects se limitaient, d'emblée, à une poignée de pays. Pour preuve, le cyberpompier de l'Etat, l'Agence nationale de la sécurité des systèmes d'information (Anssi), a mis plusieurs jours pour restaurer le réseau de l'Elysée. Difficile de trouver l'origine de l'offensive. Souvent, les assaillants brouillent les pistes en passant par des pays tiers. Autant de rebonds, sur des serveurs situés sur les cinq continents, qui rendent ce fil d'Ariane très compliqué à suivre, même pour les "cyberdétectives" de l'Etat mobilisés pour l'occasion. Mais, selon les informations recueillies par L'Express auprès de plusieurs sources, leurs conclusions, fondées sur un faisceau de présomptions, convergent vers le plus vieil allié de la France : les Etats-Unis.

Le virus porte la marque de son auteur

Le code malveillant utilisé affiche, en effet, les mêmes fonctionnalités qu'un ver informatique extrêmement puissant, baptisé Flame, identifié à la fin du mois de mai par une grande société russe d'antivirus, Kaspersky. "Très perfectionné, il peut collecter les fichiers présents sur une ma-chine, réaliser des captures d'écran et même activer le microphone d'un PC pour enregistrer les conversations, expli-que Vitaly Kamluk, spécialiste du sujet chez cet éditeur. Sa conception a demandé beaucoup d'argent et des moyens humains que seul un grand pays est en mesure de mobiliser." Ou même deux : selon la presse anglo-saxonne, le ver aurait été créé par une équipe américano-israélienne, car il devait viser initialement des pays du Moyen-Orient (Iran, Egypte). Autre élément à charge : tel un peintre reconnaissable à son trait, un virus porte les marques du savoir-faire de son auteur. Janet Napolitano, secrétaire d'Etat à la Sécurité intérieure de l'administration Obama, n'a ni confirmé ni démenti nos informations.

Contactés à ce sujet, ni l'Anssi ni l'Elysée n'ont souhaité faire de commentaires. Reste une question. Pourquoi un allié de la France lancerait-il une telle opération ? "Vous pouvez être en très bons termes avec un "pays ami" et vouloir, en même temps, vous assurer de son soutien indéfectible, surtout dans une période de transition politique", note un proche du dossier, sous le couvert de l'anonymat. Sans compter que l'Elysée joue un rôle clef dans la signature de grands contrats avec des pays étrangers, notamment au Moyen-Orient. "C'était encore plus vrai à l'époque de Nicolas Sarkozy", rappelle Nicolas Arpagian, directeur scientifique du cycle sécurité numérique à l'Institut national des hautes études de la sécurité et de la justice.

Quitte à être espionné, sans doute vaut-il mieux l'être par un allié... "Nous avons de grands partenaires avec lesquels nous collaborons et entretenons des relations de confiance, et d'autres avec qui nous ne partageons pas les mêmes valeurs", rappelle le contre-amiral Arnaud Coustillière, responsable du volet militaire de la cyberdéfense française. Il n'empêche, l'attitude de l'administration Obama suscite de nombreuses interrogations.

Vers des attaques "pires que le 11 Septembre" ?

Dans une version du livre blanc sur la défense, actuellement en cours de rédaction, des auteurs ont soulevé les ambiguïtés de Washington. "Face à la difficulté d'utiliser les voies de droit, [les Etats-Unis] ont recours de plus en plus à l'action clandestine, ce qui peut poser une question de contrôle démocratique."

Ironie du sort, le Congrès américain vient, le 14 novembre, de publier un rapport accablant sur l'"acteur le plus menaçant du cyberespace", à savoir... la Chine. Leon Panetta, secrétaire d'Etat à la Défense, a

REUTERS/Larry Downing

"La cybermenace est l'un des plus sérieux défis auxquels nous soyons confrontés en tant que nation"

Barack Obama, président des Etats-Unis, mai 2009.

REUTERS/Neil Hall

"Nous consacrerons un budget de plus d'un demi-milliard de livres [626 millions d'euros] à la cybersécurité"

David Cameron, Premier ministre britannique, octobre 2010.

