Certificate Transparency ou comment un nouveau standard peut améliorer votre veille sur certaines menaces

Christophe Brocas et Thomas Damonneville
christophe.brocas@cnamts.fr
thomas.damonneville@cnamts.fr

Caisse Nationale d'Assurance Maladie

Résumé. Certificate Transparency [6] est un projet qui vise à obliger les autorités de certifications à publier tous les certificats publics qu'elles signent dans des dépôts intègres et accessibles à tous. Cet article montre comment tirer parti de cette nouvelle obligation pour améliorer sa veille sur certaines menaces. Nous donnerons les cas d'usage où Certificate Transparency permet de détecter des émissions anormales de certificats sur nos noms de domaines et de découvrir des sites malveillants hébergés sous des noms de domaines « proches » des nôtres. Enfin, nous présenterons un retour d'expérience opérationnel et l'outillage open source que nous avons développé pour faciliter cette détection et l'investigation qui s'en suit.

1 Certificate Transparency : quelle réponse pour quel risque ?

1.1 Le risque

Le modèle de confiance des certificats publics X.509 implique notamment que toute autorité de certification (AC), dont les certificats racines ou intermédiaires sont présents dans vos navigateurs ou vos systèmes, puisse émettre un certificat pour votre organisation. Dans la plupart des cas, cette émission est opérée de manière tout à fait légitime.

Cependant, cette émission peut aussi être abusive si l'AC ne contrôle pas correctement un demandeur malveillant ou si l'AC se fait compromettre. Si ce risque est avéré pour un de vos domaines, il devient alors possible pour un attaquant, situé entre le client et votre serveur (MITM), d'usurper votre identité.

Ce type d'émissions a notamment pu être observé lors de la compromission ou d'incidents chez plusieurs AC [12] comme Diginotar, Comodo ou encore Symantec.

À ce risque s'ajoute le fait que votre organisation n'avait aucun moyen, jusqu'à maintenant, d'être avertie de ces émissions frauduleuses.

1.2 La réponse

Le principe de Certificate Transparency (CT) est d'obliger les AC à consigner dans plusieurs journaux CT chaque nouveau certificat public qu'elle crée. Ces journaux ont les caractéristiques liées à leur structure de stockage, les arbres de Merkle : garantie cryptographique d'intégrité et capacité à ne faire qu'ajouter des données sans pouvoir en supprimer ou en modifier.

Ces journaux étant librement consultables par quiconque, chaque organisation est donc désormais en capacité de vérifier si les certificats publics émis pour ses domaines sont tous légitimes.

Décrivons rapidement le contexte de cette initiative. Certificate Transparency est une proposition de Google qui a notamment créé la première version d'une RFC (6962) pour cette initiative. Depuis, malgré la reprise par l'IETF de la RFC [8], Google assure toujours le leadership de CT : fourniture d'une implémentation open source des journaux, validation des postulants à opérer des journaux CT, contrôle de la sécurité des journaux CT actuellement en production, leur éventuelle disqualification, proposition des dates de mise en œuvre des grandes étapes.

Concernant le planning de déploiement de Certificate Transparency, l'obligation de dépôt des certificats à validation étendue dans les journaux CT a été rendue effective le 1er janvier 2015. Pour tous les autres certificats, cette obligation a été fixée au 30 avril 2018 par Google [5].

La conséquence pour les AC ne suivant pas ces recommandations sera de voir rejetés ses certificats dans Chrome sous la forme d'une page d'alerte de sécurité mentionnant le fait que le certificat en question n'est pas compatible Certificate Transparency [7].

L'implémentation de Certificate Transparency dans Firefox peut être suivie au travers de ce bug [9]. Lors de la rédaction de cet article (mars 2018), l'implémentation technique est opérationnelle mais la politique de rejet n'est ni définie ni implémentée.

1.3 Fonctionnement de Certificate Transparency

Dans la figure 1, nous décrivons le fonctionnement de Certificate Transparency dans son implémentation la plus commune, à savoir avec fourniture des preuves de dépôt au travers d'une extension X.509v3 dans le certificat :

Étape 1 : Le mainteneur du site web commande un certificat public pour son site auprès d'une AC.

Étape 2 : Après les vérifications d'usage, l'AC émet un précertificat et le soumet dans plusieurs journaux CT.

