Le courrier électronique, outil de collaboration ou arme de destruction massive ?

Loïc GUEZO
Directeur Stratégie Cybersécurité SEMEA, Proofpoint
Secrétaire général, CLUSIF
Référent Cybermenaces, DCPJ/SDLC, Police Nationale

En 1971, l'ingénieur américain Ray Tomlinson envoyait le tout premier courrier électronique de l'histoire entre 2 ordinateurs, créant ainsi les prémisses d'une nouvelle forme de communication directe entre les usagers.
Pouvait-il prédire que 50 ans plus tard, ce canal serait empreint d'une dualité si forte, réussissant l'exploit d'être non seulement le canal de communication le plus utilisé mais aussi le principal vecteur de cybermenaces dans nos vies ?

Présenté il y a quelques années comme une nouvelle forme de pollution informationnelle synonyme de baisse de productivité[1], voire condamné à l'aube des réseaux collaboratifs, le courrier électronique n'est pourtant pas mort. Celui que l'on appelle communément le courriel (ou email en anglais) est même aujourd'hui le principal canal de communication numérique dans le monde, avec quatre milliards d'usagers qui font transiter plus de 300 milliards de courriers électroniques chaque jour[2], dont près de la moitié dans le cadre professionnel.

L'histoire du courriel commence dans les années 1960 avec ARPANET, l'ancêtre d'Internet appartenant à l'époque au ministère américain de la défense. Les ingénieurs travaillant sur ce réseau pouvaient déjà laisser des notes sur leurs études dans des boîtes aux lettres électroniques, hébergées sur un ordinateur. Mais c'est en 1971 que Ray Tomlinson[3] a imaginé une forme de communication plus directe en envoyant des messages d'un ordinateur à un autre, utilisant le caractère @ comme séparateur ... L'email était né.

Un temps utilisé dans les universités, les administrations publiques et pour les communications en entreprise, l'email est réellement devenu populaire dans les années 1990, avec le lancement du premier service gratuit basé sur le web (HTML). Après le premier WebMail du CERN lancé en 1994, le désormais

[1] https://www.capital.fr/votre-carriere/pour-etre-plus-productives-ces-entreprises-ont-interdit-le-mail-1301802

[2] https://www.radicati.com/wp/wp-content/uploads/2018/12/Email-Statistics-Report-2019-2023-Executive-Summary.pdf

[3] https://youtu.be/XhXk3wzemR4

incontournable service Gmail fut créé en 2004. Depuis, le courrier électronique n'a eu de cesse de s'imposer comme un allié essentiel des entreprises, plébiscité non seulement pour sa simplicité, son agilité et son accessibilité mais aussi pour sa formidable capacité à toucher une large audience de manière immédiate. Mais à mesure que l'email devenait plus accessible au public, les entreprises ont poussé le concept un peu loin, allant parfois jusqu'à saturer les destinataires.

Fléau du spam et épidémie de virus informatiques

Le premier courrier électronique non sollicité, dit spam, arrive assez rapidement dans l'histoire de l'email. En 1978, Gary Thuerk alors marketeur pour une marque d'ordinateurs qui se lançait sur le marché américain, a l'idée d'envoyer une invitation par email à des utilisateurs d'ARPANET pour inviter ces technophiles à une démonstration produit. Voulant éviter de multiplier le nombre de messages, il mit plusieurs centaines d'adresses directement dans le champ « Destinataire », réalisant le premier envoi de masse non sollicité[4].

Sans réelles règles pour contrôler la pratique, les spams ont ensuite largement proliféré jusque dans les années 2009-2010, avec à cette époque en moyenne 90 % de courriers indésirables dans les boîtes de réception. La ligne blanche ayant été de loin franchie, de nombreuses mesures ont été prises dans l'écosystème email, comme la fermeture de gros spammeurs, la mise en place de dispositifs de filtrage (via des de scores de réputation d'expéditeur par exemple) ou encore de filtres anti-spams directement opérés par les opérateurs de messagerie, sans parler des approches juridiques qui rendent le courriel non sollicité tout simplement illégal (Opt-out par défaut en Europe versus le Opt-in historique des US[5]).

Mais c'était sans compter sur les autres dérives de l'Internet. A mesure qu'il se développe et devient de plus en plus rapide (bandes passantes, nombre d'ordinateurs et d'internautes croissent de manière exponentielle), l'utilisation massive de l'email en fait un excellent vecteur de propagation des virus informatiques : dès la fin des années 90, la tentation est trop grande pour des acteurs malveillants de propager des virus informatiques le plus largement et le plus rapidement possible par ce canal.

Le premier virus à se propager en masse par email était le ver Ska, alias Happy99, en janvier 1999. Profitant de la standardisation de fait de l'usage de Microsoft Outlook, il s'est propagé d'ordinateurs en ordinateurs sous forme de pièce jointe, qui si elle était exécutée, ouvrait une fenêtre affichant un feu d'artifice animé.

