PLONGÉE AU CŒUR DE L'HISTOIRE DE TALOS

Talos
talosintelligence.com

Le groupe Talos réunit des spécialistes en menaces chevronnés qui s'appuient sur des systèmes sophistiqués pour générer des informations sur les menaces utilisées par les produits Cisco afin de détecter, d'analyser et de contrer les menaces connues et émergentes. Talos utilise une infrastructure et des systèmes sophistiqués qui offrent une visibilité inégalée sur le réseau par l'agrégation et l'analyse des données télémétriques de Cisco.

La mission du groupe Talos consiste à transformer les informations en moyens de défense et à concevoir des technologies de détection permettant d'informer et de protéger efficacement nos clients. Grâce à nos activités de recherche et développement, nous optimisons en permanence les systèmes d'analyse qui identifient et contrôlent les menaces inconnues. Notre équipe collecte et analyse les données pour générer et distribuer des connaissances directement exploitables. En protégeant et en informant nos clients sur les menaces nouvelles et en circulation, nous créons un processus de sensibilisation et d'intervention unique.

TALOS ASSURE LA PROTECTION DES ENTREPRISES DU CLOUD AU END POINT

20 MILLIARDS DE MENACES BLOQUÉES PAR JOUR
soit environ 3 blocages par jour pour chaque humain sur terre

80 MILLIONS DE REQUÊTES DNS MALVEILLANTES BLOQUÉES PAR JOUR
via Cisco Umbrella

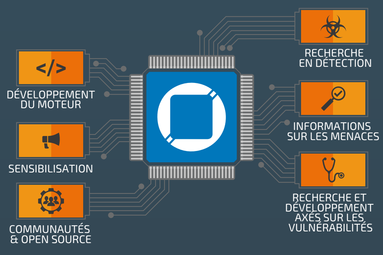
PLUS DE 180 VULNÉRABILITÉS « ZERO DAY »
(menaces inédites) découvertes par an

DÉTECTIONS DES COMPROMISSIONS DE RÉSEAU 100 FOIS PLUS RAPIDES
qu'avec les solutions concurrentes

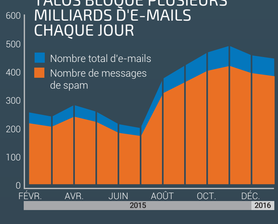
TALOS CONCENTRE SES EFFORTS SUR CINQ DOMAINES CLÉS

Recherche en détection, informations sur les menaces, développement du moteur, recherche et développement axés sur les vulnérabilités, et sensibilisation

- **Plus de 250** chercheurs spécialisés dans les menaces à temps plein
- **Plusieurs millions** d'agents de télémétrie
- **4** data centers dans le monde
- **Plus de 1 100** pièges à menaces
- **Plus de 100** partenaires en matière d'informations sur les menaces

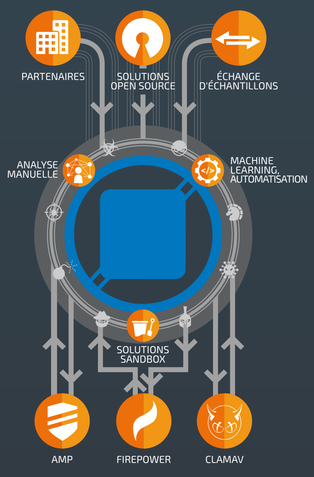


LE SPAM REPRÉSENTE 63% DE TOUT LE TRAFIC E-MAIL



COMMENT TALOS DÉTECTE-T-IL LES LOGICIELS MALVEILLANTS ?

Talos recueille des données provenant de millions d'utilisateurs du monde entier, de pièges à pirates, de solutions sandbox et de partenariats sectoriels étendus, collectant ainsi plus de 1,1 million d'échantillons malveillants uniques par jour.



