yuno By xmco

DOSSIER

ÉVOLUTION DE LA VEILLE CYBERSÉCURITÉ : COMMENT SE PRÉMUNIR DES MENACES ?

ÉDITO

Après près de 20 ans d'existence, il nous a paru intéressant chez XMCO d'analyser comment la veille en cybersécurité et la manière dont nous la traitons ont évolué au cours du temps.

Afin de répondre aux demandes de plusieurs clients, XMCO a démarré son service de veille professionnel dès 2004. **L'objectif du service était alors d'aider nos clients à suivre la découverte de vulnérabilités et la publication de correctifs ou de codes d'exploitation afin d'anticiper au maximum l'application des correctifs et plus généralement de maintenir son système d'information en sécurité.**

À l'époque, les cybercriminels se limitaient à des attaques opportunistes, bien loin de la criminalité organisée d'aujourd'hui.

Depuis, le nombre de vulnérabilités n'a cessé d'augmenter ; l'actualité et les attaques ont pris une place prépondérante dans la manière dont la veille doit être organisée. Place désormais aux APTs (Advanced Persistent Threats) financièrement motivées, ou encore à des attaquants scannant en permanence Internet à la recherche de services vulnérables ou de données à dérober.

Les entreprises ont donc elles aussi dû s'adapter et faire face à un besoin grandissant de veille technique pour limiter au maximum les attaques.

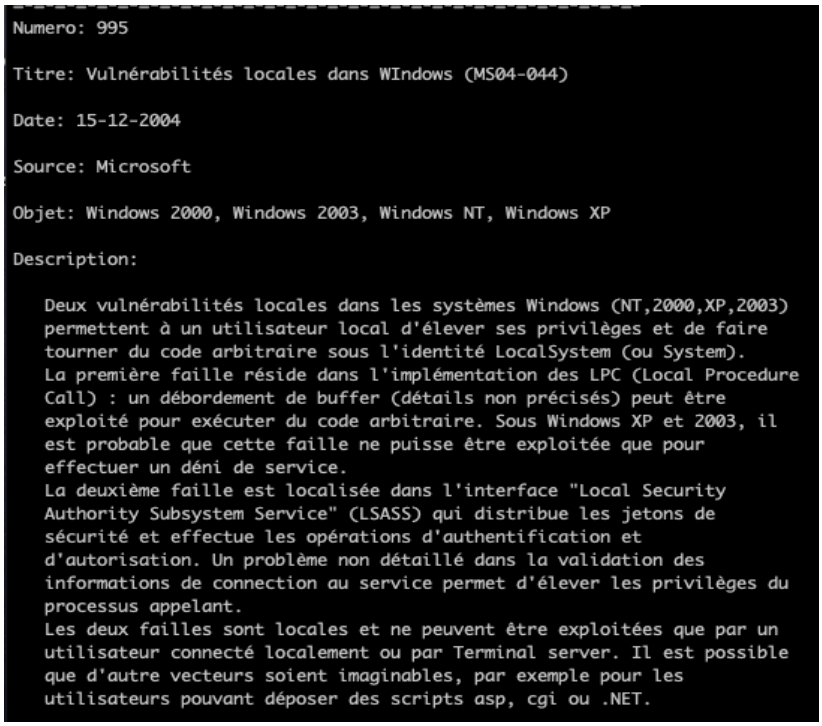
Retour vers le futur…

LES SERVICES DE VEILLE DU 20ÈME SIÈCLE

Bien avant XMCO, quelques acteurs proposaient déjà le même type de services professionnels.

La première initiative remonte à 1993 avec la liste de diffusion BugTraq . Celle-ci diffuse (souvent sans en informer l'éditeur du logiciel) les informations relatives aux failles identifiées dans les logiciels.

