Étude de cas

Une solution Cisco qui protège avant, pendant et après l'attaque

Une société pétrolière et gazière internationale fait confiance à Cisco Cloud Web Security Premium pour détecter et résoudre une infection par rançongiciel persistante.

Challenges

À l'heure où le vol ou la corruption des données d'entreprise est souvent le principal motif d'une d'attaque, la sécurité du contenu n'a jamais été aussi complexe. Selon le rapport annuel Cisco 2014 sur la sécurité, les analystes Cisco ont constaté que 100 % des réseaux d'entreprise analysés présentaient un trafic vers des sites Web hébergeant des programmes malveillants.[1] Suite à l'observation de cette activité, ils ont également déterminé que lorsque ces réseaux avaient été pénétrés, ils étaient probablement compromis depuis un certain temps et que l'infiltration principale était passée inaperçue.[2]

Les facteurs suivants rendent la détection des menaces particulièrement difficile pour les équipes de sécurité :

- **La mobilité et le cloud**, en l'absence de mesures de sécurité appropriées, réduisent la visibilité et compliquent la sécurité. Avec la généralisation du cloud computing, de la virtualisation, de la mobilité et du télétravail, à laquelle s'ajoute la tendance du BYOD, les entreprises ont de plus en plus de mal à garder le contrôle sur leurs données. Le réseau devient plus « poreux », créant dès lors davantage de vecteurs d'attaque. De plus, le déplacement d'un nombre croissant de services vitaux dans le cloud, qui deviennent donc accessibles en dehors du périmètre sécurisé de l'entreprise, ne cesse d'accroître la surface d'attaque.
- **De puissants cybercriminels**, selon le *rapport annuel Cisco 2014 sur la sécurité*, « s'emploient de manière proactive à comprendre les solutions de sécurité déployées afin d'évoluer vers des schémas de comportement moins visibles et moins détectables pour dissimuler au mieux leurs attaques ».[3] Cette stratégie complique la tâche des solutions et des professionnels de la sécurité. De leur côté, les entreprises doivent faire face à « une augmentation du trafic chiffré, du brouillage et de la randomisation dont les cybercriminels usent pour noyer les comportements de contrôle-commande (C&C) dans le trafic réel. »[4]

PROFIL DU CLIENT

Secteur : pétrole et gaz

Collaborateurs : environ 15 000

Exploitation : mondiale

Personnel de sécurité : 12 personnes

Autres mesures de sécurité : antivirus, pare-feu, système de détection des intrusions (IDS) et solution de gestion des informations et événements de sécurité (SIEM)

CHALLENGE

- Détecter les menaces avancées diffusées par le trafic Web susceptibles d'échapper aux solutions de sécurité en place et de s'immiscer sur le réseau d'entreprise
- Fournir des renseignements exploitables pour aider l'équipe en charge de la sécurité à établir la priorité des menaces
- Identifier une solution unique pouvant être déployée dans un environnement distribué tout en s'intégrant à l'infrastructure de sécurité existante et capable d'assurer une protection tout au long du processus d'attaque

SOLUTION

- Cisco CWS Premium, qui inclut toutes les fonctionnalités de Cisco CWS Essentials
- Cognitive Threat Analytics (CTA) et Advanced Malware Protection (AMP) pour automatiser la recherche des menaces à risque élevé sur le trafic Web et assurer la visibilité des attaques sophistiquées actives sur le réseau d'entreprise

