Les banques libanaises prennent-elles la réelle mesure de la cyber-menace ?

Sécurité La mise à jour des systèmes antivirus, une pratique censée faire partie du quotidien des établissements de crédit.

Les auteurs de ce papier, qui s'avèrent être des praticiens de la sécurité des systèmes d'information, s'expriment avant tout en tant que clients du système bancaire libanais.

Certains d'entre nous ont été les premiers à faire face au Malware Gauss qui a sévi dans les systèmes d'information de certaines banques libanaises. Nous avons également pris connaissance de la note de la Banque du Liban (BDL), diffusée à l'ensemble des directions informatiques bancaires du pays en réaction à cet incident. Nous avons par ailleurs lu divers communiqués dans la presse arabe et libanaise, attribués à des cadres bancaires libanais, s'exprimant pour certains au nom de la BDL.

Nous pouvons tout à fait comprendre le besoin d'une telle communication dans la presse, celle-ci visant à accroître le niveau de confiance dans le secteur bancaire libanais auprès des médias. Elle vise également à rassurer le public qui, en grande majorité, est profane dans le mode opératoire de Gauss.

Cependant, vu la nature extrêmement létale et furtive du malware Gauss, nous craignons qu'une telle analyse, pour peu qu'elle soit considérée comme suffisante et non éprouvée, nuit beaucoup plus à la réputation du secteur bancaire libanais qu'elle n'apporte la confiance recherchée.

En effet, les propos attribués à certains cadres bancaires s'exprimant dans la presse pourraient être trompeurs et donneraient l'impression que la BDL n'a pas suffisamment bien cerné le mode opératoire du malware Gauss, surtout que ce dernier s'attaque aux postes de travail des clients finaux alors qu'ils sont connectés à leur banque en ligne, plutôt qu'aux systèmes d'information eux-mêmes des banques concernées.

La solution annoncée dans la presse et consistant à se contenter de mettre à jour les systèmes antivirus des banques n'empêchera pas de futurs malware sophistiqués de prendre pour cible le secteur bancaire libanais. Plus dangereusement, cela pourrait même inciter la partie adverse, étatique ou pas, à effectuer des opérations de hacking et de cyber-espionnage encore plus létales et fréquentes...

Gauss est un outil de cyber-espionnage extrêmement sophistiqué, s'inscrivant dans la catégorie des Menaces persistantes avancées, ou APT (Advanced Persistent Threats). Ce malware est loin d'être le fruit d'adolescents bricoleurs, ou Script-Kiddies, en mal de reconnaissance.

En relatant des analyses simplistes sur Gauss, le secteur bancaire libanais ne serait pas en train de manifester une réelle aptitude à se protéger.

Par ailleurs et dès lors qu'il s'agit de la quintessence même du secteur bancaire local, il est choquant de lire dans la presse que « d'autres responsables bancaires affirment ne pas être concernés par un quelconque virus en insistant qu'ils n'ont rien à cacher ».

Est-ce que la BDL est en train d'appliquer les normes et standards de sécurité selon les règles de l'art ? Est-ce que les banques sont suffisamment sensibilisées à ces problématiques ? Est-ce que des investissements adéquats sont consentis en la matière ?

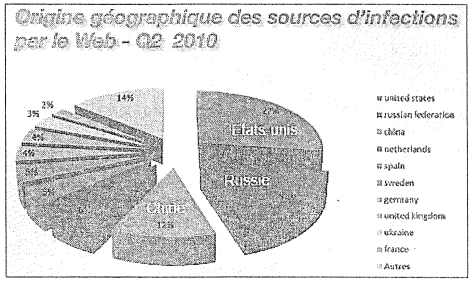
Les autorités de régulation et de contrôle doivent réellement inciter les banques libanaises à obtenir la conformité ISO 27001 en se dotant d'un véritable Système de management de la sécurité de l'information, ou SMSI. Un tel mécanisme d'amélioration continue accroîtra concrètement la réputation des banques libanaises, surtout en ce qui se rapporte à la gestion de leurs risques opérationnels.

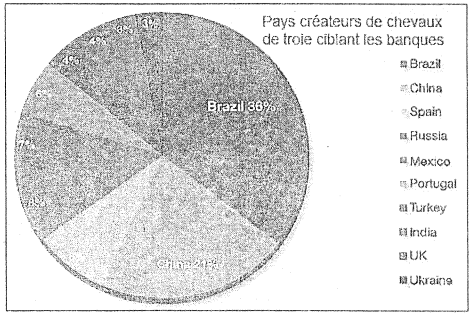
Ainsi, il apparaît clairement que le chemin est encore long pour atteindre une telle maturité. Découvrir dans la presse que plusieurs cyber-attaques ciblent de manière répétée les mêmes actifs bancaires n'est pas à l'avantage de ce secteur. Nous espérons sincèrement que cet incident déclenchera des actions plus sérieuses et plus efficaces ! Un programme de sécurité de l'information doit exister et doit reposer sur une stratégie claire avec des résultats mesurables et une réelle identification des rôles et responsabilités de toutes les parties prenantes.