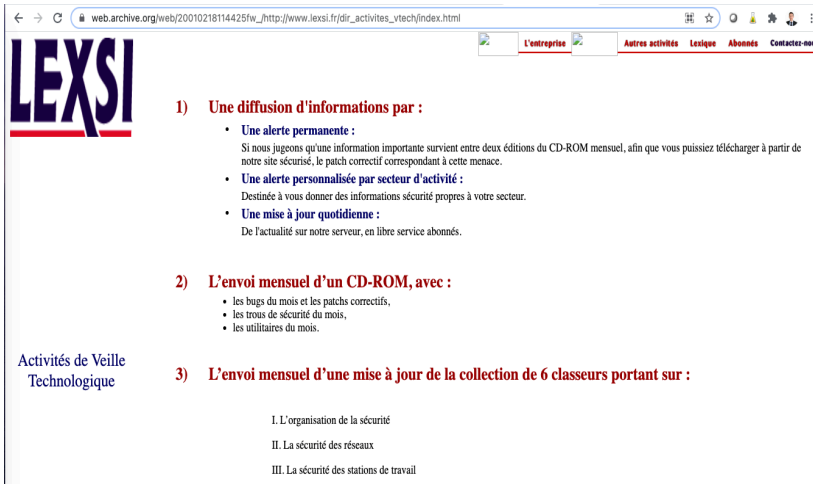
En 1997 était lancé HSC qui a certainement été le précurseur des services de veille.
HSC proposait une veille en mode texte envoyée par email. En complément, un accès HTTPS permettait d'accéder à la base de connaissance. Le service s'est ensuite étendu à la veille juridique.



```
Numero: 995

Titre: Vulnérabilités locales dans WIndows (MS04-044)

Date: 15-12-2004

Source: Microsoft

Objet: Windows 2000, Windows 2003, Windows NT, Windows XP

Description:

   Deux vulnérabilités locales dans les systèmes Windows (NT,2000,XP,2003)
   permettent à un utilisateur local d'élever ses privilèges et de faire
   tourner du code arbitraire sous l'identité LocalSystem (ou System).
   La première faille réside dans l'implémentation des LPC (Local Procedure
   Call) : un débordement de buffer (détails non précisés) peut être
   exploité pour exécuter du code arbitraire. Sous Windows XP et 2003, il
   est probable que cette faille ne puisse être exploitée que pour
   effectuer un déni de service.
   La deuxième faille est localisée dans l'interface "Local Security
   Authority Subsystem Service" (LSASS) qui distribue les jetons de
   sécurité et effectue les opérations d'authentification et
   d'autorisation. Un problème non détaillé dans la validation des
   informations de connection au service permet d'élever les privilèges du
   processus appelant.
   Les deux failles sont locales et ne peuvent être exploitées que par un
   utilisateur connecté localement ou par Terminal server. Il est possible
   que d'autre vecteurs soient imaginables, par exemple pour les
   utilisateurs pouvant déposer des scripts asp, cgi ou .NET.
```

Exemple de bulletin de la société HSC

Peu de temps après apparaissait LEXSI.
Lexsi, diffusait sa veille en envoyant un CD ROM mensuel contenant les bulletins rédigés et un panorama de la presse internationale.



Site web de la société Lexsi

Enfin, 2002 marquait l'apparition d'une seconde liste baptisée Full disclosure diffusant nombre d'informations techniques relatives aux vulnérabilités découvertes et aux correctifs de sécurité

