

Prise d'otage numérique par Rançongiciels, la nouvelle arme fatale des cyberpirates



Prise d'otage
numérique par
Rançongiciels,
la nouvelle arme
fatale des
cyberpirates

Les prises d'écran montrées, avec demande de rançon, se multiplient. Payer est souvent la seule solution



Lucy, Cryptolocker, Spylucker (Cryptolock), Neelacrypt, Petya. Si vous n'êtes pas un spécialiste de la sécurité informatique, ces noms barbares ne vous disent probablement rien. Et pourtant, ils représentent la nouvelle menace qui pèse sur vos ordinateurs. Depuis quelques années, en effet, un nouveau type de logiciel malveillant a le vent en poupe: les rançongiciels – un néologisme 2.0 dérivé du mot «rançonner» dans la langue de Shakespeare. Ces virus prennent, à distance, le contrôle de PC, tablettes ou smartphones et bloquent l'ensemble de leurs données. Pour les récupérer, les propriétaires légitimes sont sommés de payer une rançon dans un délai très court, dans une monnaie virtuelle et non traçable comme les bitcoins. Selon une étude d'Intel Security-RadFence, datant de mars 2016, le type d'attaque a augmenté de 30% au dernier trimestre 2015, par rapport à l'année précédente.

Les PME ne sont pas préparées

Des données de fraude après un piratage sont en plein essor dans le monde et en Suisse, résume Ilya Kolachenko, CEO et fondateur de l'entreprise genevoise High-Tech Bridge, spécialisée dans la sécurité informatique. C'est devenu une véritable industrie. De fait, les exemples se multiplient – proches de nous. En avril 2015 par exemple, Ralph Eberhard, patron de la grande Imprimeuse basée à Genève, témoigne dans le journal Le Temps avoir dû payer 1000 francs à des hackers. Le même mois, un peu plus loin d'ici, dans le Béarn, le PDG d'une entreprise raconte peu ou prou la même histoire, dans le journal La République des Pyrénées. De fait, à chaque fois le scénario est identique. Un matin, en allumant leurs ordinateurs, les salariés voient s'afficher sur leur moniteur un message terrifiant, généralement rouge sur fond noir, qui dit en substance: «Tous les fichiers de votre disque dur ont été cryptés. Pour les déchiffrer et les récupérer, vous devez nous payer.» Le compte de temps, les contacts exigés ne s'adressent pas dissimulés: de quelques centaines de francs pour des particuliers à quelques milliers pour les PME. Mais parfois, les sommes exigées sont astronomiques. En février 2016, un «ransomware» infecté un hôpital de Los Angeles, bloquant l'ensemble des données médicales des patients. Pour remettre les archives d'information d'urgence, les pirates ont réclamé 9000 bitcoins, soit l'équivalent de 1,6 milliard de dollars! «Malheureusement, les hackers s'attaquent à de grosses entreprises, afin de toucher le jackpot», rappelle Ilya Kolachenko. Aujourd'hui, ils se concentrent sur les PME et les particuliers, parce qu'ils ont compris que même si les sommes exigées sont minimes, l'activité se révèle moins risquée et plus facile. Si vous attaquez une grande banque, vous devez d'abord déjouer une sécurité informatique de premier ordre. Et si vous y parvenez, vous devez être certain qu'elle ne vous lâchera jamais. Elle vous traquera pendant des années s'il le faut. A l'inverse, les particuliers et les PME ne sont absolument pas préparés à ce type d'attaque et ne possèdent pas des moyens mécaniques pour retrouver les auteurs. Selon un rapport de Symantec publié en avril 2016, 37% de ces attaques ciblent des entreprises de moins de 200 salariés. Mais comment ces logiciels malveillants se diffusent-ils? «Les chevaux de Troie accidentés et les biais de courriels infectés ou de sites Internet piratés», explique la centrale Melani. Concrètement, «les hackers possèdent des robots informatiques, les botnets, qui scrutent l'ensemble des pages Internet – un peu comme Google – à la recherche de failles connues», explique Ilya Kolachenko. Lorsque'une vulnérabilité est découverte, le virus s'installe et attend sa victime, en affichant par exemple un nouveau lien. Lorsque quelqu'un clique sur ce dernier, le virus passe sur son ordinateur et crypte l'ensemble des données.»