REUTERS/Thomas Peter

"Les attaques cybernétiques sont aussi dangereuses que la guerre conventionnelle"

Angela Merkel, chancelière allemande, avril 2011.

Un instantané des cyberattaques en cours...
HoneyMap réalisé par Honeynet Project

même déclaré récemment que, par leur puissance numérique, "certains pays" seraient, d'ores et déjà, capables de provoquer un "cyber-Pearl Harbor" : "Ce serait pire que le 11 Septembre ! Des assaillants pourraient faire dérailler un train de voyageurs ou un convoi de produits chimiques dangereux. Ou, encore, contaminer les systèmes d'eau des grandes villes ou éteindre une grande partie du réseau électrique." Le tout en se cachant derrière des écrans d'ordinateurs situés à des milliers de kilomètres...

Dans le monde virtuel, tous les coups sont permis

Leon Panetta sait de quoi il parle. L'Oncle Sam a déjà utilisé ces moyens. C'était en 2010, lors de l'opération "Jeux olympiques", lancée conjointement avec Israël contre l'Iran. Leur logiciel Stuxnet aurait endommagé un grand nombre des centrifugeuses utilisées par Téhéran pour enrichir de l'uranium. Spectaculaire, cette opération ne doit pas faire oublier que d'autres nations oeuvrent dans l'ombre. Dans le plus grand secret, de nombreux pays, démocratiques ou non, fourbissent leurs armes numériques. Des forces secrètes se constituent, des mercenaires vendent leurs services aux plus offrants. Sans foi ni loi. La Toile n'est pas un champ de bataille comme les autres. Oubliez les codes de l'honneur, les conventions internationales ou les alliances. Tous les coups sont permis. Et mieux vaut avoir les moyens de se battre. Dans le cyberespace, personne ne vous entendra crier.

Pour s'en convaincre, il suffit de se rendre au quartier général de l'Otan, à Bruxelles. Tou-tes les nuits, vers 1 heure, c'est le même rituel, explique l'un des responsables européens de la sécurité au sein de l'organisation. "Sur une carte, à l'écran, on voit des dizaines de lumières s'allumer en Chine, explique-t-il. Ce sont les hackers qui, le matin, lancent des attaques lorsqu'ils arrivent au boulot. Et, le soir, elles s'éteignent quand ils rentrent chez eux." Même constat d'un proche de la NSA, l'agence de renseignement des Etats-Unis : "Parfois, nous enregistrons une baisse sensible des tentatives d'intrusion sur nos sites, témoigne-t-il. Invariablement, cela correspond à des jours fériés en Chine."

Mais l'image d'une "superagence" où des armées de pirates travailleraient en batterie pour ravir les secrets de l'Occident ne reflète pas la réalité. Selon ce même agent, "leur capacité offensive est beaucoup moins centralisée qu'on pourrait l'imaginer. De nombreuses régions ont mis en place leur propre dispositif, qui dépend du bureau politique local. Et il n'est pas rare que ces factions se combattent entre elles."

Coût d'une attaque : quelques centaines de milliers d'euros

Un hacker, qui souhaite rester anonyme, pense, lui aussi, que l'on surestime un peu le "cyberpéril jaune". "J'ai eu l'occasion de voir travailler les Chinois, ce ne sont pas les plus affûtés, dit-il. Leurs techniques sont assez rudimentaires par rapport à celles des Américains ou des Israéliens..."

A chaque pays sa spécificité. En Russie, le dispositif d'attaque est opaque. De nombreux spécialistes occidentaux du renseignement soupçonnent l'existence d'une relation triangulaire entre l'Etat, la mafia et certaines sociétés de conseil informatique qui seraient le bras armé du Kremlin. "Avez-vous déjà vu, en Russie, un hacker avoir des problèmes avec la police ? questionne Garry Kasparov, ancien champion du monde d'échecs, aujourd'hui l'un des opposants au président Poutine. Non, parce que l'on sait qui se trouve aux manettes, dans l'ombre..."