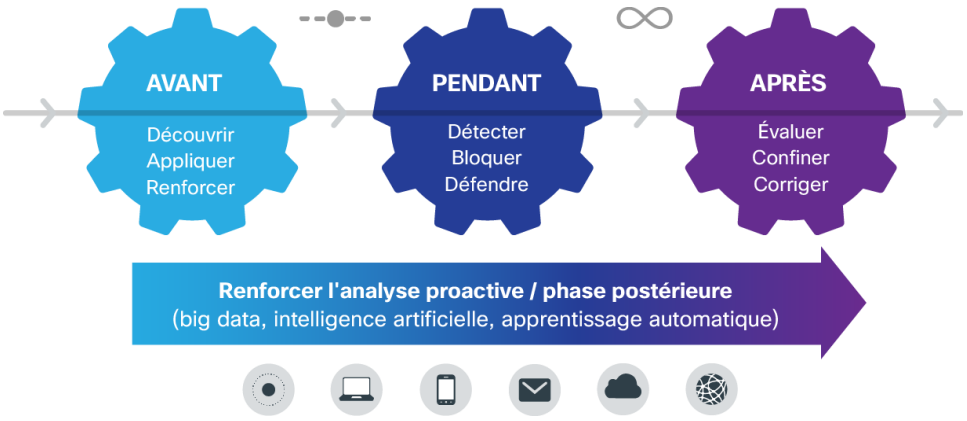
LES RÉSULTATS

- Identification et éradication des programmes malveillants persistants et non détectés précédemment
- Protection contre les menaces tout au long du cycle de l'attaque
- Possibilité pour l'équipe de sécurité du client de se concentrer sur les menaces prioritaires

[1] *Rapport annuel Cisco 2014 sur la sécurité (en anglais) :* http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.
[2] Ibid.
[3] Ibid.
[4] Ibid.

Dans ce contexte où les menaces sont toujours plus complexes et ne cessent d'évoluer, une nouvelle approche de la sécurité du contenu tend à privilégier la détection par rapport à la défense. Aujourd'hui, les entreprises doivent se tourner vers l'analyse des contenus et comportements suspects et vers la recherche avancée de preuves informatiques pour avoir une meilleure visibilité des menaces déjà présentes sur leurs réseaux ; c'est ce que l'on appelle la phase « postérieure » de l'attaque.

Figure 1. Un nouveau modèle de sécurité : sécurité continue après l'attaque



Cisco® Cloud Web Security (CWS) aide les entreprises à assurer une sécurité continue sur l'ensemble du réseau étendu. Variante de Cisco Web Security basée dans le cloud, la plate-forme Cisco CWS étend la sécurisation aux terminaux mobiles et aux environnements distribués. Elle protège les utilisateurs grâce à des informations sur les menaces collectées au niveau mondial et à des fonctions de défense optimisées. Elle assure également la protection des utilisateurs itinérants. Dotée de toutes les fonctionnalités de Cisco CWS Essentials, Cisco Web Security intègre également deux moteurs innovants de détection des programmes malveillants qui automatisent la recherche des menaces à haut risque au niveau du trafic Web :

- **Cognitive Threat Analytics (CTA)** est un système d'analyse des comportements du réseau en temps quasi réel qui tire parti de l'apprentissage automatique et de statistiques avancées pour repérer toute activité inhabituelle sur un réseau (indicateurs de compromission (IOC)). CTA repère les anomalies et oriente ensuite les analystes de sécurité vers les problèmes potentiels, ce qui permet à la fois de réduire leur charge de travail et de définir la priorité des menaces.
- **Advanced Malware Protection (AMP)** utilise des analyses de réputation de fichiers, de sandboxing et rétrospectives pour identifier et stopper les menaces à tous les stades des attaques.

L'association de ces solutions permet à CWS Premium d'identifier de nouveaux biais de contrôle-commande auparavant non détectés par le secteur de la sécurité.

Cette étude de cas examine comment CWS Premium a aidé une société pétrolière et gazière internationale :

- Visibilité accrue face à un volume de trafic Web important et en constante augmentation (plus de 35 millions de requêtes HTTP/HTTPs par jour)
- Mise à disposition d'informations sur les menaces exploitables permettant aux équipes de sécurité d'établir plus facilement la priorité des menaces
- Déploiement d'une solution unique qui s'intègre à l'infrastructure de sécurité existante et qui assure une protection tout au long du cycle de l'attaque, c'est-à-dire avant, pendant et après l'incident

Solution

Cisco a recommandé au client d'effectuer une mise à niveau vers CWS Premium, qui inclut les moteurs CTA et AMP, afin de bénéficier d'une visibilité accrue sur son réseau et d'aider l'équipe de sécurité à catégoriser les menaces.

L'analyse rétrospective d'AMP permet de détecter les fichiers habilement déguisés et les programmes malveillants sophistiqués considérés comme « sains » lorsqu'ils ont traversé les lignes de défense du périmètre. AMP alerte sur-le-champ l'administrateur de la sécurité et lui permet de voir quel utilisateur sur le réseau est susceptible d'avoir été contaminé et à quel moment.