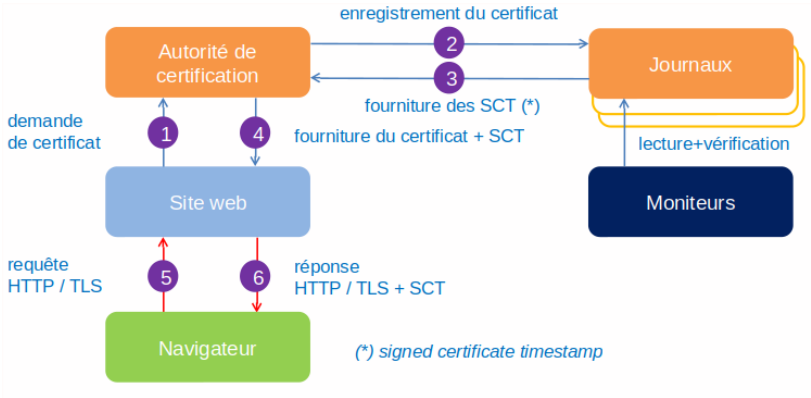

Fig. 1. Fonctionnement standard de Certificate Transparency

Étape 3 : En retour, les journaux lui donnent une preuve cryptographiquement signée de ce dépôt, un Signed Certificate Timestamp (SCT).

Étape 4 : L'AC signe le précertificat concaténé aux SCT et remet ce certificat à son client. Techniquement, les SCT sont stockés dans une extension X.509v3 du certificat. Deux autres méthodes de communication des SCT existent, nous les décrivons ci-après.

Étapes 5 et 6 : Lors du handshake TLS, le site web envoie le certificat contenant les SCT et le navigateur vérifie si le certificat a bien été déposé dans plusieurs journaux CT valides.

Moniteurs : Il ne s'agit pas là d'une étape du processus d'émission de certificats compatibles CT. Figurent ici des services de surveillance des journaux CT qui permettent de faire des recherches sur les certificats consignés dans ces journaux. Nous allons détailler l'usage de ces services en vue d'améliorer notre veille sur certaines menaces.

L'étape de communication des SCT au navigateur peut aussi se faire de deux autres manières :

via une extension TLS dédiée : dans ce cas, c'est le mainteneur du site web qui soumet aux différents journaux CT le certificat qu'il a reçu de l'AC. Ensuite, il distribue les SCT, envoyés par les journaux CT, auprès du navigateur via une extension TLS dédiée.

via l'extension TLS gérant l'OCSP stapling : le mainteneur du site requête le point de distribution OCSP de l'AC et distribue auprès du navigateur les SCT qu'il obtient en réponse via l'extension TLS gérant l'OCSP stapling.

Ces deux méthodes de distribution impliquent des modifications du fonctionnement des navigateurs, des serveurs web et de la manière de gérer son site et ses certificats par le mainteneur du site.

À la vue de ces contraintes, la manière de distribuer les SCT qui se généralise est l'incorporation des SCT au sein du certificat via une extension X.509v3.

2 Outillage disponible

Pour effectuer une surveillance des certificats déposés dans les journaux CT, il existe trois types d'outillage que nous pouvons exploiter :

- recherche interactive de certificats : l'outil CRT de Comodo [2] ;
- recherche interactive de certificats et programmation de surveillance de domaines avec notification : outils CT de Facebook [4], service CertSpotter de SSLMate [10] ;
- les moniteurs de journaux CT fournissant des API que l'on peut utiliser depuis nos scripts : le service CertStream [1].

3 Notre usage

3.1 Nos objectifs

Lors de l'annonce en avril 2017 par Google de la généralisation de l'exigence de Certificate Transparency pour avril 2018, nous avons réfléchi aux applications possibles au sein de notre entreprise. Nous avons pu déterminer deux types de surveillance que nous pourrions mettre en place grâce à CT.

3.2 La surveillance des certificats émis sur nos domaines

Le premier usage que nous avons identifié est celui d'une surveillance de la conformité des émissions des certificats sur nos domaines DNS et par extension, la maîtrise des services mis en ligne par notre organisation. Au sein de notre DSI, une entité a notamment pour mission de centraliser les achats de certificats publics pour les besoins des projets. Elle connaît donc les certificats qui sont commandés et peut, par rapport à une liste de certificats émis, détecter ceux qui ne sont pas passés par eux. Il est intéressant de fournir à cette équipe un moyen efficace d'assurer ce contrôle.

Les risques couverts par cette surveillance sont :

1. L'émission frauduleuse ou non souhaitée d'un certificat sur un de nos domaines légitimes. Cela couvre les 2 risques suivants :
   - L'autorité de certification n'a pas correctement vérifié la légitimité du demandeur et a émis un certificat à un tiers non habilité.

   - L'infrastructure DNS a été compromise. L'attaquant peut alors demander un certificat pour un nom d'hôte de notre organisation à une AC pratiquant la validation automatisée comme Let's Encrypt. L'attaquant peut ensuite mettre en ligne son service malveillant sur son serveur tout en usurpant notre identité auprès de nos utilisateurs avec le certificat. Si une alerte d'émission de certificat est générée et que nous la surveillons, nous sommes en capacité de détecter l'incident et de réagir.
2. L'émission légitime d'un certificat et une éventuelle mise en ligne d'un service associé mais en dehors de tout cadre préconisé.

