Communiqué de presse

Le coût additionné des attaques par cryptovirus touchant les PME françaises s'élève à plus de 700 millions d'euros par an

L'enquête terrain inédite menée par l'IRT SystemX auprès de PME et TPE françaises, victimes de cyberattaques, dévoile l'impact réel des cyber-préjudices et fait voler en éclats deux grandes croyances communément admises : le nombre de cyberattaques réussies s'avère bien supérieur aux estimations habituellement rendues publiques, tandis que le coût moyen des cyberattaques se révèle en revanche beaucoup plus faible que supposé. Zoom sur les 9 principaux enseignements de cette étude, dévoilés à l'occasion de la conférence « Cyber-Préjudices : au-délà des idées reçues » organisée par l'IRT SystemX, la Fédération Française de l'Assurance et la Chaire Cyber Insurance, ce 25 juin.

Palaiseau, le 25 juin 2019 – SystemX, unique IRT dédié à l'ingénierie numérique des systèmes du futur, dévoile les principaux enseignements de sa première enquête terrain menée sur 3 ans* auprès de plus de 60 entreprises françaises**, principalement des PME/TPE de moins de 50 personnes, victimes de cyberattaques. Toutes les régions et secteurs economiques sont représentés. L'objectif de cette enquête était de **mesurer les préjudices causés au tissu économique**, puis d'élaborer des modèles de calcul des coûts ainsi que de l'exposition d'une entreprise au risque Elle a également permis de collecter des signaux faibles, annonciateurs de nouvelles tendances, et notamment d'évolutions à attendre sur le mode opératoire de certaines formes d'attaques

Parmi les catégories d'attaques étudiées, l**e rançonnage par cryptovirus et les fraudes au président et faux ordres de virement** prennent la plus grande place. Ont également été rencontrées : l'escroquerie au faux support technique, la prise de contrôle de messagerie, le piratage téléphonique, la fraude aux sentiments, l'usurpation d'identité, la mauvaise protection des caméras, la captation de nom de domaine, le défaçage ou encore le vol de compte bancaire. A noter **la grande rareté des attaques DDos par déni de service contre des PME**, ce qui constitue l'un des résultats inattendus de cette enquête et confirme que ce type d'attaque résulte avant tout d'un ciblage intentionné de la part d'un tiers.

« *Cette enquête terrain est inédite en France : elle transmet une vision profondément renouvelée des attaques informatiques notamment grâce à une précision des chiffres jamais atteinte. Initiée dans le cadre du projet EIC (Environnement pour l'Interopérabilité et l'Intégration en Cybersécurité), elle remet en cause les chiffrages habituels, ce qui modifie la vision à porter sur le cyber-risque* », explique Gilles Desoblin, Responsable de la thématique Défense et Sécurité, IRT SystemX.

Parmi les principaux enseignements de cette enquête :

- **La fréquence des attaques réussies en matière de cryptovirus est plus haute que supposée jusqu'alors** : pour une PME de moins de 50 salariés, la probabilité d'être victime ne se mesure annuellement plus en *pour mille* mais en *pour cent*, se situant entre **2 et 5%** (soit entre 100 000 et 250 000 entités par an). Elles ne se situent donc plus dans la catégorie des événements rares.

- **Le coût moyen d'une attaque par cryptovirus est inférieur à ce qu'il est généralement communiqué via les médias :** en effet, le coût moyen pour une TPE s'évalue actuellement en milliers d'euros par attaque réussie, en non en dizaines, centaines voire en millions d'euros. A noter que la progression des coûts n'est pas proportionnée seulement à celle de la taille d'une entreprise, mais dépend d'autres facteurs parfois inattendus tels que le mode de gestion des ressources humaines .

- **La médiane constatée (de l'ordre du millier d'euros) est basse et se situe nettement au-dessous de la moyenne**, ce qui signifie qu'un grand nombre d'attaques réussies trouvent des solutions à faible prix, particulièrement quand les sauvegardes ne sont pas affectées.

- Toujours concernant les cryptovirus, **les coûts additionnés subis** par l'ensemble des victimes de moins de 50 employés – entreprises ou associations – en France s'élèvent à un montant supérieur à **700 millions d'euros par an**.

