Recherche d'indicateurs de compromission dans des journaux DNS chiffrés

Adam Oumar Abdel-Rahman, Olivier Levillain, Eric Totel

Recherche d'indicateurs de compromission dans des journaux DNS chiffrés

A. O. Abdel-rahman, O. Levillain, E. Totel

Contexte et objectif du projet PRESTO

Dans un contexte où le chiffrement se généralise, tant pour protéger les communications que les données stockées, certaines techniques de détection d'intrusions ou d'investigation numérique deviennent inopérantes. Plutôt que de remettre en cause l'utilisation omniprésente du chiffrement, le projet de recherche PRESTO a pour objectif d'explorer des mécanismes cryptographiques avancés pour permettre de concilier chiffrement et analyse de sécurité via un déchiffrement partiel et maîtrisé des données. Un des cas d'usage étudiés est l'investigation numérique (forensics), avec en particulier l'application au chiffrement des journaux DNS.

Cas d'usage DNS (stockage)

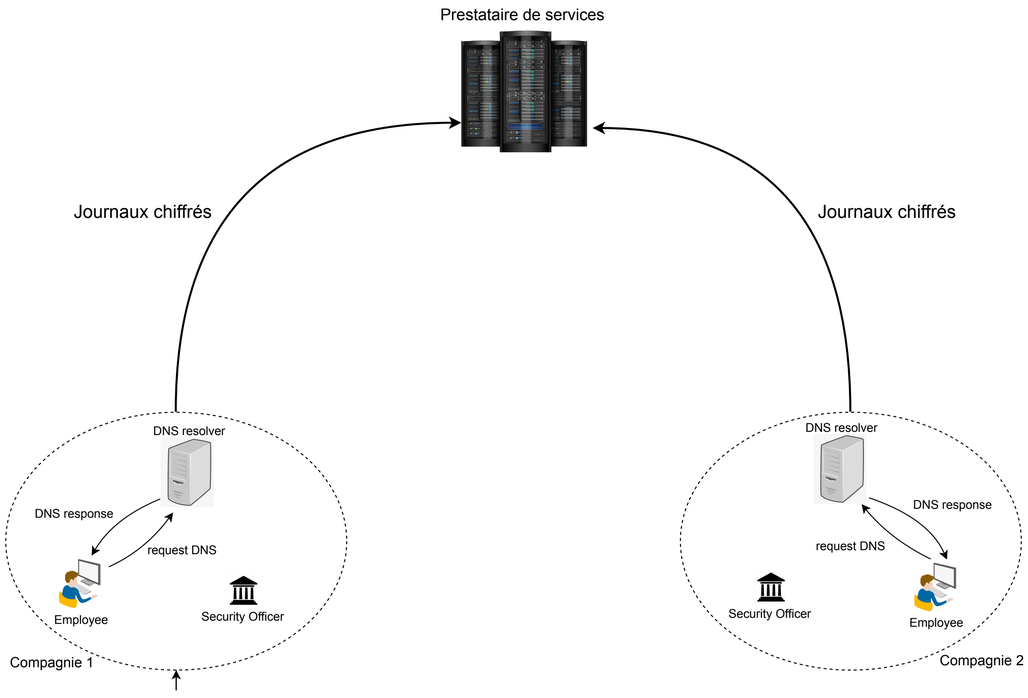
Nous avons une plateforme composée : — d'organisations avec des résolveurs DNS internes, et tels que les employés de chaque organisation utilisent les résolveurs DNS internes de leur organisation ; — d'un prestataire de services qui stocke les journaux chiffrés de ces organisations ; — d'une autorité générale en charge d'investigations (communiquer des IoCs et/ou générer des trappes permettant au prestataire de services d'analyser les journaux chiffrés).

Stockage de journaux DNS

Les journaux DNS sont enregistrés sous forme chiffrés. Trois schémas ont été étudiés dont un basé sur une approche asymétrique et deux autres basés sur des approches symétriques. La recherche dans les journaux chiffrés consiste à extraire les journaux DNS contenant un domaine ou une adresse IP donné dans une période donnée. Pour chaque requête DNS, les mots clés considérés sont le nom de domaine réqueté et les adresses IP retournées.

Schémas symétriques à l'aide des PRF Les mots clés sont utilisés pour construire des indexes qui seront associés aux journaux chiffrés et donc permettant un filtrage de journaux pertinents. le premier schéma est tel que les indexes sont construits de façon déterministe et le second est celui du [2] dont les indexes sont construits en rajoutant des aléas (probabiliste).