Parallèlement, CTA détecte les menaces les plus furtives qui ont réussi à s'infiltrer et qui opèrent activement sur le réseau d'entreprise. Ce système innovant de détection des programmes malveillants fait appel à l'analyse comportementale et à la détection des anomalies pour identifier les terminaux compromis. CTA repose sur des méthodes avancées d'analyse statistique et sur l'apprentissage automatique pour identifier séparément les nouvelles menaces, en apprenant de ce qu'il voit et en s'adaptant au fil du temps, sans nécessiter d'ajustement ni de configuration.

CTA a identifié une preuve d'activité d'un programme malveillant sur le réseau du client et l'a signalée. Le programme en question se composait d'un ensemble de modules contrôlés par une entité malveillante. En l'occurrence, la charge utile était le rançongiciel CryptoLocker. Ce programme malveillant sophistiqué chiffre les fichiers présents sur les ordinateurs des victimes et verrouille les appareils jusqu'à ce qu'une rançon soit versée.[5]

Comme l'indique la figure 2, le pirate a utilisé une infrastructure de contrôle-commande pour lancer l'attaque. Cette campagne s'est déroulée en quatre étapes clés :

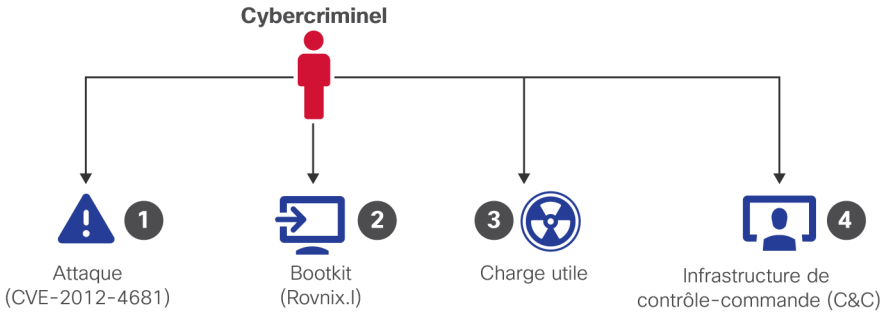
Étape 1 Le pirate a utilisé une attaque (CVE-2012-4681) pour tirer parti d'une vulnérabilité du composant Java Runtime Environment (JRE) dans la mise à jour Oracle de Java 6 vers Java SE 7. Il a ainsi pu exécuter du code à distance tout en échappant à l'administrateur de la sécurité.

Étape 2 Le bootkit (Rovnix.I) s'est ensuite installé sur l'ordinateur pour assurer une présence permanente.

Étape 3 La charge utile a alors été libérée, rendant le programme malveillant pleinement opérationnel. (En l'occurrence, la charge utile était le rançongiciel CryptoLocker.)

Étape 4 Enfin, l'attaque a créé des biais de contrôle-commande afin de maintenir l'opération active.

