Communiqué de presse - Icodia

Icodia reçoit le label France Cybersecurity

À l'occasion du neuvième Forum International de la Cybersécurité qui s'est tenu les 24 et 25 janvier à Lille, Icodia a reçu le label France Cybersecurity pour sa solution de filtrage antivirus et antispam des e-mails.

Ce label est destiné à promouvoir les solutions de cybersécurité françaises et atteste de la qualité et des fonctionnalités des produits labellisés.

Pour Icodia, les questions de cybersécurité sont une priorité et une composante de toutes ses solutions.
On observe une recrudescence des attaques et des infections par e-mails[1] qui menacent l'intégrité des systèmes d'information. De plus en plus souvent, les virus sont capables de contourner les solutions existantes[2]. La plupart des antivirus/antispams classiques ne sont pas suffisament rapides et réactifs face à ces risques. Ce constat a incité Icodia à concevoir son propre système de protection.

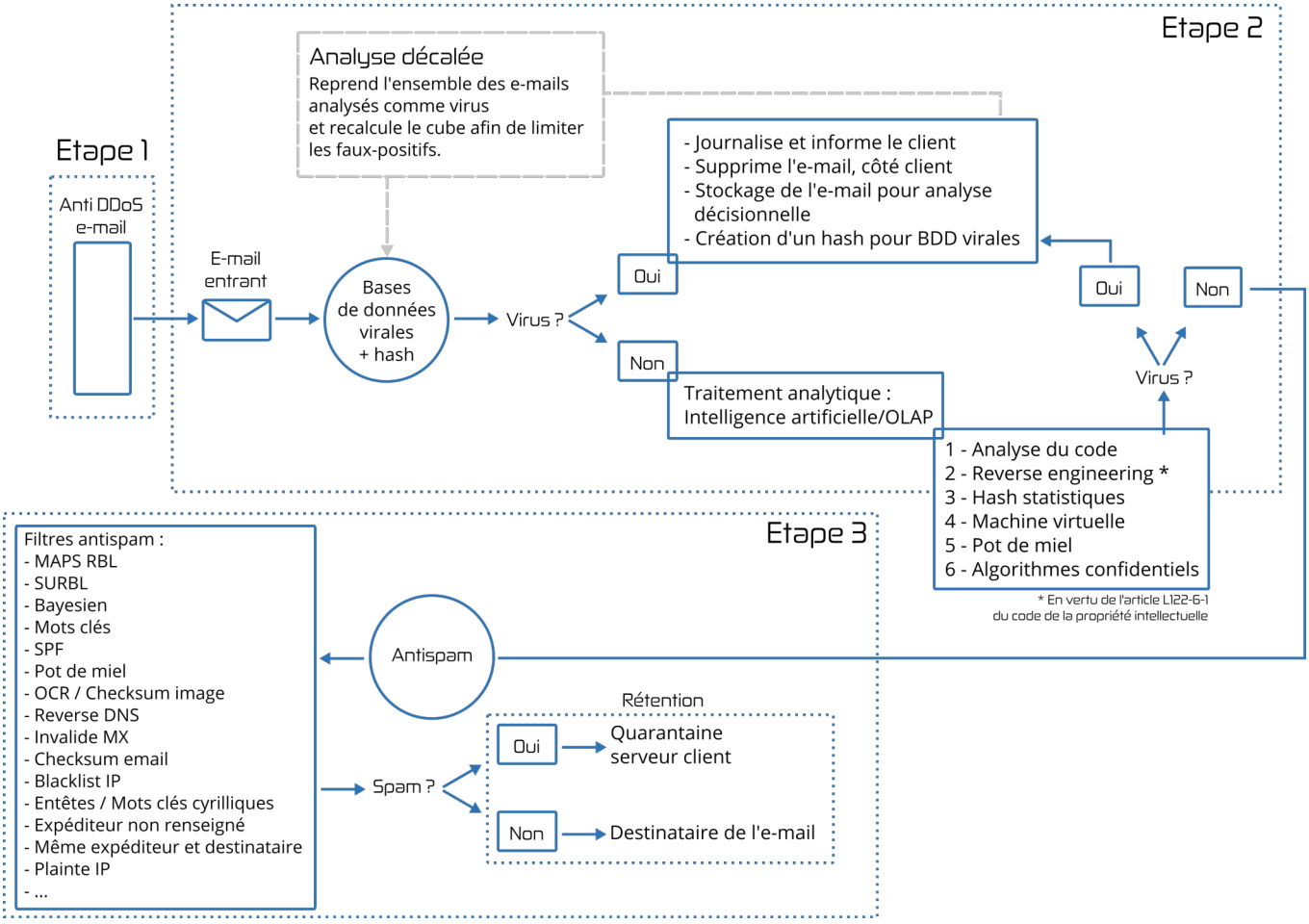
IcoCerberus.Mel est une solution propriétaire développée par le pôle R&D d'Icodia.
Elle intègre des technologies d'intelligence artificielle, dont l'hypercube OLAP. Elle apprend seule et crée de nouvelles empreintes et signatures en identifiant les comportements douteux. Cela lui permet de construire sa propre base de données virale et d'alimenter son réseau décisionnel.