EN RÉSUMÉ

- **90 000** victimes ont été ciblées chaque jour
- **9 000** adresses IP uniques ont reçu des exploits en une journée
- **74 %** des exploits ont été transmis via Adobe Flash
- **62 %** des infections Angler ont distribué un ransomware
- **40 %** des utilisateurs ayant reçu des exploits ont été compromis
- **300 dollars** le montant moyen de la rançon payée à Angler

ÉTUDE DE CAS : ANGLER

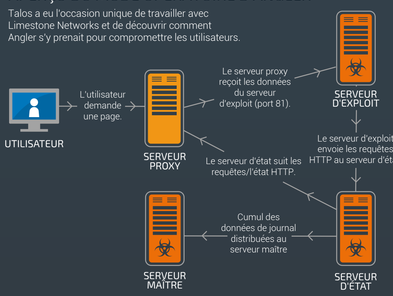
En octobre 2015, Talos a porté un sérieux coup à Angler, l'un des kits d'exploits les plus répandus, en découvrant qu'un grand nombre de serveurs proxy utilisés par Angler étaient hébergés sur les serveurs du fournisseur de services Limestone Networks.

MESURES PRISES PAR TALOS:

- Blocage de l'accès des clients par une mise à jour des produits empêchant les redirections vers les serveurs proxy d'Angler
- Publication de règles Snort visant à détecter et à bloquer les vérifications effectuées par les contrôles d'intégrité
- Distribution de règles à la communauté via Snort
- Publication de mécanismes de communication tels que des protocoles afin de permettre à d'autres d'assurer leur protection et celle des clients
- Publication d'indicateurs de compromission afin de permettre aux acteurs de la protection d'analyser l'activité de leur propre réseau et de bloquer l'accès au reste des serveurs
- Notification des fournisseurs d'hébergement touchés afin qu'ils arrêtent les serveurs malveillants

APERÇU DU MODE OPÉRATOIRE D'ANGLER

Talos a eu l'occasion unique de travailler avec Limestone Networks et de découvrir comment Angler s'y prenait pour compromettre les utilisateurs.



ANECDOTES DE LA LUTTE CONTRE LA CYBERCRIMINALITÉ

« Un de nos cybercriminels préférés est parvenu à installer son propre enregistreur de frappe sur son système en enregistrant les fichiers sur un site FTP censé être sécurisé, qui les a tout bonnement publiés sur le Web en accès libre. Ces fichiers contenaient non seulement son nom d'utilisateur et son mot de passe, mais également ses informations bancaires. On a vu plus futé. »

CRAIG WILLIAMS
Responsable technique, responsable de la sensibilisation à la sécurité

« J'ai appelé un cyberescroc et je suis parvenu à le convaincre que je pouvais uniquement payer par chèque. Il m'a alors donné son adresse, qui m'a conduit à la société responsable de l'escroquerie. Une autre fois, j'ai tellement énervé un escroc qu'il est sorti du scénario qui lui était imposé et a commencé à m'insulter en chuchotant pour que son chef ne l'entende pas. »

JAIME « WIK » FILSON
Chargé de recherche, Maître en méfaits et impostures

« [Un employé Talos] a présenté un exposé à la conférence Defcon 19, où il expliquait comment s'évader de prison de façon électronique. Plus tard, dans un épisode de la série télévisée Mr. Robot, ils ont fait s'évader quelqu'un de prison. Et la série a utilisé mot pour mot le résultat généré par son outil personnalisé. »

PATRICK MULLEN
Responsable de l'équipe de recherche en intervention

« Un vendredi après-midi, notre directeur nous a tous réunis et a appelé le numéro associé à une escroquerie de nettoyage d'ordinateur. Il a demandé à l'un d'entre nous de créer une machine virtuelle et de suivre les instructions de l'escroc, qu'il avait mis sur haut-parleur. Notre directeur s'est fait passer pour un novice en informatique assez agressif et un peu sourdingue, et tout le monde devenait écarlate à essayer de retenir ses rires. À la fin, il a dit à l'escroc qu'il venait de se faire avoir et que nous avions récupéré tous ses outils. »

BRITTANY LAWLER
Chargée de recherche