LA VEILLE EN 2004 : GOOGLE READER, SECUNIA ET SECURITY FOCUS

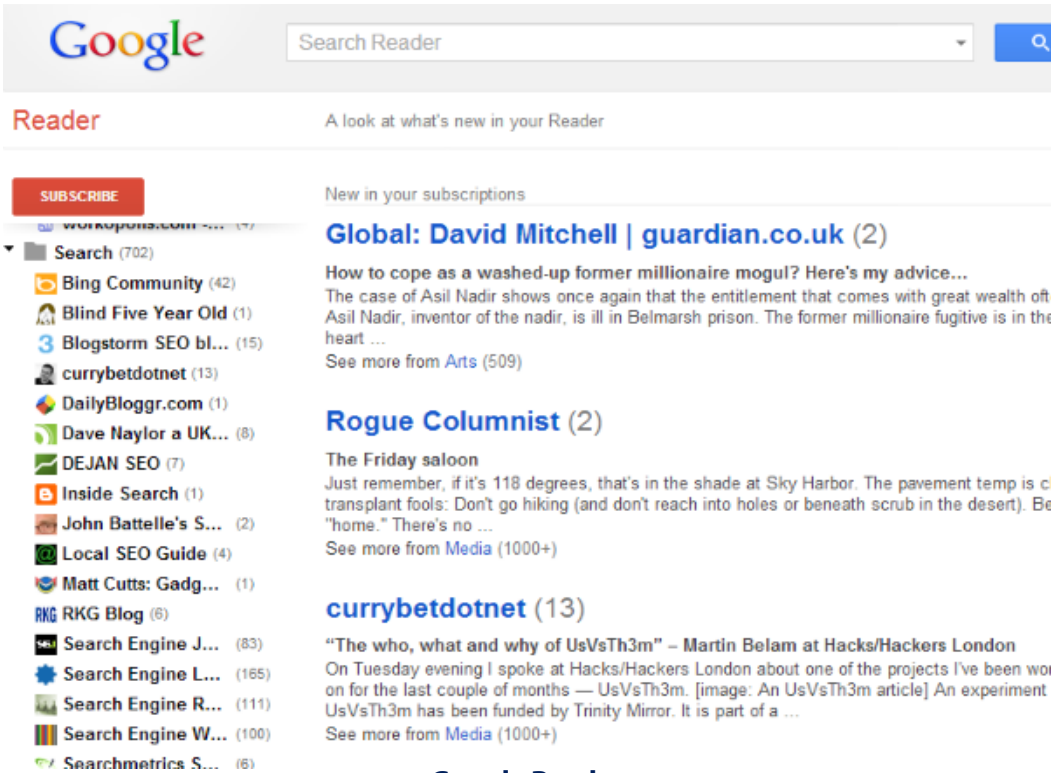
En 2004, les problématiques de sécurité émergeaient à peine dans les préoccupations des sociétés. Quelques RSSI commençaient à prendre leurs marques et ne savaient pas toujours par où commencer (et maintenant ?). Pour beaucoup la veille apportait les premiers éléments de réponse à ces éternelles questions (toujours valables aujourd'hui) : quoi PATCHER ? et par où commencer ?

Les entreprises commençaient tout juste à s'intéresser aux problématiques de patch management, mais il leur manquait souvent un cadre pour adresser efficacement ce besoin quotidien de surveillance. La veille était une activité souvent manuelle, artisanale et sa diffusion auprès des intéressés était limitée (et donc de fait, tout comme son efficacité).

