Une vague d'attaques de logiciels de rançon frappe des sociétés suisses trop vulnérables

LES PME PRISES EN OTAGES

« THIERRY JACOLET

Les Transports publics fribourgeois (TPF) ont aussi été frappés par un virus de rançon la semaine passée, par chance sans réel impact sur l'activité. Charles Ellena-archives

Virus » «Notre entreprise a été victime d'une *ransomware* Attack-RYK et infectée par un virus et ce malgré nos systèmes de protection et pare-feu des plus efficaces et actuels.» C'est par courrier que Bourquin SA a averti ses clients et partenaires au mois de juin qu'elle venait d'être victime d'un logiciel de rançon ukrainien. Impossible d'utiliser les serveurs: le virus les a mis hors service, paralysant une partie de l'activité. Comme cette société de cartonnage basée à Val-de-Travers (NE), les PME sont des proies vulnérables pour les cybercriminels spécialisés dans la prise d'otage de données d'entreprises.

«Ce phénomène a lieu depuis 3 ou 4 ans», confirme Max Klaus, responsable adjoint de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) au niveau fédéral, sans pouvoir donner de statistiques. «Mais nous observons ces dernières semaines des vagues d'attaques contre les entreprises.» Ces logiciels de rançon baptisés CryptoWall, Locky ou Samsam sont devenus le cauchemar des patrons. Et ils sont actuellement 1755 à rôder en ligne autour des sociétés à la recherche d'une faille dans les murs de protection…

1 Pourquoi les PME sont une proie facile?

Steven Meyer mesure quotidiennement cette flambée d'attaques au sein de l'entreprise de cybersécurité ZENData qu'il dirige à Genève et qui est toujours plus sollicitée. «En ce moment, les *ransomware* sont très actifs et couvrent la grande masse des cyberattaques», témoigne-t-il. «Ceux qui refusent d'investir dans la cybersécurité de nos jours prennent un gros risque pour leur société.» Un antivirus, système de pare-feu et autres mesures de protection à la pointe ne garantissent pas le risque zéro face aux 300 000 nouveaux virus créés par jour. «Si l'antivirus bloque 99% des virus, il en reste encore 3000 qu'il ne reconnaîtra pas», prévient le directeur. D'où l'intérêt d'un renfort via une entreprise spécialisée dans la surveillance et la détection des nouveaux risques.

«Les PME artisanales sont souvent mal préparées à ce type d'attaques», estime Stéphane Koch, consultant indépendant dans le domaine de la sécurité de l'information et vice-président d'ImmuniWeb SA. «La majorité des sociétés n'a pas de plan B. Et même si elles investissent pour diminuer le risque, le maillon faible est souvent humain.»

2 Comment procèdent les cybercriminels?

La plupart des attaques de logiciels de rançon ont lieu par courriels qui font office d'hameçons. «Les cybercriminels envoient des e-mails à des milliers d'adresses et s'il y a une faille, le virus pénètre dans le système», détaille Max Klaus. Ils ont toutefois tendance à cibler les cadres et dirigeants d'entreprises susceptibles de payer de grosses sommes ou parce que leurs adresses e-mails sont visibles sur le Net.

Il suffit d'un clic sur le document pour libérer la bête qui va crypter les données

C'est le cas de Bourquin SA: les malfrats ont usurpé l'adresse de hauts responsables pour arroser les collaborateurs d'e-mails contenant des virus en attachement. Il suffit d'un clic sur le document pour libérer la bête qui va crypter les données, la sauvegarde (ou back-up) et les serveurs auxquels l'ordinateur infecté est relié. Le système informatique est verrouillé tant que la rançon n'est pas payée.

3 Quelle est l'étendue des dégâts?

Des logiciels de rançon encore plus vicieux s'infiltrent en toute discrétion dans le serveur de la PME sans lâcher le virus. Ils attendent des semaines pour mieux cibler leurs proies et lancer l'offensive. A Fribourg, ce modus operandi a failli coûter cher à l'entreprise fusionnée des imprimeries Sensia et Canisius.

«Quand nous avons voulu utiliser les back-up après l'attaque, nous avons remarqué qu'ils étaient aussi infectés par le virus», confie Beat Schultheiss, membre de la direction. «Il était dans le système depuis quelques semaines! Tout l'administratif a été perdu.» Les Transports publics fribourgeois (TPF) ont aussi été frappés par un virus à retardement vraisemblablement d'origine nord-coréenne la semaine passée sans réel impact sur l'activité.

Serveurs hors de combat, perte de chiffres d'affaires, réparations coûteuses, réputation écornée… «Les dommages peuvent mettre en péril l'existence des PME», assure Stéphane Koch. Rien que la facture de l'intervention d'urgence est déjà salée. «Il peut y en avoir pour 10 000 francs juste en frais de réparation entre les restaurations, le nettoyage du système et la vérification du système pour une PME d'une dizaine d'ordinateurs», évalue Steven Meyer. Bourquin SA a pu limiter les dégâts grâce à des spécialistes informatiques externes qui ont rétabli en quelques jours la situation.

