

Les cyberattaques ne cessent de se multiplier

INFORMATIQUE Les «ransomwares» sont l'une des menaces qui mobilisent actuellement le plus de moyens autour de la planète

Difficile, voire impossible, d'établir un catalogue exhaustif des menaces qui planent aujourd'hui dans le cyberspace, tant elles évoluent sans cesse, changeant même souvent de forme. Chacune des initiatives lancées à Lausanne, Genève ou Paris tente de lutter contre un ou plusieurs de ces fléaux, dont voici un aperçu.

1 Les «ransomwares»

C'est le type d'attaque le plus virulent qui frappe particuliers, entreprises, administrations et hôpitaux. Le principe est simple: les pirates informatiques parviennent à infecter un ordinateur, par exemple via une pièce jointe glissée dans un e-mail. Ensuite, toutes les machines connectées du réseau sont à leur tour touchées. L'attaquant parvient à bloquer l'accès à ces ordinateurs, qui deviennent inutilisables. Il exige ensuite un rançon pour rendre l'accès à ces machines et parvient aussi parfois à voler des données. Il y a eu bien sûr le précédent WannaCry en 2017, qui a infecté des dizaines de milliers de PC. Ces derniers mois, de très nombreux hôpitaux et PME, voire des multinationales, ont été affectés.

2 Le «phishing»

Phénomène ancien, le «phishing» fait toujours des ravages. De très nombreux internautes continuent à se faire avoir par des e-mails qui semblent avoir été envoyés par Goo-

gle, Netflix ou Swisscom et qui exigent des données complètes. Des données ensuite facilement exploitées par des pirates.

3 Les attaques entre États

On sait très peu de choses de ces attaques, dont ni les victimes ni les agresseurs ne font la publicité. Mais régulièrement, des États, souvent cachés derrière des groupes de hackers à leur solde, tentent de paralyser en partie des États ou des infrastructures vitales de certains pays. La Russie, la Chine et la Corée du Nord sont souvent citées. Mais en parallèle, tous les États occidentaux se livrent à des activités d'espionnage.

4 Les vols de données

Plus une semaine ne se passe sans qu'un vol massif de données n'intervienne, que ce soit chez des géants du web, des sites de rencontre ou érotiques ou même des institutions financières. Très souvent, ces données, d'une grande valeur, se retrouvent plus tard en libre accès, permettant à leurs propriétaires de procéder à de nouvelles attaques.

5 Les discours extrémistes

C'est une catégorie un peu à part, qui touche tous les internautes. Les discours de haine, les contenus violents, le cyberharcèlement, les contenus terroristes sont autant de problèmes qui peuvent toucher tout le monde, et pour lesquels les géants de la tech ont une grande part de responsabilité. ■ A. S.

MAIS ENCORE

Les groupes étatiques, la menace la plus forte

Fin 2019, les groupes français Thales et israélien Verint publiaient un annuaire mondial des groupes de pirates informatiques les plus menaçants. Sur les 66 groupes d'attaquants de haut niveau, 49% sont considérés d'origine étatique ou soutenus par un État. Dans le reste des groupes, 26% sont des «hacktivistes», des militants motivés par des idéologies communautaires, religieuses, politiques.

Vingt pour cent sont des cybercriminels, motivés par l'appât du gain, 5% des cyberterroristes

2,7 milliards

Les cyberattaques ne cessent de se multiplier

INFORMATIQUE Les «ransomwares» sont l'une des menaces qui mobilisent actuellement le plus de moyens autour de la planète

Difficile, voire impossible, d'établir un catalogue exhaustif des menaces qui planent aujourd'hui dans le cyberspace, tant elles évoluent sans cesse, changeant même souvent de forme. Chacune des initiatives lancées à Lausanne, Genève ou Paris tente de lutter contre un ou plusieurs de ces fléaux, dont voici un aperçu.

1 Les «ransomwares»

C'est le type d'attaque le plus virulent qui frappe particuliers, entreprises, administrations et hôpitaux. Le principe est simple: les pirates informatiques parviennent à infecter un ordinateur, par exemple via une pièce jointe glissée dans un e-mail. Ensuite, toutes les machines connectées du réseau sont à leur tour touchées. L'attaquant parvient à bloquer l'accès à ces ordinateurs, qui deviennent inutilisables. Il exige ensuite une rançon pour rendre l'accès à ces machines et parvient aussi parfois à voler des données. Il y a eu bien sûr le précédent WannaCry en 2017, qui a infecté des dizaines de milliers de PC. Ces derniers mois, de très nombreux hôpitaux et PME, voire des multinationales, ont été affectés.

2 Le «phishing»

Phénomène ancien, le «phishing» fait toujours des ravages. De très nombreux internautes continuent à se faire avoir par des e-mails qui semblent avoir été envoyés par Goo-

gle, Netflix ou Swisscom et qui exigent des données complètes. Des données ensuite facilement exploitées par des pirates.

3 Les attaques entre États

On sait très peu de choses de ces attaques, dont ni les victimes ni les agresseurs ne font la publicité. Mais régulièrement, des États, souvent cachés derrière des groupes de hackers à leur solde, tentent de paralyser en partie des États ou des infrastructures vitales de certains pays. La Russie, la Chine et la Corée du Nord sont souvent citées. Mais en parallèle, tous les États occidentaux se livrent à des activités d'espionnage.

4 Les vols de données

Plus une semaine ne se passe sans qu'un vol massif de données n'intervienne, que ce soit chez des géants du web, des sites de rencontre ou érotiques ou même des institutions financières. Très souvent, ces données, d'une grande valeur, se retrouvent plus tard en libre accès, permettant à leurs propriétaires de procéder à de nouvelles attaques.

5 Les discours extrémistes

C'est une catégorie un peu à part, qui touche tous les internautes. Les discours de haine, les contenus violents, le cyberharcèlement, les contenus terroristes sont autant de problèmes qui peuvent toucher tout le monde, et pour lesquels les géants de la tech ont une grande part de responsabilité. ■ A. S.

MAIS ENCORE

Les groupes étatiques, la menace la plus forte

Fin 2019, les groupes français Thales et israélien Verint publiaient un annuaire mondial des groupes de pirates informatiques les plus menaçants. Sur les 66 groupes d'attaquants de haut niveau, 49% sont considérés d'origine étatique ou soutenus par un État. Dans le reste des groupes, 26% sont des «hacktivistes», des militants motivés par des idéologies communautaires, religieuses, politiques.

Vingt pour cent sont des cybercriminels, motivés par l'appât du gain.

2,7 milliard