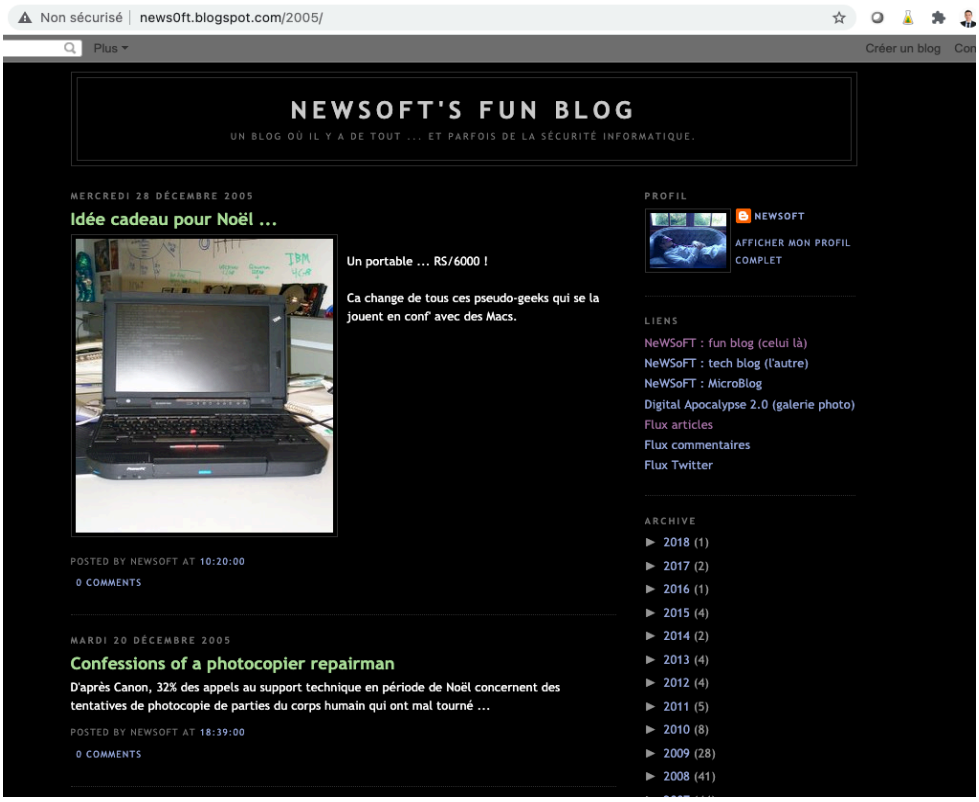
C'est pour répondre à cette situation, XMCO a lancé son service de veille en 2004.

Le service était alors composé de 5 veilleurs en charge de produire une veille le matin, de consolider les informations et de rédiger les quelques bulletins journaliers avant d'envoyer par email à nos clients les informations relatives à leurs technologies.
Les bulletins concernaient Windows bien entendu, mais aussi des OS obscurs disparus (ou presque depuis) tels que Solaris, AIX, et Cie. Un extranet était déjà disponible et permettait d'accéder à notre base de connaissances.
En 2004 XMCO réalisait une veille très artisanale, se basant principalement sur :

• Un Google reader chargé de surveiller une centaine de flux RSS.
• Des scripts développés pour suivre certains sites d'éditeurs lorsque ceux-ci proposaient une section dédiée aux vulnérabilités de leurs produits.
• Des sites agrégeant et recensant plusieurs sources :
    o SecurityFocus et BugTrack pour l'apparition de nouveaux bugs
    o SecurityFocusSecunia, iDefense et FrSIRT, packetstorm pour s'informer sur la sortie de patches
    o MilW0rm et xfocus pour les exploits
• Les mailing-lists d'éditeurs et la mailing list «Full-disclosure»
• Les blogs, comme celui de Cédric Blancher (Ma petite parcelle d'Internet) et Nicolas Ruff (news0ft)



Google Reader



Blog de Nicolas Ruff

Les thématiques techniques (nouvelles vulnérabilités, exploits, virus) prédominaient dans les services de sécurité des entreprises, et les sujets liés aux thématiques du renseignement, qu'on appelle aujourd'hui Cyber Threat Intelligence (quels attaquants cible mon secteur d'activité ? Comment le font-ils ? Comment les détecter ?) n'étaient que peu voire pas connus des entreprises.

Conscient de l'importance de la Cyber Threat Intelligence (CTI), nous complétions dès 2006 notre veille de bulletins de type INFO, bulletins dédiés à la CTI.

C'est la même année que le premier numéro de notre magazine sur l'actualité, «l'Actusécu», vit le jour (il continue son chemin après plus de 58 numéros).

actusécu
By xmco

LA VEILLE DÉBUT 2010

La veille au début des années 2010 est marquée par l'émergence de l'Internet 2.0, faisant la part belle à l'interactivité entre utilisateurs.

De nouvelles vulnérabilités techniques apparaissent. D'un nouveau type, elles viennent affecter de nouveaux types d'appareil : Les ordinateurs (ou réseau de travail des entreprises) ne sont plus les seuls à faire les frais des attaques des pirates. Ces derniers ciblent de plus en plus fréquemment les systèmes industriels (on se souvient de Stuxnet en 2010) ou encore l'IoT (botnets constitués de réfrigérateurs, de TV ou encore de routeur).