Pest-il payer la rançon ou non?
Face à cette situation, la centrale Melani recommande de ne pas céder à l'extorsion car, en payant la rançon, vous participez au financement de l'activité des criminels et leur permettez d'améliorer l'efficacité de leurs prochaines attaques. De plus, il n'existe aucune garantie que les criminels respecteront leur engagement et vous enverront réellement la clé vous permettant de récupérer vos données.» En pratique, les choses s'avèrent plus compliquées, notamment pour les PME qui, privées de leurs fichiers clients, voient toute leur activité bloquée. «Si vous êtes infectés, il n'existe pas 3000 solutions», reconnaît Ilya Kolachenko. La première consiste à faire des recherches sur Internet, afin de savoir s'il existe déjà une clé de décryptage contre le rançongiciel. Malheureusement, c'est rarement le cas. La seconde, c'est payer. Si vous vous adressez à une entreprise comme la nôtre, nous finirons par remonter jusqu'au coupable et nous parviendrons peut-être à récupérer vos données. Mais cela va prendre beaucoup de temps. Même si cela peut paraître absurde, c'est moins coûteux pour une PME de régler la rançon que de lancer des investigations.» (TDC)

«Lire la suite»



Ilya Kolachenko, CEO et fondateur de l'entreprise genevoise High-Tech Bridge, spécialisée dans la sécurité informatique. C'est devenu une véritable industrie. De fait, les exemples se multiplient – proches de nous. En avril 2015 par exemple, Ralph Eberhard, patron de la grande Imprimeuse basée à Genève, témoigne dans le journal Le Temps avoir dû payer 1000 francs à des hackers. Le même mois, un peu plus loin d'ici, dans le Béarn, le PDG d'une entreprise raconte peu ou prou la même histoire, dans le journal La République des Pyrénées. De fait, à chaque fois le scénario est identique. Un matin, en allumant leurs ordinateurs, les salariés voient s'afficher sur leur moniteur un message terrifiant, généralement rouge sur fond noir, qui dit en substance: «Tous les fichiers de votre disque dur ont été cryptés. Pour les déchiffrer et les récupérer, vous devez nous payer.» Le compte de temps, les contacts exigés ne s'adressent pas dissimulés: de quelques centaines de francs pour des particuliers à quelques milliers pour les PME. Mais parfois, les sommes exigées sont astronomiques. En février 2016, un «ransomware» infecté un hôpital de Los Angeles, bloquant l'ensemble des données médicales des patients. Pour remettre les archives d'information d'urgence, les pirates ont réclamé 9000 bitcoins, soit l'équivalent de 1,6 milliard de dollars! «Malheureusement, les hackers s'attaquent à de grosses entreprises, afin de toucher le jackpot», rappelle Ilya Kolachenko. Aujourd'hui, ils se concentrent sur les PME et les particuliers, parce qu'ils ont compris que même si les sommes exigées sont minimes, l'activité se révèle moins risquée et plus facile. Si vous attaquez une grande banque, vous devez d'abord déjouer une sécurité informatique de premier ordre. Et si vous y parvenez, vous devez être certain qu'elle ne vous lâchera jamais. Elle vous traquera pendant des années s'il le faut. A l'inverse, les particuliers et les PME ne sont absolument pas préparés à ce type d'attaque et ne possèdent pas des moyens mécaniques pour retrouver les auteurs. Selon un rapport de Symantec publié en avril 2016, 37% de ces attaques ciblent des entreprises de moins de 200 salariés. Mais comment ces logiciels malveillants se diffusent-ils? «Les chevaux de Troie accidentés et les biais de courriels infectés ou de sites Internet piratés», explique la centrale Melani. Concrètement, «les hackers possèdent des robots informatiques, les botnets, qui scrutent l'ensemble des pages Internet – un peu comme Google – à la recherche de failles connues», explique Ilya Kolachenko. Lorsque'une vulnérabilité est découverte, le virus s'installe et attend sa victime, en affichant par exemple un nouveau lien. Lorsque quelqu'un clique sur ce dernier, le virus passe sur son ordinateur et crypte l'ensemble des données.»

Le Net Expert
INFORMATIQUE
MAGAZINE & CEST ARTICILE

Source : Sécurité informatique: Rançongiciels, la nouvelle arme fatale des cyberpirates – News High-Tech: Hard-/Software – tdg.ch