Figure 2. Les quatre étapes clés de l'attaque

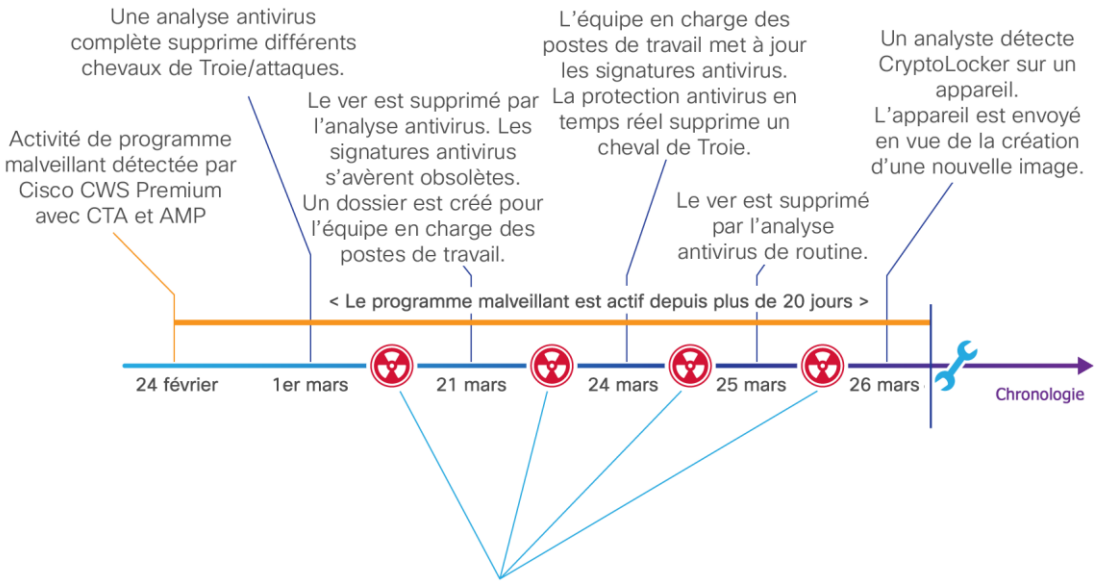


[5] Le malvertising, procédé utilisé pour diffuser des programmes malveillants, a joué un rôle majeur dans la diffusion de CryptoLocker, qui a depuis lors été neutralisé. Très répandus, le malvertising et les rançongiciels sont utilisés par les cybercriminels pour lancer des campagnes extrêmement ciblées via le Web. Pour plus de détails, consultez notre rapport semestriel 2014 sur la sécurité (en anglais) : http://www.cisco.com/web/offer/grs/190720/SecurityReport_Cisco_v4.pdf.

L'équipe de sécurité du client a tenté de résoudre la menace avec des programmes antivirus. Cependant, comme il s'agissait d'une infection par rootkit, le programme malveillant était profondément ancré dans le système contaminé. Les antivirus ne pouvaient dès lors l'éliminer que partiellement. CTA a ainsi continué d'informer l'équipe de sécurité de la présence d'une activité malveillante persistante jusqu'à l'éradication totale de l'infection.

La figure 3 illustre la chronologie complète, depuis la détection de l'activité du programme malveillant jusqu'à la résolution de la menace.

Figure 3. Chronologie de l'activité du programme malveillant : de la détection à la résolution



La situation qu'a connue le client démontre l'importance du travail de CWS Premium dans la phase postérieure de l'attaque. Elle met également en évidence toute la difficulté de stopper des attaques sophistiquées en utilisant uniquement des antivirus. Le système CTA a identifié la présence des biais de contrôle-commande actifs. En outre, il a identifié plusieurs autres domaines utilisés dans l'exfiltration des données. De telles infections sont la preuve incontestable de failles de longue date dans l'infrastructure du client.

Résultats

Dans le monde actuel, où les équipes de sécurité sont amenées à gérer quotidiennement un nombre élevé d'incidents, nous ne pouvons pas nous permettre de commencer à rechercher une aiguille dans une meule de foin. Les équipes de sécurité ont besoin d'aide pour se focaliser sur les attaques les plus sophistiquées. Or, CTA a été spécialement conçu pour détecter et hiérarchiser ces attaques.

Dans le cas de l'infection du client par le rançongiciel CryptoLocker, CWS Premium a détecté l'activité suspecte et a appliqué les informations de sécurité existantes pour bloquer certains biais de contrôle-commande créés sur le périphérique infecté. Le pirate a alors utilisé une adresse IP supplémentaire avec une réputation inconnue. Ce nouveau biais est, quant à lui, resté opérationnel tout au long de l'infection. Cet exemple met en avant les avantages (le blocage automatique), mais aussi les inconvénients (les nouveaux biais non bloqués) de la détection

basée sur la réputation Web et sur les signatures lorsqu'elle est utilisée seule, et souligne l'importance d'une protection continue après l'attaque.

Vous trouverez ci-dessous l'analyse des biais de contrôle-commande identifiés par le système CTA de CWS Premium, ainsi que des exemples de statistiques et de requêtes du trafic Web.

