Toulouse, 15 mai

MANIFESTE DE « RESISTANCE CYBER », collectif spontané regroupant chefs d'entreprise en cybersécurité, responsables et représentants de clubs, associations, clusters, référents cyber, journalistes, référents du domaine numérique.

La menace est devenue réalité … aux yeux de tous et toutes

Une réalité d'envergure puisqu'un grand nombre d'entreprises viennent d'être impactées par le cryptolocker Wanacry(pto).
La propagation est actuellement contenue.
Les impacts sont en cours d'évaluation, leurs conséquences se trouveraient fondamentales pour les hôpitaux, banques et industries.
L'origine de l'attaque est inconnue et laisse penser à une action criminelle même si la source profonde pourrait être étatique.
Si l'attaque, elle-même, n'est pas complexe, elle utilise des failles de sécurité existantes depuis mars 2017.
Les systèmes d'information et les outils de protections étant, notamment, rendus obsolètes par le comportement du Malware.
Cette attaque fait échos aux attaques récentes assez semblables au piratage des mails de Hilary Clinton, l'attaque contre TV5 monde, et à l'espionnage des messageries de candidats à l'élection présidentielle française.

En quelques mots : nous venons d'échapper à une véritable catastrophe.

Et cela, grâce à un chercheur anglais qui a réussi en 2 jours à trouver le « bouton de désactivation » de l'attaque.
Un « coup de génie » mais dont le paramètre aléatoire ne peut se voir considéré.
Les effets auraient pu être destructeurs si des infrastructures vitales avaient été touchées : aéroport, contrôle aérien, gares, centrales nucléaires, …

Tous types d'entreprises et institutions ont été touchés.

Même les grands groupes, sensés être rodés à ce genre de menaces, n'ont rien anticipé.

Nous, experts, estimons, sans nul doute, que cette attaque n'est que le prémisse d'une opération de plus grande envergure.

Celle qui consisterait à paralyser une activité économique ou à dérober des données sensibles au fonctionnement de tout un pan, à minima, de nos industries et de notre production.

Ces menaces nouvelles (même si elles existent depuis plusieurs années sous d'autres formes) se sont professionnalisées et utilisent des techniques qui ne sont plus décelées par les protections actuelles.
Cette situation s'explique par un décalage essentiel entre les capacités de détection et les techniques d'attaques élaborées.
Il faut en faire constat :
Nous avons laissé la main aux professionnels de l'attaque par notre conservatisme et nos doctrines défensives dépassées et des entreprises de sécurité obnubilées par des intérêts économiques maintenant d'un autre âge.
Les nouvelles techniques d'attaque utilisent des méthodes de dissimulation contre lesquelles une doctrine de protection périmétrique ne peut rien.
Les solutions sont simples mais les outils obsolètes...
Des outils dépassés (1), des attaques ciblées (2), des alertes en trop grand nombre (3) constituent les 3 éléments qui font que les entreprises seront de plus en plus dépassées et attaquées.

Les entreprises doivent changer leur modèle de protection et de détection.
Avec peu de moyens et quelques bonnes pratiques les attaques Wanacry auraient pu être évitées.

Ce type d'attaque cyber se développe rapidement en raison de 3 enjeux économiques :
- La professionnalisation des attaquants qui perçoivent des revenus conséquents en volant ou bloquant des entreprises,
- La récupération de données personnelles ou d'entreprises constitue le moteur de la guerre économique que se livrent les grands groupes numériques. Quand un produit est gratuit c'est que « Vous êtes le produit ». En substance, l'enjeu se trouve être la collecte de données pouvant être valorisées. Les pirates l'ont, eux, bien compris.
- Le manque de moyens et de ressources des entreprises qui doivent faire face aux enjeux de la transition numérique et voient arriver de nouveaux risques inconnus ! Particulièrement dans les secteurs à risques (santé, industrie, finance et assurances) et les startups/TPE/PME.

L'enjeu du sujet est, de toute évidence, colossal.

La conservation d'une avance technologique, la protection de nos données personnelles ou privées, la préservation des emplois d'aujourd'hui et ceux des générations à venir, est au cœur du sujet.
Les entreprises et collectivités comprennent de plus en plus l'enjeu mais les investissements restent très insuffisants.
Le peu de budgets dépensés sur ces sujets restent d'ailleurs dédiés à l'achat de solutions non souveraines qui remettrons en jeu notre capacité de maîtrise sur nos données personnelles.

Nous en appelons à toutes les volontés et consciences, aux professionnels, aux directeurs informatiques, aux dirigeants, aux politiques.
Nous devons mettre en place des solutions fortes.

La réalité dépasse aujourd'hui le meilleur des films de science fiction et les enjeux deviennent de l'ordre de la sécurité publique et du niveau d'un état d'urgence.
Nous pesons nos mots.

Ne pas agir, ne pas réagir, serait acquiescer devant un terrorisme informatique à l'égal de tous les terrorismes : froid et brutal, sans mesure, sans loi, …et difficilement punissable.
Protéger nos données, protéger nos productions … pour protéger nos emplois, nos ressources, notre innovation, notre avenir en fait.
Laisser faire est compromettre notre Nation.

Nous proposons et demandons la mise en place, sans perte de temps :

- D'un crédit d'impôt sécurité pour PME/ETI, visant à financer par de outils souverain la protection du patrimoine informationnel des entreprises ;
- La stimulation d'une offre de sécurisation des PME, des ETI et des universités, écoles, établissements de Santé, collectivités locales… ;
- La mise en place d'une plate forme de réponse à incident pour les PME/ETI ;
- Le regroupement des entreprises innovantes autour de technologies d'avenir comme l'Intelligence Artificielle et les techniques de bigdata ;
- L'émergence d'une offre de sécurité pour les fournisseurs d'OIV, qui peuvent représenter un danger pour les donneurs d'ordre,
- L'émergence d'une offre de cyber assurance,
- L'émergence d'un catalogue de produits de confiance adaptés aux PME.
- La mise place de plateformes de tests qualificatifs de solutions afin de permettre aux entreprises de délivrer des produits certifiés de qualité qui ne présentent pas de failles de sécurité qui pourraient être exploitées,
- La formation à la bonne pratique du web dans les écoles ;
- L'ouverture de formations d'ingénierie à la cybersécurité.

Pour faire face, nous avons le choix …
Le choix de soutenir une position conservatrice et archaïque, seulement défensive et réservée à quelques uns, d'une conception dépassée de notre industrie ou de favoriser l'émergence de solutions nouvelles et innovantes.

Nous appelons les chefs d'entreprises et décideurs à nous rejoindre pour faire face et proposer des solutions concrètes.

Le terrorisme informatique n'aura pas de prise sur notre volonté de faire gagner la France !

Les tous premiers Signataires de ce manifeste sont :

Jean-Nicolas Piotrowski,
Président d'ITrust, Président du ThinkTank Cybersécurité PRISSM
Daniel Benchimol,
Président du cluster Digital Place, Entrepreneur
Damien Bancal,
Zataz, influenceur, blogueur
Luc Marta de Andrade,
Président de Uneed, Président du Think Tank NUX (Next Humanity)
Clément Saad,
Président de Pradéo, Représentant Frenchtech Montpellier
Marc Brami,
Directeur de GSMag, Journaliste
Ely de Travesco,
Président de Phonesec, Bugbountyzone
Philippe Coste,
Head Of Innovation Operation Epitech

Ils se regroupent sous le nom « Resistance Cyber ».