IcoCerberus.Mel est intégré aux services d´hébergement mutualisé de la plateforme Icodia. Il est également disponible pour tous les serveurs virtuels et dédiés de la gamme d'Icodia.
IcoCerberus.Mel est proposé en mode externalisé (SaaS), pour les personnes utilisant des services e-mails en dehors du réseau d'Icodia. Il est compatible avec toutes les solutions de messagerie tierce (MS Exchange, MS Office 365, Zimbra, Domino, IBM Notes, Novell, etc.).

1. https://news.icodia.com/general/les-ransomwares-en-2016
2. https://news.icodia.com/email/attaques-de-virus-via-email-quelques-conseils-pour-vous-proteger

IcoCerberus.Mel en détails

La solution d'Icodia propose une protection en 3 étapes, à laquelle s'ajoute la rétention des e-mails en cas d'indisponibilité. Cette protection se fait en temps réel.



1 - La protection contre les attaques de serveurs entrant de messagerie.

Depuis quelques années, des botnets, de plus en plus nombreux, envoient des virus qui évoluent de plus en plus vite. Il faut donc, avant même tout système de filtrage antivirus et antispam, disposer de sécurités permettant de réguler le trafic entrant, et de bloquer le trafic illégitime, afin que les applicatifs de traitement puissent travailler dans de bonnes conditions.

C'est l'utilité de ce premier système, composé de pare-feux actifs et de filtres réseau statistiques pouvant bloquer une attaque réseau en amont des filtres (attaques DDoS, par exemple).

2 - Le filtrage antivirus

Les virus arrivent en masse, et évoluent aujourd'hui très rapidement, beaucoup plus qu'avant.
L'infection virale est maintenant une activité mercantile développée, qui dispose de moyens plus importants (exemple : les cryptolockers, comme Locky ou Zepto).
Le principal problème lorsqu'on utilise uniquement des bases virales est la configuration de 'course' de ces infections virales : l'attaquant utilise un botnet important pour envoyer en masse, sur un court laps de temps, un nombre important de virus, avant qu'ils ne soient reconnus par les éditeurs antivirus, qui feront ensuite une mise à jour. Ils espèrent, par l'inondation de pourriels non détectés, infecter le plus de machines possibles. Ces virus sont d'ailleurs de plus en plus évolués, aussi bien par leur forme (fausse facture, relance de facture, etc.) que par leur code source (code obscurci[3]).
Il n'est donc plus possible de filtrer les virus uniquement par un système de bases antivirales multiples. C'est sur ce constat que nous avons décidé de développer notre propre solution, innovante.

3. https://fr.wikipedia.org/wiki/Code_impénétrable

Elle se base sur 7 méthodes :
a/ Un système de 5 bases virales différentes, fonctionnement 'traditionnel' d'un outil de filtrage antivirus, avec une demande de mise à jour des bases la plus fréquente possible ;
b/ La rétention temporaire (quelques dizaines de secondes) d'e-mails, afin de pouvoir faire des statistiques sur la masse de messages envoyés ;
c/ Une technologie hypercube OLAP (décisionnelle), qui permet d'analyser le comportement et l'habitude des transactions de messages, afin de déterminer un ou plusieurs comportement douteux ;
d/ La rétro-analyse de code qui, via un environnement sécurisé, va simuler et analyser le comportement d'un script (ou programme) existant dans un email afin de déterminer sa dangerosité ;
e/ Le hachage de pièces jointes permettant d'effectuer des statistiques sur les pièces jointes et alimenter le réseau décisionnel hypercube ;
f/ Des 'adresses espionnes' qui sont placées judicieusement sur des réseaux, permettant de ne recevoir généralement que des pourriels, et alimentant également le réseau décisionnel hypercube ;
g/ L'utilisation de la base différée après traitement afin d'affiner encore plus et éviter les faux-positifs[4].