Tableau 1. Infrastructure d'une attaque

Ordre	Serveur distant	Adresse IP de destination	Pays de destination	Nombre de demandes	Statut de l'activité
1	Serveur C&C n° 1	109.XXX.XXX.XXX	Pays-Bas	17 (tentatives)	Bloquée par la réputation Web
2	**Serveur C&C n° 2**	**94.XXX.XXX.XXX**	**Luxembourg**	**75**	**CANAL ACTIF**
3	Serveur C&C n° 3	fistristy.com	Luxembourg	175 (tentatives)	Bloquée par la réputation Web
4	Serveur C&C n° 4	ffeed5.com	Russie	7 (tentatives)	Bloquée par la réputation Web

Tableau 2. Menaces identifiées par CTA qui ont ensuite été supprimées de l'appareil

Nom de la menace	Suppression
Worm/Cridex	19 mars
Worm/Cridex.E	19 mars
Trojan/Tesch.B	19 mars
Java Exploit/CVE-2012-4681	19 mars
TrojanDownloader:Win32/Upatre	19 mars
Worm/Cridex	21 mars
Trojan:Win32/Viknok.C	24 mars
Worm/Cridex	24 mars
Crypto Defense	26 mars

Communication avec le serveur C&C n° 1 (109.XXX.XXX.XXX)

Caractéristiques de la communication :

- Sur les 17 requêtes envoyées sur ce serveur, toutes étaient des communications de contrôle-commande bloquées par le système de réputation.
- Ces requêtes ont été détectées par CTA comme des tentatives d'utilisation de la chaîne URL comme canal de communication (contrôle-commande). L'URL (indiquée plus bas sous « Exemple de requête HTTP (anonymisée et tronquée) ») représente un message codé. Une structure similaire à la chaîne URL (adresse IP/m/lbQ.*) a été partagée par plusieurs URL utilisées dans cette attaque. Le blocage de la communication par le système de réputation fournit davantage de preuves contextuelles.
- Le pirate a également configuré un deuxième biais de contrôle-commande sur un serveur qui ne faisait pas encore partie du flux de réputation afin de s'assurer que le programme malveillant reste opérationnel. L'URL en tant que telle est un message codé.

Exemple de requête HTTP (anonymisée et tronquée)

http://109.XXX.XX.XXX/m/IbQXXXVjjpcE6+54HXXXdmmGcNZxtMZdvqyB5EkJAUmL/1sOXXXvq5zzXtIu9SzgnJhjWlxdE7FiqDEYFm5A+TPlXXXQpGhxGu0r3WLZoX1KHnCShKJDAufwiISy69wApgn4e79NFw/108XXX.g+fq4XXXOTYke6uhGHDOEeqje76v7z7i+wgqXXXFBuMz5k08yocxOH63bwQ9JMfwy8uNRM…

Communication avec le serveur C&C n° 2 (94.XXX.XXX.XXX)

Caractéristiques de la communication :

- Sur 75 requêtes envoyées à ce serveur, toutes étaient des requêtes de contrôle-commande.
- Deux tentatives de contrôle-commande ont été détectées par CTA dans le **trafic HTTP vers l'adresse IP (aucun domaine spécifié).** Ce type de comportement signale une ou plusieurs requêtes anormales représentant une communication hors séquence vers une adresse IP saine. Une telle activité peut servir à vérifier qu'un programme malveillant est toujours actif ou à lui permettre d'exfiltrer des données et de recevoir des instructions complémentaires de son infrastructure (de contrôle-commande) malveillante. Ce genre de trafic n'est pas lié à une activité normale de navigation sur Internet.
- Les solutions basées sur les signatures et sur la réputation n'ont permis de détecter aucune de ces 75 requêtes de contrôle-commande.

Exemple de requête HTTP (anonymisée et tronquée)

http://94.XXX.XXX.XXX/m/IbQXXXVjj7iA+O54XXXodmmGcNZxtMZdvqyB5EkJAUmLb3pvGIRvqizzXtIu9SzgnJhjWlxdE7FiqDEYFm5A+TPlXXXQpGhxGu0r3WLZoX1KHnCShKJDAufwiISy69wApgn4e79NFw/108XXXog+fq4XXXaE0qfJf1FwaIZJKnDc7U0H30+XkiXXXIApkslTo5yvM0TkHrZncwIvumxLCQ+fq4XXXOT…

Communication avec le serveur C&C n° 3 (fistristy.com)

Caractéristiques de la communication :

- Sur 175 requêtes envoyées au domaine fistristy.com, toutes étaient des communications de contrôle-commande.
- Toutes ces requêtes ont été bloquées par les solutions de signatures et de réputation Web.