Schémas asymétrique à l'aide d'IBE (Identity Based Encryption[1]) Les mots clés sont utilisés comme des clés publiques et la trappe permettant l'analyse des journaux chiffrés est la clé privé associée.

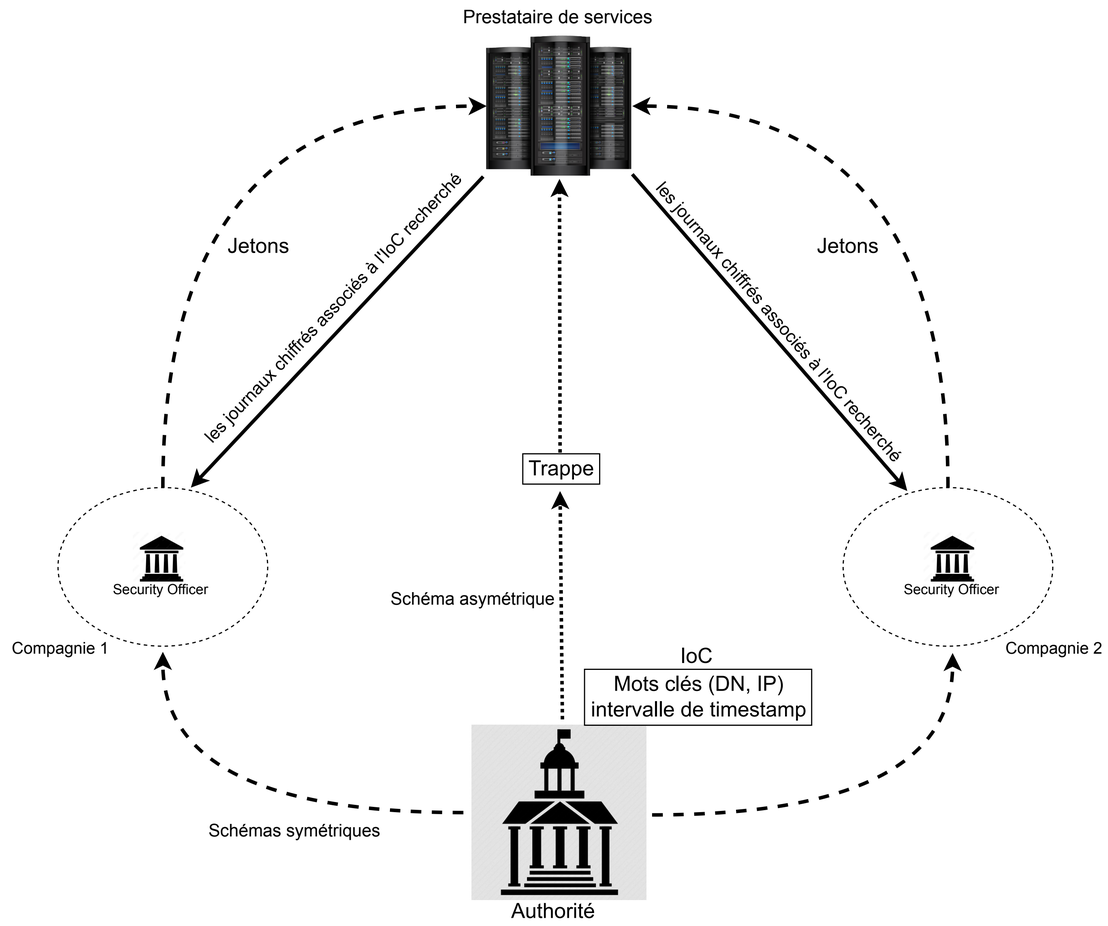


Cas d'usage DNS (Recherche d'IoC)

Journaux chiffrés à l'aide des schémas symétriques Chaque organisation crée ses jetons (dans le cas déterministe) associés au mot clé recherché et les envoie au prestataire de services. Dans le cas probabiliste, les organisations construisent les trappes nécessaires à l'analyse des journaux chiffrés et les envoient au prestataire.

Journaux chiffrés à l'aide d'IBE Dans asymétrique, l'autorité génère la trappe et l'envoie au prestataire de services.

Une fois l'analyse faite, le prestataire de services envoie à chaque organisation les résultats trouvés qui la concerne.



Partenaires du projet PRESTO

Financement ANR-19-CE39-0011

Références

[1] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. In Joe Kilian, editor, *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer, 2001.

[2] Brent Waters, Dirk Balfanz, Glenn Durfee, and Diana K. Smetters. Building an Encrypted and Searchable Audit Log. In *NDSS*, 2004.