REUTERS/Minoru Iwasaki/Pool

"Les questions de sécurité alimentaire, d'énergie et de cybersécurité deviennent plus aiguës"

Hu Jintao, secrétaire général du Parti communiste chinois, novembre 2012.

Contrairement à ce que l'on pourrait croire, les Européens ne sont pas en reste. La France, c'est une surprise, dispose d'une force de frappe numérique. Mais on trouve aussi, sur l'échiquier mondial, des Etats moins avancés sur le plan technique, tels l'Iran et la Corée du Nord. Nul besoin, en effet, d'investir dans des infrastructures coûteuses. Il suffit d'un ordinateur, d'un accès à Internet et de quelques centaines de milliers d'euros pour monter une attaque. Car sur la Toile, comme dans la vraie guerre, on trouve toutes sortes d'armes sur le marché. Il suffit de frapper aux bonnes portes. Au lieu d'une kalachnikov, on repartira avec un logiciel malveillant (malware, dans le jargon) qui permettra de prendre le contrôle d'un système ennemi. La première motivation : "Faire du business !"

"C'est un enjeu de domination. En maîtrisant l'information, on contrôle tout", résume Jonathan Brossard. Ce hacker français renommé intervient aujourd'hui dans des groupes internationaux. Son job consiste à s'introduire dans les systèmes informatiques pour en révéler les failles - et trouver des parades. Pour lui, les risques d'un cyberconflit existent, mais ils masquent une autre motivation, bien plus puissante : "Faire du business ! Etre capable de griller un réseau électrique, c'est bien, mais le véritable enjeu, c'est surtout de gagner des parts de marché." Connaître, dans le détail, la proposition d'un concurrent, lors d'un gros appel d'offres, donne un avantage décisif. Pour l'avoir

négligé, certaines sociétés ont péri. Des pirates - chinois semble-t-il - ont pillé les secrets du géant canadien des télécoms Nortel pendant près de dix ans, au point de l'acculer à la faillite. De tels exemples abondent.

Et la France n'est, malheureusement, pas épargnée. Les grandes entreprises du CAC 40 compteraient même parmi les plus vulnérables d'Europe. Sur ce nouveau champ de bataille invisible, on ne compte pas les morts, mais les points de PIB perdus. Et, derrière, sans doute des emplois par milliers.

Batailles de virus

STUXNET
Découverte : juin 2010.
Cible : ce logiciel a détruit des milliers de centrifugeuses nucléaires, en Iran.
Origine supposée : opération "Jeux olympiques", menée par les Etats-Unis et Israël.

DUQU
Découverte : septembre 2011.
Cible : lié à Stuxnet, ce ver informatique a servi à espionner le programme nucléaire iranien.
Origine supposée : Etats-Unis et Israël.

MAHDI
Découverte : février 2012.
Cible : capable d'enregistrer les frappes sur un clavier et les photos et textes d'un ordinateur, Mahdi a été retrouvé en Iran, en Afghanistan et en Israël.
Origine supposée : inconnue.

WIPER
Découverte : avril 2012.Cible : ce virus fait disparaître les données des disques durs des ordinateurs infectés. Il a touché des compagnies pétrolières iraniennes.
Origine supposée : inconnue.

FLAME
Découverte : mai 2012.
Cible : ce logiciel très sophistiqué aurait espionné depuis 2007 plusieurs pays, dont l'Iran, la Syrie, le Soudan, ou encore l'Arabie saoudite.
Origine supposée : opération des Etats-Unis et d'Israël.

GAUSS
Découverte : juin 2012.
Cible : capable d'espionner les transactions financières et messages électroniques, ce virus s'est répandu au Liban, en Israël et en Palestine.
Origine supposée : inconnue.

SHAMOON
Découverte : août 2012.
Cible : les ordinateurs des compagnies pétrolières saoudiennes Aramco et RasGas au Qatar ont été attaqués par ce virus.
Origine revendiquée : groupe de hackers appelé "Glaive tranchant de la justice", peut-être d'origine iranienne.