PHILIPPE LAURIER *coresponsable du module intelligence économique à l'École polytechnique (département HSS)*

LE PIRATAGE INFORMATIQUE EN FRANCE : UN CYBERIMPÔT

Une étude de terrain menée depuis 2016 par SystemX sur la quantification du risque informatique sur l'ensemble du territoire français, avec une soixantaine de petites entreprises et d'associations loi 1901 victimes d'attaques, révèle que le seuil symbolique de 1 % de probabilité d'être victime d'une attaque par chiffrement de données, par an, est largement franchi. Aujourd'hui, réunir quelques dizaines de petits patrons, par exemple de TPE, est la quasi-certitude statistique de trouver parmi cet auditoire une victime sur l'année.

DES CENTAINES DE MILLIONS D'EUROS DE PRÉJUDICE

Deux types d'attaques ressortent du paysage : d'une part les cryptovirus (chiffrer vos données, puis vous réclamer une rançon), d'autre part la fraude « au président » (ainsi que les faux ordres de virements) trop hâtivement circonscrite à ne relever que de l'ingénierie sociale. Chacun des deux engendre un préjudice annuel chiffrable en centaines de millions d'euros au moins. L'espionnage par voie numérique s'ajouterait à ce duo, mais sa faible détectabilité le maintient dans l'ombre, hormis lorsqu'il décide de se rendre visible, par exemple avec les captations de mots de passe permettant les prises de contrôle de votre messagerie.

Le volume, souvent sous-évalué, des attaques par cryptovirus est atténué par leur faible coût financier unitaire, typiquement de quelques milliers d'euros pour une petite PME, loin en cela des sommes, parfois surévaluées, lues dans les gros titres de presse. Le fait que la médiane et le mode soient quant à eux encore bien au-dessous de ce montant moyen dessine une pyramide des préjudices faite d'une base très large, constituée d'une majorité de victimes pour lesquelles le dégât restera modeste, souvent grâce à la présence de sauvegardes régulières. Mais la pointe, avec son étroitesse, montera très haut dans sa traduction pécuniaire, jusqu'à devenir létale pour des entreprises aux trésoreries souvent tendues.

Face au « cyberimpôt » que représentent les fraudes et attaques numériques, chiffrables en centaines de millions d'euros annuels pour l'économie, il devient urgent de repenser à moindre coût la sécurité intrinsèque de nos communications, plutôt que de se contenter d'apposer chez l'utilisateur final des couches de sécurité onéreuses sur un substrat insécurisé.

L'X EN PREMIÈRE LIGNE ?

L'École polytechnique en serait un observatoire représentatif, qui subit des tentatives régulières à l'instar de ce « Pour déverrouiller votre accès au courrier, veuillez cliquer ici » diffusé sur la messagerie un vendredi soir – horaire prisé des pirates – *via* le compte d'une personne interne. Le caractère rudimentaire de ce libellé, qui joue lui aussi sur une espérance d'ordre statistique puisqu'il balaye un public nombreux, s'efface aujourd'hui devant la qualité des formulations, des motifs, des usurpations d'identités, et laisse craindre à court terme une incapacité à discerner le vrai du faux, l'original de sa copie piégée.