Cette période fût également marquée par l'émergence des réseaux sociaux. Bien que ceux-ci renouvellent les perspectives de communication des marques avec leurs utilisateurs, ils entrainent dans le même temps l'apparition d'un nouveau type de menace cyber : l'atteinte à la e-reputation.

Enfin, l'outillage pour diffuser l'information commence à faire son apparition, à l'instar de MISP (plateforme open-source dédiée à la CTI) dont les débuts remontent à 2011. Les standards STIX (format de données) et TAXII (protocole d'échange) font leur début à partir de 2012.

L'écosystème des cyber-attaquants et de la défense aux attaques se structurent également :

• **De nouveaux groupes d'attaquants**, parfois supportés par des entités étatiques, et particulièrement bien organisés apparaissent (on parle alors d'APT ou Advanced Persistent Threat).
• **Des CERTs** (Computer Emergency Response Team) émergent un peu partout autour du globe. En France, ces CERTs (ou CSIRT) sont fédérés autour d'un groupe informel baptisé InterCERT, mais également au sein d'association internationales. Ces CERTs ont pour objectif l'échange de bonnes pratiques, le partage d'information autour des menaces émergentes liées à l'environnement cyber, etc.

Avec la création de l'ANSSI en 2009 qui vient remplacer la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information), l'Etat français annonce clairement son intention d'aider les sociétés françaises à garder leur système d'information protégé (newsletter, référencement des CERTs français).

Côté XMCO, la tendance était à la mise à disposition de nos bulletins sur le plus grand nombre de support possible : application mobile, plateforme SaaS, API, nos bulletins se devaient d'être consultables par tous les moyens.

LA VEILLE DÉBUT 2020

Les bouleversements initiés au début des années 2010 ont continué à prendre de l'ampleur pour plusieurs raisons :

• **L'interconnectivité des outils** entre eux créent une chaine de dépendance qui rend difficile un silotage strict des systèmes. Une vulnérabilité exploitée au sein d'une technologie amène un développement horizontal facilité. Il en est de même avec l'interdépendance entre les entreprises et leurs systèmes d'information. Les schémas de « suply-chain » sont de plus en plus commun (SolarWinds, Centreon)

• **La monétisation des données personnelles d'utilisateurs** diversifie les cibles et les opportunités d'attaques. Toutes les thématiques sont bonnes pour tromper les internautes : évènement internationaux (sportifs, conflits, …), accusations mensongères, … L'hameçonnage ne se fait plus uniquement par email, mais également sur les réseaux sociaux (arnaque à la romance). Dans tous les cas, l'objectif est d'obtenir des données ayant une valeur marchande (données personnelles, accès systèmes, …) et/ou de l'argent.

Résultat, là où 150 vulnérabilités par mois étaient découvertes en 2006, plus de 1500 sont découvertes par mois en 2021.

Les origines des vulnérabilités se diversifient également : **là où les vulnérabilités découvertes dans les années 2000 résultaient d'un problème technique (dépassement de mémoire, attaque par déni de service), les vulnérabilités découvertes en 2020 sont de plus en plus liées à des problèmes de logique applicative** (exceptions et effets de bords non-anticipées lors de la phase de développement dus à la place toujours importante de l'automatisation des taches, interaction entre les multiples composants des systèmes toujours plus complexes).

Face à des groupes d'attaquants toujours plus structurées et organisées, **la Cyber Threat Intelligence s'impose comme une discipline incontournable pour aider les sociétés à mieux anticiper les actions de ces groupes d'attaquant.**

La CTI est une discipline novatrice en ce qu'elle va au-delà de la veille en vulnérabilité pour fournir des indicateurs sur les comportements des groupes d'attaquants (vecteurs d'attaques préférés, adresses IP utilisées, noms de fichiers, méthodes de déploiement dans le SI, secteurs ou pays visés…). Ces éléments appelés indices de compromission sont catégorisés et agrégés autour d'« Advanced Peristant Threat » (APT) et enrichis à chaque nouvelle action de l'attaquant.