Exemple de requête HTTP

hXXp://fistristy.com/aa/

Communication avec le serveur C&C n° 4 (ffeed5.com)

Caractéristiques de la communication :

- Sur 7 requêtes envoyées au serveur ffeed5.com, toutes étaient des communications de contrôle-commande bloquées par CWS Premium.
- CTA a détecté six requêtes de la catégorie **Trafic HTTP anormal**. Cette catégorie de comportements inclut les comportements de programmes malveillants qui ne correspondent pas aux règles comportementales établies par l'analyse CTA continue. Le terme « règles » fait référence à l'état des modèles statistiques établis par le système CTA, qui « apprend » les tendances et les caractéristiques du trafic Web analysé. CTA ajuste automatiquement ces règles en fonction des changements du réseau (par exemple, la nuit et le jour) afin de garantir les meilleurs résultats de détection possibles.
- CTA utilise des méthodes d'analyse du comportement du réseau à long terme pour mettre en corrélation des activités à première vue isolées. Il compare ensuite ces données aux comportements d'utilisateurs individuels sur l'ensemble du réseau du client afin d'affiner ses capacités de détection des menaces furtives et persistantes.

Exemple de requête HTTP

hXXp://ffeed5.com/cmd?version=1.5&aid=555&id=24c6b407-5010-4d8d-a266-ffdac7d6f901&os=6.1.7601_1.0_64

Conclusion

Avec un réseau comptant plus de 15 000 utilisateurs et générant plus de 35 millions de transactions Web par jour, en moyenne, l'équipe de sécurité du client avait besoin d'une solution plus simple pour surveiller l'activité et hiérarchiser les événements de sécurité. Le client avait également besoin d'une solution capable de bloquer les menaces et d'identifier rapidement celles susceptibles de passer entre les mailles du filet. Le personnel de sécurité devait pouvoir être alerté de la présence d'une activité suspecte persistante jusqu'à ce que la menace ait été entièrement écartée.

Parce qu'il a déployé CTA, inclus dans la solution Cisco CWS Premium, le client dispose désormais d'un système d'analyse des comportements du réseau en temps quasi réel qui tire parti de l'apprentissage automatique et de statistiques avancées pour identifier les indicateurs de compromission sur le réseau. Dans le cas de la contamination par le rançongiciel CryptoLocker, CTA a continué d'informer l'équipe de sécurité sur l'activité malveillante jusqu'à ce que l'infection ait été entièrement éradiquée. Enfin, grâce à la visibilité qu'offre CTA sur le comportement des programmes malveillants, l'équipe de sécurité du client peut concentrer son attention sur les menaces prioritaires avant, pendant et après l'attaque.

Plus d'infos

Doté des moteurs CTA et AMP, Cisco CWS Premium s'inscrit dans le cadre de la stratégie de Cisco qui vise à assister les entreprises pour faire face aux problèmes de sécurité connus et émergents. L'objectif est de les aider à détecter, à comprendre et à neutraliser les menaces grâce à une analyse continue et à des informations sur la sécurité livrées en temps réel depuis le cloud et partagées sur toutes les solutions de sécurité pour une efficacité accrue. Grâce à l'association de ces trois solutions, CWS Premium peut identifier de nouveaux biais de contrôle-commande jusqu'à lors non détectés par les solutions de sécurité classiques et aider les entreprises à faire face aux menaces tout au long du cycle de l'attaque.

Pour en savoir plus sur l'offre de services CWS Premium, rendez-vous sur http://www.cisco.com/go/cws.

Pour plus d'informations sur CTA, rendez-vous sur http://www.cisco.com/go/cognitive.

Pour plus d'informations sur AMP, rendez-vous sur http://www.cisco.com/go/amp.

Siège social aux États-Unis
Cisco Systems, Inc.
San Jose, Californie

Siège social en Asie-Pacifique
Cisco Systems (États-Unis) Pte, Ltd.
Singapour

Siège social en Europe
Cisco Systems International BV Amsterdam.
Pays-Bas

Cisco compte plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et numéros de fax sont répertoriés sur le site de Cisco, à l'adresse **www.cisco.com/go/offices**.

Imprimé aux États-Unis C36-733153-00 10/14