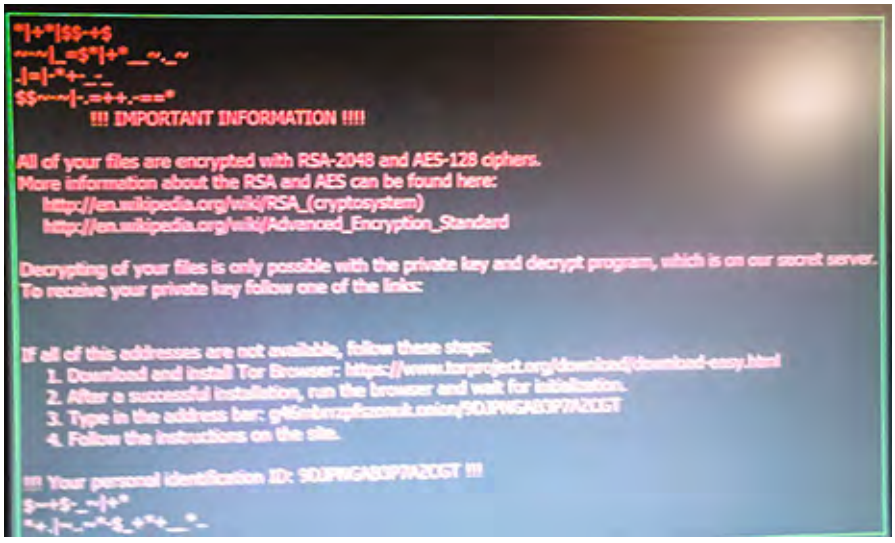
© GORODENKOFF

La faible détectabilité de l'espionnage par voie numérique le maintient dans l'ombre.

DES PONCTIONS UNITAIREMENT TOLÉRABLES, COLLECTIVEMENT CONSIDÉRABLES

Pareille pyramide explique mieux la médiatisation de quelques cas graves, voire mortels, qui forment la partie visible de l'iceberg, mais masquent la banalisation insidieuse des attaques à bas coût : logique d'acceptabilité intellectuelle d'ailleurs entretenue par les pirates, dont les rançons demandées ont un montant usuel de l'ordre de 2 000 à 3 000 euros, c'est-à-dire tolérable dans l'arbitrage qu'un entrepreneur sera tenté d'effectuer entre endosser les conséquences des pertes de données ou s'en « libérer » par rançon (libération illusoire, puisque les observations montrent la récurrence future des répliques d'attaques pour qui aura déjà été victime). Qui a payé… paiera, ou tout au moins y sera exposé sans limite de durée. Quoique ces répliques soient automatisées pour la plupart, tel cas récent chez un artisan a montré que les pirates s'étaient ménagé un accès *via* le dispositif informatique domestique de ce gérant pour revenir chiffrer à nouveau les données sur son système d'information professionnel dans les semaines suivantes.

Le coût général de ces cryptovirus commence à être cerné, malgré une omerta qui a longtemps régné çà et là : de manière cocasse et paradoxale, il ressort de nos études sur le terrain une règle empirique que plus une entreprise possède un service communication structuré, plus elle sera réticente à communiquer sur les attaques subies.



DR

Message de demande de rançon par cryptovirus (capture d'écran).

LE PRÉJUDICE NATIONAL EST DIFFICILE À CERNER

Rapporté à notre PIB national, de l'ordre de 2 100 milliards, un tel montant semblerait équivalent à 1 pour mille. Mais cette comparaison est pourtant impropre. En effet, d'une part le chiffre d'affaires qu'aura perdu telle entreprise mise à l'arrêt du fait du piratage se traduira parfois en commandes pour son concurrent (et pour son fournisseur, on se souvient d'un pirate allemand lié familialement à un petit prestataire informatique, qui espérait ainsi générer des clients demandeurs de secours), mais donc pas par une perte pour le PIB : les préjudices individuels ne s'additionnent pas pour constituer le préjudice collectif. D'autre part, ces recensements de jours de travail ou de commandes perdus, et des frais tels que de remise en route, mesurent mal les manques à gagner futurs, ceux qui résultent d'investissements annulés par l'entreprise. De même, ils ne donneront qu'une perception comptable tronquée des dégâts indirects à long terme causés par la mort d'une entreprise.

« Qui a payé… paiera ! »

Il serait plus juste de raisonner en termes de nuisance au fonctionnement économique, qui oriente trop d'investissements vers une sécurité, d'ailleurs imparfaite, plutôt que vers de l'équipement productif ; qui mobilise des temps/homme croissants au détriment d'autres tâches plus utiles, enfin qui accapare l'esprit des décideurs confrontés à ces risques.

UN CYBERIMPÔT

Voyons en tout cela un impôt, qualifiable de cyberimpôt, qui handicape l'économie, nuit aux relations interentreprises et dérentabilise en partie la numérisation de ces sociétés. Ce cyberimpôt rogne le constituant immatériel qu'est la confiance, qui permet d'ouvrir un courrier électronique sans hésitation, et avec elle la fluidité de l'activité. Cet impôt s'alourdit au fil des années, en proportion de l'augmentation des attaques, et affecte l'emploi ainsi que la dynamique des producteurs de richesses.