Grâce à cette base de données d'attaquants, la CTI peut permettre une meilleure sécurisation du Système d'Information en fournissant des indicateurs pour effectuer des contrôles ciblés qui, couplés à une veille technique, peuvent permettre une priorisation efficace de la résolution des vulnérabilités présentes sur un système d'information.

Renommé Yuno en 2020, le service de veille du CERT-XMCO a su se développer et prendre en maturité pour s'adapter à l'émergence de ces nouveaux défis :

• 40 personnes rédigent quotidiennement des bulletins, des dizaines de scripts de surveillance de sources, des centaines de comptes Twitter et d'éditeurs suivis
• +30 bulletins sont rédigés par jour en moyenne
• Des résumés de la semaine, des avis d'expert, des alertes, des résumés de publications, des tendances, etc.
• Plus 1500 technologies suivies
• Plus de 1000 sources surveillées (listes de diffusions, sites éditeurs, comptes twitter, dépôts github, blogs spécialisés…)
• Un Portail et une API pour suivre vos bulletins, personnaliser la réception de vos alertes et gérer vos plans d'actions

Avec près de 60 000 bulletins rédigés depuis sa création, Yuno entend répondre aux enjeux actuels et à venir :

• Criticité, type d'exploitation, dommages potentiels, versions impactées, remédiation…Les bulletins de veille ne contiennent que l'essentiel pour vous aider dans votre prise de décision.
• Cyber-attaques en cours dans un pays, nouvelle législation, apparition d'un nouveau ransomware : prenez de la hauteur dans votre priorisation à l'aide de bulletins environnementaux.
• Plus de 1500 technologies suivies : centralisez le suivi de toutes les technologies de votre système d'information en un seul endroit.
• Bulletins journaliers : soyez rapidement informés de la parution d'une vulnérabilité, d'un patch ou d'un code d'exploitation
• Déplacez la charge de la veille à une équipe d'expert et concentrez-vous sur l'essentiel : définir votre stratégie de défense, et élaborer votre planning de patch
• Aperçu de la menace, guide, actu sécu : utilisez la veille yuno pour sensibiliser vos collaborateurs et lutter contre l'ingénierie sociale
• Bénéficiez de plan d'actions directement intégrés à votre veille : gérez efficacement votre patch management

Ils en parlent mieux que nous

FLOWBIRD Urban Intelligence

« La veille Yuno permet d'avoir des informations orientées sur nos services déclarés. Elle permet de maintenir les connaissances auprès de mes équipes. Je m'en sers également comme outil de sensibilisation car certains bulletins permettent d'expliquer et d'appuyer mes messages. »

Yohann Guiot, RSSI et DPO Groupe, FLOWBIRD

ELSAN

« Le service nous permet de définir nos périmètres et de donner des accès distincts à chacun de nos 120 établissements tout en conservant une vision globale sur chacun des établissements.

Grâce à la plateforme nous savons qui est concerné par une vulnérabilité. Cela nous permet de mieux communiquer et de mieux gérer les correctifs.

Toutes les sources et failles du monde sont filtrées. Nous savons que nous ne recevons que ce qui nous intéresse. »

Grégoire Saugy, RSSI, ELSAN

Tous les vendredis, retrouvez un résumé des actualités marquantes de l'écosystème cyber sur notre compte linkedin.

in **NOUS REJOINDRE SUR LINKEDIN**

Retrouvez-nous

Sur notre site :

www.xmco.fr

Sur les réseaux sociaux :

Envie d'échanger ?

sales@xmco.fr

01 79 35 29 30

xmco We deliver cybersecurity expertise

+33 (0)1 79 35 29 30
info@xmco.fr

www.xmco.fr

Nos partenaires :