La solution que nous avons retenue pour couvrir ces risques est la mise en œuvre, sur le service CertSpotter, d'une surveillance des certificats concernant les noms de domaines de notre entreprise. Lors de l'émission d'un certificat concernant un de ces noms de domaines, nous recevons un courrier électronique.

3.3 La surveillance des certificats émis sur des domaines « voisins »

Jusqu'à maintenant, une équipe de veille sécurité n'avait que peu de moyens pour détecter des domaines malveillants « voisins » de ses domaines DNS légitimes, comme ceux utilisés lors d'attaques de phishing. La difficulté est encore accrue pour découvrir les noms d'hôtes des services malveillants.

La possibilité de surveiller l'émission des certificats permet d'avoir une source d'informations qualifiées, à la fois sur les domaines malveillants mais aussi sur les noms réels des services utilisés lors de ces attaques. Et ce, souvent, avant même la mise en œuvre des sites web en question.

Le risque couvert ici est celui des attaques, visant nos utilisateurs, hébergées sous un domaine proche d'un de nos domaines DNS et utilisant HTTPS.

La solution que nous avons retenue pour couvrir ce risque est de développer nos propres scripts utilisant l'API de CertStream.

3.4 Outillage développé

Nous avons donc développé **CertStream Monitor** un outillage de surveillance des émissions de certificats sur des domaines « proches » de nos noms de domaines ou de nos métiers. Cet outillage, décrit à la figure 2, est disponible sous licence libre sur notre compte GitHub [3].

Depuis la publication fin 2017 du service CertStream – accessible gratuitement – de consolidation et de publication des CTL (Certificate

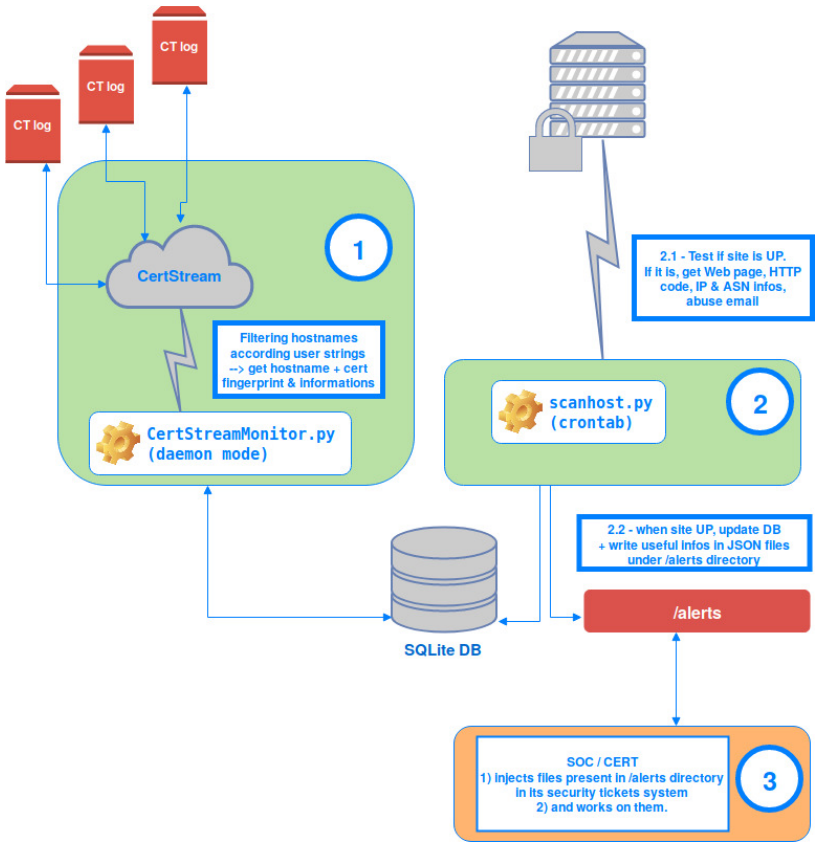

Fig. 2. Schéma de fonctionnement de CertStream Monitor

Transparency Logs) par la société Cali Dog Security, il est désormais plus aisé de récupérer, au fil de l'eau, les déclarations de certificats émis par différentes autorités de certification. Sont aussi mis à disposition une API et des bibliothèques permettant de surveiller leur flux de données afin de pouvoir automatiser la détection de certificats émis sur des domaines liés aux – ou approchants des – domaines nous appartenant déjà.

Un **premier script** `CertStreamMonitor.py` récolte des informations pertinentes pour notre organisme.

Ce script permet, à l'aide d'un jeu d'expressions régulières, de récupérer les certificats émis pour des domaines approchants des nôtres. Ces certificats peuvent être utilisés par des services web malveillants ciblant nos utilisateurs et assurés. Nous stockons en base les noms de domaines couverts par le certificat, l'AC émettrice, les dates de validité et le numéro de série du certificat.