Puis ont suivi beaucoup de logiciels malveillants, comptant parmi eux les plus destructeurs de l'histoire. En commençant par Melissa en 1999, du nom d'une danseuse nue de Miami, qui se présentait comme une liste de mots de passe de sites pornographiques. Aussitôt ouvert par la victime, le virus s'envoyait de lui-même à ses 50 premiers contacts. Une méthode radicale allant jusqu'à infecter les services gouvernementaux américains...
A peine un an plus tard, c'est ILOVEYOU qui entre

[4] https://fr.wikipedia.org/wiki/Spam

[5] https://www.cnil.fr/fr/cnil-direct/question/opt-opt-out-ca-veut-dire-quoi

en scène. Se propageant beaucoup plus vite que Melissa, il infecte en quelques heures des milliers d'ordinateurs de particuliers ainsi que des réseaux d'entreprises et d'institutions comme la Central Intelligence Agency (CIA) ou le parlement anglais. Afin de limiter sa propagation et de sécuriser leurs installations, de nombreux administrateurs systèmes sont obligés d'éteindre leurs serveurs emails, mais le mal est fait : un ordinateur connecté à Internet sur 10 aurait été infecté dans le monde.

Plus récemment en 2020, c'est un acte d'accusation[6] du DOJ américain ciblant 6 officiers russes du GRU qui a permis de mieux faire connaître au grand public leurs pratiques, via des campagnes de "rançongiciels" destructeurs ou de l'approche ciblée par email... Il est particulièrement intéressant de voir comment ces campagnes de courriers électroniques malicieux ont été menées, notamment dans le cadre de l'opération visant l'équipe de campagne présidentielle d'Emmanuel Macron en 2017 ou les jeux olympiques d'hiver de PyeongChang en 2018 (visant des athlètes, le CIO et des partenaires des jeux d'hiver …). Intéressant car quelques années après, ce sont ces méthodes, désormais rodées, qui sont utilisées par les cybercriminels, en passant subtilement par les partenaires ou sous-traitants des organisations[7] : une récente étude Proofpoint montre que 98 % des entreprises ont reçu des menaces par courrier électronique de la part de cybercriminels se faisant passer pour leurs fournisseurs.

Ingénierie sociale ou piratage psychologique ?

Presque tous les pièges tendus sur le canal email ont en commun une chose : ils ont besoin de l'humain pour fonctionner. 94 % des cyberattaques sont aujourd'hui initiées via la boîte email et 99 % d'entre elles nécessitent en effet une action humaine pour se déclencher (clic, ouverture de pièce-jointe). On comprend alors aisément l'importance de l'ingénierie sociale, ce véritable piratage psychologique qui entraîne les destinataires à cliquer.

Les techniques d'ingénierie sociale sont utilisées par les cybercriminels depuis l'émergence des premiers virus, et n'ont eu depuis de cesse de se perfectionner, jusque dans les sphères professionnelles. Personne n'est aujourd'hui à l'abri, y compris au sein des institutions les plus prestigieuses ou les plus sensibles, à l'image de chercheurs en médecine renommés, récemment visés par des leurres d'ingénierie sociale sophistiqués[8]. L'objectif des cyberattaquants est de déstabiliser les destinataires et de les inciter à prendre une mauvaise décision, comme renseigner des codes, partager des identifiants de connexion ou effectuer un virement.

Les pirates informatiques s'appuient sur plusieurs leviers afin de générer un scénario d'échec. Le premier est celui de l'émotion. Dans son ouvrage "Thinking Fast and Slow", Daniel Kahneman décrit deux systèmes de pensée distincts : le processus émotionnel et intuitif, et le processus plus lent de

[6] https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

[7] https://www.proofpoint.com/us/blog/email-and-cloud-threats/98-organizations-received-email-threats-suppliers-what-you-should-know

[8] https://www.proofpoint.com/us/blog/threat-insight/badblood-ta453-targets-us-and-israeli-medical-research-personnel-credential

la logique rationnelle. Les cybercriminels vont ainsi chercher à déclencher des émotions chez leurs victimes pour les pousser à cliquer rapidement sur le message, faisant abstraction de l'usage de la raison : "votre compte Netflix est sur le point d'être suspendu" ou "votre paiement a été refusé".

Jouer de la fatigue de son destinataire est également devenu courant. De nombreuses cyberattaques visant les entreprises se produisent ainsi le vendredi après-midi, lorsque les usagers sont fatigués de leur semaine et baissent la garde avant de partir en week-end. Lorsque notre cerveau est fatigué, il délègue en effet ce qui semble être des choix faciles à des fonctions cérébrales inférieures, beaucoup plus automatisées. Et en cas de réussite, les cybercriminels ayant ouvert une brèche le vendredi pourront profiter de tout le week-end pour exploiter leur accès, période durant laquelle l'entreprise victime a moins de chance de réagir.