Du moment que beaucoup trop de temps s'est écoulé entre la divulgation, par Kaspersky, de l'infection virale et la réaction « publique » de la BDL, nous pouvons légitimement nous demander si celle-ci a désigné un porte-parole officiel en cas de crise. Une telle personne s'appuierait sur un Computer Security Incident Response Team (CISRT) ou structure équivalente afin de diagnostiquer l'incident et de protéger le secteur bancaire et ses clients de toute information inexacte, voire dangereuse dans les médias.

Il n'est pas honteux d'admettre nos défaillances face à une menace cybernétique sans cesse évoluée et complexe, tant que nous nous engageons à y pallier tout en rassurant les citoyens en portant à leur connaissance l'ensemble des mesures requises pour endiguer et éradiquer ce malware.

N'oublions pas que de gigantesques institutions financières et non financières de par le monde ont été victimes de cyber-attaques. Même des entreprises spécialisées en sécurité des systèmes d'information ont eu elles-mêmes à subir les affres de telles attaques. Néanmoins, grâce à la mise en place d'un véritable SMSI, elles étaient aptes à rebondir et réagir rapidement et professionnellement.





Les initiés connaissent les trois attributs fondateurs en sécurité que sont la disponibilité, l'intégrité et la confidentialité de l'information. Ces derniers sont nécessaires, mais non suffisants. Il faut les agrémenter de la « responsabilité ultime » ou Accountability, seule garante d'un SMSI efficace.

Pour finir sur une note plus légère, nous nous amusons tous lorsque les Libanais applaudissent lors de l'atterrissage de leur avion sur le tarmac de l'AIB, alors qu'il est plus que normal et prévisible de vivre un atterrissage réussi ! Le même constat s'applique ici aux banquiers qui « mettent régulièrement à jour leurs systèmes antivirus » : quoi de plus normal et attendu en 2012 ?

Une cyber-sécurité durable ne sera possible qu'à travers un programme d'amélioration continue !

Zouheir ABDALLAH, Élias DIAB, Hadi el-KHOURY, Michel GHANEM et Jocelyne ZIADÉ

Télévision

Sélection du jour réalisée par R
Programmes communiqués par les chaines et publiés sc

Chaines locales

LBCI 23:00
08:00 Familia 23:30
09:00 Al-Hout 00:00
10:00 Nharkoum Saïd 01:00
11:30 Harim el-Sultan 02:00
12:30 Bayyaet el-Ward 03:30
13:30 Feriha 04:30
14:30 Infos 05:00
15:00 Helwi el-Hayet 06:00
16:30 Ochk wa Jaza' 06:30
17:45 Harim el-Sultan
18:45 Feriha **OTV**
19:50 Hayda Lebnan 08:00
19:57 Journal 11:30
20:30 Lawla el-Hob 12:30
21:30 Ahmar bi el-Khat el-Arid 13:30
23:00 Ochk wa Jaza'. 14:15
14:45
Future TV 16:30
07:00 Journal 17:00
07:30 Akhbar el-Sabah 17:45
08:00 Infos 18:45
08:15 Akhbar el-Sabah 19:45
09:00 Infos 20:30
09:15 Kalam Beyrouth 21:30
10:00 Infos 23:30
10:15 Aalam el-Sabah
11:00 Infos **MTV**
11:15 Aalam el-Sabah 07:20
12:00 Infos 08:00
12:15 Aalam el-Sabah 08:20
13:00 Ma Malakat 12:30
Aymanoukoum 14:00
14:00 Zay el-Ward 16:00
15:00 Infos 18:00
16:00 Journal arménien 19:00
16:15 Journal anglais 19:50
16:40 Journal français 19:52
17:00 Documentaire 20:45
17:30 Marianna wa Scarlett 22:00
20:15 DNA
20:30 Inter-Views 00:00
22:00 Zay el-Ward 00:15

Chaines câblées

TF1 17:03
18:25 Quatre mariages pour une lune de miel 18:00
18:20
20:05 Le juste prix 18:33
21:00 Journal
21:50 Série *Criminal Minds* 18:38
22:35 Série *Criminal Minds* 19:39
00:15 Série *Dexter*. 20:09
20:11
France 2 20:30
18:50 On ne demande qu'à en rire 21:03
22:47
19:50 Volte-face 23:00
21:00 Journal 23:10
21:45 Téléfilm *Médecin-chef à la santé* 23:39
00:00 Magazine *Un jour, un destin*. 23:57
France 3 00:01