Un **second script**, `scanhost.py`, permet de vérifier quand et si le site correspondant au certificat est en ligne. Si c'est le cas, le script récupère l'adresse IP, le titre de la page web, les informations concernant l'AS [11]

gérant l'adresse et l'adresse abuse de l'AS. Il met à jour la base de données et consigne les informations récupérées dans un fichier écrit dans un répertoire d'alertes.

Il reste ensuite à exploiter les informations consignées dans ces fichiers.

3.5 Résultats obtenus

Nous avons pu détecter 105 noms d'hôtes qualifiés et sans doublon sur une période d'un mois et demi. Les types de sites remontés sont les suivants :

- Des sites au nom «voisin» du nom de domaine de notre entreprise mais légitimes. Exemple : `social-ameli.fr`. Après analyse des données du WHOIS, le domaine appartient bien à une de nos caisses primaires (i.e. représentants locaux de l'entreprise nationale). Il s'agit donc d'une création de site utile pour l'organisme en question mais déployé sans concertation et sans suivre aucune recommandation interne.
- Des sites malveillants et/ou fournissant des services payants visant nos utilisateurs. Exemple : `cpam-75.fr`. L'objet du site est de s'insérer entre nos utilisateurs et l'Assurance Maladie afin de pousser nos utilisateurs à utiliser des services téléphoniques très coûteux (2,99 € l'appel + 2,99 € par minute).
- Des sites d'hameçonnage utilisant l'image de notre entreprise.

3.6 Limites de la démarche

La surveillance reposant sur la scrutation des certificats émis est une source d'informations qualifiées mais elle comporte, bien entendu, des limites.

Cette surveillance ne nous apporte aucune visibilité sur les attaques utilisant des sites web uniquement accessible en HTTP. La surveillance ne nous aidera pas non plus si le nom de domaine du site malveillant ne contient pas de noms proches de nos noms de domaines ou de nos métiers. D'autre part, si le certificat détecté est un certificat de type wildcard, nous découvrons le nom de domaine malveillant mais pas le nom des services web malveillants. Enfin, si une AC compatible CT se fait corrompre, il se peut qu'un attaquant puisse faire signer un certificat sans générer un SCT. Le certificat en question n'apparaîtra jamais dans les journaux CT mais il générera une alerte de Sécurité, au moins sous Chrome.

4 Conclusion

Toute entreprise, petite ou grande, dotée ou non d'une entité dédiée à la veille de menaces, peut mettre à profit Certificate Transparency à peu de frais pour être informée de la délivrance de certificats de manière anormale ou non tracée sur ses domaines DNS. De même, elle pourra détecter les domaines DNS proches ainsi que les noms d'hôtes pouvant héberger des sites malveillants visant ses utilisateurs.

Les services en ligne, les API et nos scripts [3] sont disponibles. Il n'y a plus qu'à les utiliser pour surveiller ses noms de domaines, ou ceux approchant, et intégrer les alertes ainsi remontées dans ses processus de sécurité.

Références

1. Cali Dog Security. Service et API CertStream. `https://certstream.calidog.io/`.
2. Comodo. Portail de recherche Certificate Transparency CRT. `https://crt.sh/`.
3. Département Sécurité Caisse Nationale d'Assurance Maladie. CertStream Monitor. `https://github.com/AssuranceMaladieSec/CertStreamMonitor/`.
4. Facebook. Outils Certificate Transparency. `https://developers.facebook.com/tools/ct/`.
5. Google. Annonce de l'échéance de mise en oeuvre de Certificate Transparency en avril 2018. `https://groups.google.com/a/chromium.org/forum/#!msg/ct-policy/sz_3W_xKBNY/6jq2ghJXBAAJ`.
6. Google. Certificate Transparency. `https://www.certificate-transparency.org/`.
7. Google. Conséquences dans Chrome d'un certificat non compatible CT. `https://groups.google.com/a/chromium.org/d/msg/ct-policy/wHILiYf31DE/iMFmpMEkAQAJ`.
8. IETF. RFC 6962 bis. `https://tools.ietf.org/html/draft-ietf-trans-rfc6962-bis-27`.
9. Mozilla. Bogue permettrant de suivre l'implémentation de Certificate Transparency dans Firefox. `https://bugzilla.mozilla.org/show_bug.cgi?id=1355903#c4`.
10. SSLMate. Outils Certificate Transparency CertSpotter. `https://sslmate.com/certspotter/`.
11. Wikipedia. Autonomous System. `https://fr.wikipedia.org/wiki/Autonomous_System`.
12. Wikipedia. Autorités de certification, compromission et émission frauduleuse de certificats. `https://en.wikipedia.org/wiki/Certificate_authority#CA_compromise`.