Troisième levier exploité par les cybercriminels : la confiance. Lorsque l'on est confronté à un choix, notre cerveau opte généralement pour la solution qui va le plus nous inspirer confiance. C'est pour cette raison que de nombreuses marques de confiance se voient usurpées, comme "DHL" ou "Amazon" plutôt que d'autres services de livraison ou e-commerce moins connus. Plus vicieux encore, les cybercriminels savent que les utilisateurs qui ont un doute vont regarder sur quel lien ils sont redirigés avant de cliquer, expliquant qu'ils sont quatre fois plus susceptibles de cliquer[9] sur des liens malveillants s'ils pointent vers Microsoft SharePoint et dix fois plus susceptibles de cliquer s'ils redirigent vers Microsoft OneDrive.

Objectif : protéger l'email

L'email n'étant pas près de disparaître, mieux vaut mettre tous les moyens en œuvre pour protéger ce canal et déjouer les assauts de cybercriminels plus motivés et organisés que jamais pour gagner de l'argent sur le dos des utilisateurs et des entreprises. Heureusement, de nombreuses initiatives à travers le monde ont été lancées pour contrer ces menaces et tenter de sécuriser « plus nativement » l'infrastructure email.

Parmi les initiatives les plus emblématiques, on peut saluer la mise en œuvre du standard DMARC (Domain-based Message Authentication, Reporting & Conformance). Créé en 2012 par des opérateurs majeurs de messagerie tels que Google, Yahoo!, AOL et Microsoft, DMARC constitue sans doute à ce jour l'arme la plus puissante pour lutter contre le spoofing (usurpation d'identité) et le phishing (hameçonnage). Ce protocole permet d'authentifier correctement les expéditeurs, pour protéger les employés, les clients et leurs partenaires, contre les cybercriminels qui cherchent à usurper l'identité d'une marque de confiance.

DNSSEC[10], les extensions de sécurité du DNS déployées à partir des années 2000, ont également largement contribué à sécuriser l'email. Le fonctionnement même d'Internet dépendant largement du DNS, ces extensions permettent de renforcer la sécurité de toutes les interactions de

[9] https://www.proofpoint.com/us/blog/user-protection/why-onedrive-and-sharepoint-attacks-are-successful-and-how-fight-back

[10] https://tools.ietf.org/html/rfc4033

type page web consultée, email envoyé ou encore photo récupérée sur un réseau social. D'autres protocoles, comme le chiffrement TLS (Transport Layer Security) continuent à se développer et seront sans nul doute des armes puissantes utilisées de plus en plus systématiquement dans les prochaines années pour sécuriser notre monde numérique. Le dernier en date, DoH (DNS Over HTTPS) étant curieusement repoussé par la NSA[11] …

In fine, l'humain restant dans l'œil du cyclone, c'est surtout dans cette direction qu'il faut travailler pour se protéger. Les entreprises ne peuvent désormais plus s'affranchir d'une réelle stratégie de cybersécurité centrée sur les personnes, incluant des programmes de sensibilisation et de formation réguliers et approfondis.

Vers une nouvelle pandémie mondiale ?

Et si l'email n'était qu'une pièce d'un puzzle beaucoup plus complexe ? De nouvelles formes d'attaques sophistiquées font leur apparition dans le paysage de la cybermenace, à l'image de l'affaire SolarWinds ou encore de la récente suspicion d'attaque de Microsoft par un groupe étatique chinois[12].

Avec de telles affaires, c'est toute la confiance numérique qui est mise à mal et l'extrême dépendance des organisations publiques et privées auprès de certains acteurs ne peut qu'être source d'inquiétudes, notamment vis à vis des risques d'espionnage ou de cataclysme numérique systémique. Si un opérateur de ressources numériques d'envergure mondiale tel que Microsoft perd le contrôle, alors cette pandémie numérique presque annoncée ne concernera évidemment pas que l'email, mais tout notre ensemble d'outils de collaboration… Une telle conjecture risque vite de devenir incontrôlable.

Car que se passera-t-il si un prochain patch Tuesday de Microsoft s'opère sous le contrôle d'un attaquant tierce ? Si potentiellement l'ensemble des postes informatiques sous Windows du monde entier est atteint, nous serions sous le coup d'une potentielle arme numérique de destruction massive...

[11] https://twitter.com/bortzmeyer/status/1379780232564109312

[12] https://www.lefigaro.fr/secteur/high-tech/faille-chez-microsoft-30-000-organisations-americaines-victimes-de-hackers-chinois-20210306