- Dans cette observation de transfert de richesse, **le gain enregistré par les pirates déroge à l'image communément admise**. La sortie de capitaux, due conjointement aux cryptovirus et aux fraudes aux président – soit plus de 200 millions d'euros -, masque des modèles économiques très différents entre ces formes de criminalité. Les calculs réalisés au sujet des cryptovirus font ressortir **un ratio entre l'argent rançonné (sommes versées) et le préjudice total de l'ordre de 1/25 chez les PME/TPE**. A contrario, les fraudes au président, malgré leur recours accentué à des acteurs humains et à l'ingénierie sociale, laissent entrevoir des marges finales plus élevées.

- L'étude dévoile également **la sous-estimation du préjudice humain occasionné par ces attaques** (fragilisation des personnes, perte de cohésion de groupe), avec la nécessité d'assister les décideurs pendant cette phase où ils doivent mener des arbitrages en situation de forte incertitude.

- A contrario, **le préjudice sur l'image des entreprises touchées est surestimé**, puisqu'il est souvent superficiel et passager, sauf si cela coïncide avec un temps fort de la société (lancement de nouveau produit ou événement-jalon important).

- Si **les relations entre entreprises partenaires se sont confirmées être l'une des principales failles en cas d'attaque et de leurre**, par exemple en matière de rançonnage avec des courriers du type « facture modifée » ou de fausses adresses bancaires (FOVI), l'observation plus fouillée fait ressortir qu'une partie très importante des coûts d'attaque provient de **la déficience d'acteurs de l'écosystème** de l'entreprise : prestataire ou éditeur informatique, opérateur télécom, fournisseur de messagerie, électricien, banquier, etc. Il est apparu que ces déficiences ou le manque de réactivité de nombre de ces acteurs alimentent le risque dans des proportions au moins comparables à celles engendrées par les déficiences internes.

- Enfin, contrairement à l'image d'une sécurité informatique qui s'obtiendrait par de forts investissements, l'étude souligne que la majorité des préjudices observés aurait pu être évitée ou atténuée par des modes de protection à coût modeste, et par une série de bonnes pratiques accessibles à la plupart des entreprises.

« *Ce travail terrain a également permis de relever l'évolution du paysage général, puisque nous sommes passés en quelques années d'une époque où les entreprises se découvraient exposées, à aujourd'hui où elle se savent désormais visées mais se croient protégées. Beaucoup de victimes ont fait part de leur surprise lors d'une attaque car de bonne foi, elles pensaient avoir déployé des protections suffisantes. L'ignorance principale ne tient plus en une sous-estimation des attaques mais en une surestimation des défenses* », explique Philippe Laurier, chercheur, spécialiste des questions d'intelligence économique, IRT SystemX et en charge de cette enquête.

*Réalisée entre 2016 et 2019
** Entreprises invididuelles, TPE et PME de moins de 50 personnes et secteur associatif

À propos de l'IRT SystemX

Créé en 2013 dans le cadre du programme des investissements d'avenir, l'Institut de Recherche Technologique SystemX se positionne comme un accélérateur de la transformation numérique de l'Industrie, des services et des territoires. Dans le cadre de sa feuille de route 2019-2025, l'IRT s'est fixé trois principales missions : accélérer l'usage des technologies pour la création de valeur, renforcer les capacités R&D collaboratives des entreprises et stimuler la production de connaissances de l'écosystème académique autour de défis scientifiques majeurs.

Centrés sur l'ingénierie numérique des systèmes du futur, ses travaux de recherche couvrent les enjeux de 4 secteurs applicatifs prioritaires : Mobilité et Transport autonome, Industrie du futur, Défense et Sécurité, Environnement et Développement durable. Ses domaines scientifiques et techniques sont au nombre de 8 : Science des données et IA ; Interaction homme-machine ; Calcul scientifique ; Optimisation ; Ingénierie système et conception logicielle ; Sûreté de fonctionnement des systèmes critiques ; Sécurité numérique et blockchain ; IoT et réseaux du futur. L'ensemble des cas d'usage et projets menés par l'IRT se situent au croisement de ces secteurs applicatifs et domaines scientifiques et techniques et s'appuient sur une ou plusieurs plateformes technologiques développées au sein de l'institut. Basé sur le plateau de Paris-Saclay, Lyon et Singapour, SystemX a lancé depuis sa création en 2012, 36 projets de recherche (dont 24 en cours), impliquant une centaine de partenaires économiques et 32 laboratoires académiques, et compte 350 collaborateurs dont 140 ressources propres.

Contacts presse

Marion Molina – Claire Flin
Tél. 06 29 11 52 08 / 06 95 41 95 90
marionmolinapro@gmail.com / clairefline@gmail.com