Pourquoi s'équiper d'un EDR ?

Antonin Garcia, RSSI chez Veepee :

« En quelques secondes, nous pouvons initier des jobs de collecte à distance qui nous permettent de récupérer des artefacts, sans même que l'utilisateur ne le remarque. »

Veepee, ex vente-privee.com, est le pionnier de la vente événementielle en ligne en Europe. Ce retailer né en 2001 compte 5000 salariés et au moins autant de terminaux à protéger.

Antonin Garcia et Valentin Kiffer, respectivement **RSSI et Security Engineer,** expliquent à quels enjeux de sécurité ils sont confrontés et les raisons qui les ont poussés à s'équiper de **l'EDR HarfangLab.**

Antonin, quand vous êtes arrivé chez Veepee en tant que RSSI, quels ont été les principaux enjeux de sécurité auxquels vous avez dû répondre ?

Antonin Garcia : En 2019, fort de sa stratégie de développement européen initiée en 2006, et après les rachats des sociétés Privalia et Vente-exclusive en 2016, vente-privee.com a changé de nom et est devenue Veepee, une marque globale présente dans 10 pays.

Quand je suis arrivé, tous les services de ces entités étaient en cours de convergence : toutes les nouvelles infrastructures, les sites web, le back office, mais aussi la livraison, les entrepôts, toutes les fonctions support qui sont derrière. **Un des plus gros défis a été de faire converger ces trois entités vers une même vision de la sécurité.**

Mais ce qui est particulier chez Veepee, c'est le fait qu'on héberge, on déploie et on développe quasiment tous nos services en interne. Je pense que c'est une chance parce que nous restons en maîtrise sur notre Système d'Information, que nous avons beaucoup d'autonomie, mais également des experts techniques qui peuvent porter tous leurs services et innovations.

Vous avez énormément de données clients en votre possession, c'est une mine d'or pour de potentiels attaquants. Quelle est votre première préoccupation dans ce contexte ?

A.G : **Il s'agit clairement du ransomware,** surtout du fait que notre IT soit hébergée chez nous. Pour la petite histoire, fin 2020, nous avons été visés par le logiciel malveillant Emotet*.

C'était fin décembre, et à l'époque nous étions équipés d'un antivirus traditionnel. Nous avions sécurisé une grande partie de notre infra mais, manque de chance, c'est tombé sur une partie du SI où les politiques de sécurité n'avaient pas encore été alignées. Sur une partie du SI, des mécanismes de protection avaient été mis en place pour empêcher l'exécution du malware, mais sur une autre entité, ça ne l'était pas.

Nous étions coincés : nous avions l'empreinte du virus, mais nous n'avions pas la capacité de pouvoir la rentrer dans la base de données de l'antivirus. Il a donc fallu attendre plus de 48h pour que le support de l'éditeur agisse... Heureusement, seuls 4 postes de travail ont été touchés et la menace a été rapidement contenue à ce périmètre. Il n'y a donc eu aucune compromission des données de nos clients.

Comment avez-vous réagi pour prévenir la menace par la suite ?

A.G : Début 2021, nous avons déployé en urgence des services open source de collecte de télémétrie sur l'ensemble des terminaux, afin de disposer d'outils de forensics, c'est à dire de moyens pour effectuer de la recherche de compromissions a posteriori. Nous avons pu obtenir de la visibilité sur la totalité des postes de travail et des serveurs.

Nous avons organisé des campagnes de sensibilisation, et nous nous sommes dit qu'au moins, si on voyait un fichier Emotet écrit quelque part, nous pouvions intervenir et le supprimer. Donc avec la télémétrie, nous avions enfin la détection. **Mais le problème dans la seule détection, c'est que si quelque chose se lance, on ne peut pas réagir :** on sort le popcorn, on se fait chiffrer, puis rançonner.

Valentin Kiffer : De plus, si un poste était compromis, et que celui-ci était à l'autre bout du globe, nous devions passer par un technicien local. Or, c'est compliqué de leur demander de la collecte d'artéfacts : ce sont des choses qu'ils ne maîtrisent pas forcément, parce qu'ils ne viennent pas du domaine de la cybersécurité.

Qu'est-ce qu'il vous manquait pour adapter votre niveau de sécurité à vos besoins ?

A.G : L'antivirus fonctionne principalement avec une base de données qui doit être mise à jour régulièrement, et il est possible qu'il ne détecte pas une menace qui n'est pas déjà enregistrée dans sa base. Or, **aujourd'hui, on se fait attaquer par des malwares dont la signature n'est pas forcément connue.** Donc c'est un outil qui ne répond plus totalement aux nouvelles menaces.

Moi ce que je veux bloquer, ce sont des attaques et des éléments ciblés, du fichier, du hash ou de l'IP personnalisée. C'est ça qui nous a poussés à nous équiper de l'EDR HarfangLab. Je voulais surtout le moteur IoC (Indicators of Compromise), parce qu'on peut mettre le hash dedans, et tout bloquer en quelques secondes sur l'ensemble du parc.

V.K : En fait **il nous manquait vraiment le « R » de EDR** (Endpoint Detection & Response). Cela nous a permis de bénéficier d'une capacité de réponse que l'on n'avait pas avant avec l'EPP.

Qu'est-ce que cela a changé concrètement ?

V.K : Grâce à Harfanglab, **nous pouvons détecter des menaces qui étaient là depuis un certain moment, alors que notre EPP était passé à côté.** En plus de ça, nous sommes maintenant en capacité d'isoler une machine du réseau, de contenir la menace puis d'aller investiguer à distance dessus : savoir quand le malware a été déposé, ce qu'il a fait, comment il persiste, et d'y remédier. On avait des machines qui avaient des réminiscences d'infections, et là, sachant qu'on va pouvoir aller très loin dans la détection mais surtout dans les réponses, on est plus rassurés.

A.G : Valentin me disait l'autre jour : « Mais comment faisait-on avant d'avoir un EDR? ». Parce que la vraie question, une fois qu'on a détecté un problème, c'est : « Comment on investigue, comment on lance une procédure de remédiation ? ». L**à, en quelques secondes, nous pouvons initier des jobs de collecte à distance qui nous permettent de récupérer ces artefacts, sans même que l'utilisateur ne le remarque.** Et derrière, nous pouvons dérouler une investigation ou une analyse forensique complète, chose qu'on ne faisait pas avant. **Avec un EDR, on peut intervenir immédiatement et partout dans le monde, c'est vraiment le jour et la nuit.**

Note :
* Emotet est un logiciel malveillant de type cheval de Troie. Destiné à l'origine à dérober des informations bancaires, ses nuisances se sont ensuite diversifiées, notamment en tant que service de compromission initiale, qui peut être revendue aux organismes cybercriminels rançonneurs. Il est distribué principalement via des campagnes de phishing. Emotet utilise différentes techniques pour essayer d'échapper aux détections et aux analyses. Il est polymorphe, ce qui signifie qu'il peut changer sa représentation à chaque téléchargement, échappant ainsi aux détections basées sur les signatures.