Si la tendance à l'aggravation se maintient, l'adage voulant que « l'impôt tue l'impôt » – hérité de Jules Dupuit (X1822) – se transformerait en « le cyberimpôt tue l'éco-

1 À 2 MILLIARDS DE DÉGÂTS POUR LES CRYPTOVIRUS

Les cryptovirus causent chez les seules entreprises de moins de 50 employés un montant de préjudice estimable à plus de 700 millions d'euros par an. Élargie à l'ensemble des entreprises, établissements publics et associations de loi 1901 françaises de toutes tailles, cette estimation aboutit à un coût de l'ordre de 2 milliards par an, en gardant à l'esprit qu'il s'agit de l'option basse des fourchettes dégagées.

LES FRAUDES « AU PRÉSIDENT »

En comparaison, les « fraudes au président » s'avèrent source de sortie de capitaux plus importantes, estimables à plus de 100 millions d'euros par an. Le ministère de l'Intérieur évoque environ 80 millions d'euros captés par an sur les dernières années, montants massivement transférés hors de France, mais reconnaît qu'il ne couvre pas tout le périmètre réel. Par leurs razzias ciblées sur les comptes bancaires des entreprises ainsi ponctionnés, de tels voleurs « propres » ne les tuent pourtant pas moins, comme en atteste une entreprise de 60 employés liquidée après avoir retrouvé ses avoirs bancaires vidés fin août – autre période prisée des pirates – en 2015.

nomie » ; d'ailleurs, les niveaux d'ores et déjà observés attestent d'un seuil intermédiaire, résumable en blessure pour l'économie, devenant mortelle pour quelques-uns.

FUITE DE CAPITAUX

Une autre matérialisation de cette ponction apparaît sous forme de sortie des capitaux : les rançons versées par les entreprises, quoique difficiles à estimer concernant les très grandes entreprises, qui répugnent à communiquer sur ces sujets sensibles pour leur image de marque, constituent pour l'essentiel des sorties de cet argent hors du territoire français. Ce racket est un tribut versé par la France. Sur ce point cependant, les torts élevés subis par l'ensemble des victimes des cryptovirus se prolongent par des sorties de capitaux quant à elles faibles. Le dégât direct général se révèle environ 35 fois supérieur à ce qu'encaissera le pirate, c'est-à-dire son « chiffre d'affaires » : ce type d'attaque casse beaucoup, saccage le patrimoine d'une société, mais récupère assez peu de butin. Ainsi, la monnaie « exfiltrée » de France par ce type d'attaque se compte en dizaines de millions d'euros, avec un plancher vraisemblable de l'ordre de 20 millions pour les entreprises de moins de 50 personnes.

Ajoutées aux « fraudes aux sentiments », très actives sur les réseaux sociaux et visant en particulier les personnes en situation de solitude, et à l'ensemble des autres types d'attaques, le flux sortant d'argent se mesure au total en centaines de millions d'euros par an, soit pour comparaison plus de 1 % du déficit de notre balance courante (de 24 milliards en 2016).

DR

Photographies utilisées par les « fraudes aux sentiments ».

VERS UNE ASPHYXIE DE L'ÉCONOMIE ?

Ces niveaux de préjudice, individuels comme collectifs, auxquels s'ajoute un *pretium doloris* lui aussi sous-estimé, alors qu'il s'agit de crises anxiogènes et déstabilisatrices, ne constituent plus un épiphénomène mais un fait central dont la présence passe de la simple gêne au handicap ou à la douleur. Toute future aggravation forte, comme la pente actuelle semble l'y conduire, conduirait à terme à une asphyxie lente du tissu économique. Certainement serait-il bon, à l'instar de ce que préconise Louis Pouzin (50), en première étape de repenser à moindre coût le fonctionnement en soi de nos réseaux de télécommunication, plutôt que de se contenter d'apposer chez l'utilisateur final des couches de sécurité onéreuses sur un substrat insécurisé. Faute de quoi, sinon, à terme le *cyberimpôt tuera cette fois le cyber*. ■

« Ce cyberimpôt rogne la confiance »

© FABIAN

Le bitcoin est la monnaie préférée des rançonneurs.