4 Comment éviter ces attaques?

Les cybercriminels ont toujours un coup d'avance avec leurs logiciels de rançon. C'est pourquoi l'équipement de défense des PME doit être à la hauteur de la menace virale qui enfle d'année en année. «Un système de protection efficace ne suffit plus», avertit Stéphane Koch. «La formation des employés (dont le CEO), une stratégie de sauvegardes multiples de données hors connexion internet, savoir qui appeler en cas de problème, et un plan de communication de crise, sont devenus des éléments indissociables de la transformation numérique de notre société.»

Bourquin SA a non seulement joué la transparence avec ses clients et partenaires, mais aussi décidé de renforcer la sensibilisation et la formation de son personnel à ces menaces. «Cela doit faire partie de nos priorités, tout comme l'analyse régulière de la gestion des risques avec un système plus actualisé», affirme Cynthia Uelligger, directrice des ventes et responsable du site de Couvet. «Malgré les mesures prises, il y aura toujours une impression de grande vulnérabilité…» »

TROIS QUESTIONS À STÉPHANE KOCH

STÉPHANE KOCH
Consultant indépendant en sécurité de l'information

La Suisse est-elle à la hauteur de la menace des virus malveillants?
Non. D'abord, parce qu'il manque une réelle culture du numérique en Suisse. Nous sommes encore dans des actions de prévention en Suisse et non dans l'éducation à une transformation numérique, qui s'intègre dans les matières scolaires de manière pédagogique. Il y a clairement un manque de réactivité et de connaissance. La Confédération a tardé à mettre en place une unité de coordination contre la cybercriminalité. Si nous comparons avec les moyens mis en place en France pour aider les entreprises, il n'y a pas photo.

Qu'attendez-vous des autorités fédérales?
Plus de moyens alloués en Suisse pour éduquer les citoyens et les entreprises face aux cyberrisques. Le manque de conscience politique est flagrant. Par exemple la réforme de la loi fédérale sur la protection des données (LPD) n'aboutira pas avant fin 2019, alors qu'elle était prévue pour août 2018. De plus cette «nouvelle» loi risque d'être obsolète par rapport au Règlement européen sur la protection des données (RGPD). Ce genre de situation démontre bien un certain laxisme et une forme d'illettrisme numérique au niveau politique. Pour avoir une vision effective de la situation et de l'impact économique réel de la cybercriminalité en Suisse, il faudrait créer un index économique de la cybersécurité. Car c'est d'abord un problème économique.

A quoi servirait un tel index?
Il recenserait l'ensemble des attaques informatiques dont les entreprises et les particuliers sont victimes, les coûts directs et indirects qu'elles ont engendrés. Le nombre de cas traités par les unités de lutte contre la cybercriminalité et le système judiciaire. Et combien de cas annoncés ont abouti à une condamnation. Ces données une fois compilées, donneraient une vision réaliste de la manière dont notre pays appréhende la transformation numérique. » TJ

LE CRIME ORGANISÉ DERRIÈRE LES VIRUS

Pas besoin d'être expert en cryptographie ou en piratage pour pouvoir s'enrichir dans cette nouvelle industrie criminelle. Envoyer des virus aux quatre coins de la planète est un jeu d'enfant. Les cybercriminels biffent les frontières et ne sont pas actifs sur le terrain. «Ils enlèvent le facteur humain et matériel qui leur ferait courir un risque énorme», explique Steven Meyer, directeur de l'entreprise de cybersécurité ZENData. «Comme c'est très rentable, le crime organisé s'est spécialisé dans les *ransomware* (logiciels de rançon, ndlr). Il investit beaucoup là-dedans.» Une activité à part entière qui lui rapporterait plus que la drogue et la prostitution. Le virus Ryuk, qui a attaqué la semaine passée les Transports publics fribourgeois (TPF) tout comme les services de justice de l'Etat américain de Géorgie, aurait rapporté près de 3,7 millions de dollars rien qu'entre août 2018 et janvier 2019.

En Suisse, le montant de la rançon tient dans une fourchette de 600 à 5000 francs pour une petite PME jusqu'à des centaines de milliers de francs pour une grande boîte. Celles qui passent à la caisse le font en bitcoin, une cryptomonnaie qui permet d'éviter tout traçage. Aucune des PME contactées n'a cédé au chantage, parce qu'elles pouvaient compter sur de récentes sauvegardes des données. La Confédération recommande d'ailleurs de ne pas payer la rançon qui ne ferait qu'alimenter la force de frappe de ces malfrats qui sévissent en Suisse depuis l'Afrique centrale, les pays de l'Est et l'Asie. TJ