Voici les différentes étapes :
- Le système filtre tous les emails entrant via les 7 méthodes ;
- Il informe le destinataire et l'expéditeur d'un email (si souhaité), lorsqu'un virus est détecté ;
- Il indique le type de virus ;
- Il nettoie le contenu de l'email ;
- Il transmet au destinataire les éléments qui ne sont pas infectés, si existant ;
- Aucun message n'est effacé sans information, et nous stockons dans un cluster de stockage (dans notre datacenter) tous les messages détectés comme virus, pour une analyse différentielle par d'autres applicatifs.

3 - Le filtrage antispam

Le système antispam des services emails ICODIA est un système efficace, de conception complexe, alliant de nombreux filtres qui peuvent être communs à la plateforme entière, ou personnalisés par profil.
L'administrateur peut activer ou désactiver un à un tous les filtres mis en place, et affiner le filtrage en fonction des besoins.

L'utilisation de listes d'adresses autorisées ou bloquées, paramétrables selon les besoins, s'ajoute à la chaine de filtrage antispam pour limiter les faux positifs.
Les messages classifiés comme SPAM sont stockés dans une base de données accessible en ligne ; aucun message n'est supprimé, mais simplement classifié, avec un entête email spécifique.

Les différents types de filtrages antispams sont :
- RBL (MAPS ET SURBL) / IP : utilisation de nombreuses bases de données publiques contenant des plaintes liées à des adresses IP et/ou nom de domaine reconnus pour envoyer du spam ;
- Pot de miel : utilisation d'e-mail piège, pouvant augmenter la reconnaissance de mailing spam par exemple ;
- Reverse DNS / MX invalide : vérification de la conformité de l'envoi de l'email par rapport à la norme ;
- Mots clés : liste de mots clés complexes (expressions régulières), reconnus et analysé par nos opérateurs;
- SPF : norme de vérification du nom de domaine de l'expéditeur d'un courrier électronique par sa zone DNS, normalisée dans la RFC 7208 ;
- OCR : analyse des contenus texte d'une image ;
- Bayésien : technique statistique de détection de pourriels s'appuyant sur la classification naïve bayésienne[5] ;
- Hypercube OLAP : basé sur la même technologie que l'antivirus mais spécifique au spam.

4 - La rétention finale et l'envoi au(x) serveur(s) destinataire(s)

Les serveurs de filtrage d'Icodia bénéficient d'une redondance complète à tous les niveaux et d'une capacité de montée en charge très importante.
La disponibilité des services est donc garantie, ainsi que la bonne réception des messages.

Le serveur de destination ne bénéficie pas nécessairement des mêmes garanties. Particulièrement s'il s'agit d'un serveur local dans une entreprise relié à Internet au moyen d'un lien grand public (ADSL, FTTH, par exemple).

4. https://fr.wikipedia.org/wiki/Faux_positif
5. https://fr.wikipedia.org/wiki/Classification_naïve_bayésienne

Dans ce cas, la rétention des messages est une stratégie défensive appropriée : les serveurs d'Icodia conservent les messages envoyés pendant l'indisponibilité du service local et les transmettent dès qu'il est de retour en ligne.

Le délai de rétention peut aller jusqu'à une semaine, voire plus sur demande.

A propos d'Icodia

Icodia a été créé en 2000 à Rennes.
Son activité principale est l'hébergement très haute disponibilité et l'ensemble des services annexes, (ingénierie logicielle, protection des données, cybersécurité, recherche et développement...).

La recherche et le développement représentent plus de 50% de son activité.

La réunion des compétences réseau, logiciel et sécurité rendent la plateforme d'hébergement optimisée et toujours en avance sur son temps.
L'ensemble des outils d'automatisation de la gestion permettent des gains de temps très importants, une réduction maximale du taux d'erreur et une réactivité optimale.

Icodia, hébergeur direct, est opérateur de ses propres liens dans son propre datacenter assimilé TIER IV[6].
Pour assurer une fiabilité optimale, tous les composants essentiels à la plateforme sont redondants : liens Internet, firewalls, passerelles, serveurs DNS, routeurs, connectiques, refroidissement, etc.

L'exigence d'Icodia est la plus élevée du marché en matière de sécurité, fiabilité, et disponibilité du service, avec une astreinte technique 24/7/365.
Chaque écart de température, de tension électrique, d'humidité, de peering réseau, etc., alerte le centre opérationnel.

Le service technique est également joignable 24/7/365.

6. https://fr.wikipedia.org/wiki/Uptime_Institute#Tier_IV_-_La_tolérance_aux_pannes