Faculté des Sciences & Techniques — Université de Limoges

*Master 1ère année*

*Sécurité des Usages TIC*

Examen — mai 2019

*Durée : 1h30 — Tous documents autorisés*

## PKI — 15 points

### 1 – Attaque ShadowHammer : ASUS réagit et publie un outil de diagnostic

**15pts** Par Sébastien Gavois pour Impact-Hardware, le mardi 26 mars 2019 à 17:45

Des pirates ont utilisé des **serveurs d'ASUS** pour diffuser un programme malveillant **signé numériquement** avec un **vrai certificat du fabricant** ❶. Il ciblait ensuite des centaines de machines. Malgré la gravité de la situation, ASUS a finalement publié un communiqué revenant sur l'affaire.
Au cours de l'année dernière, une version frelatée de l'utilitaire « *ASUS Live Update* » a été téléchargée et installée sur des dizaines de milliers d'ordinateurs.
Problème, ce fichier et son **cheval de Troie** ❷ étaient signés numériquement avec un certificat valide du fabricant. Il ne s'agissait en fait que de la première vague d'une attaque dont le but était de « *cibler chirurgicalement un groupe d'utilisateurs inconnus, identifiés par les adresses MAC de leurs cartes réseau* ».
Elle s'est déroulée entre juin et novembre 2018, mais n'a été identifiée que récemment. Le pot aux roses a été révélé par Kaspersky grâce à l'ajout d'une nouvelle technologie de détection des menaces en janvier, puis confirmée par Symantec.

**Un faux Live Update signé et diffusé par ASUS**

« *Live Update* » est un petit programme installé par défaut sur les ordinateurs du fabricant et servant de passerelle pour les mises à jour des BIOS/UEFI, des pilotes, des applications maison, *etc*.
ASUS étant le cinquième plus gros fabricant de PC dans le monde (en volume), cette attaque pouvait potentiellement toucher un très grand nombre de machines et donc **faire de gros dégâts** ❸. « *Selon nos statistiques, plus de 57 000 utilisateurs des produits Kaspersky Lab ont installé cet outil qui contient une porte dérobée, mais nous pensons qu'il a pu être distribué à près d'un million de personnes* », explique Kaspersky.
Toujours selon Kaspersky, « *il s'agit d'une attaque très sophistiquée* ». La raison pour laquelle le virus est resté dans l'ombre aussi longtemps tient au fait que le programme était **signé avec des certificats légitimes** ❹, provenant par exemple d'« *ASUSTeK Computer Inc* », qui étaient **hébergés sur des serveurs officiels** comme `liveupdate01s.asus.com` et `liveupdate01.asus.com` ❺.
Ce n'est d'ailleurs pas un, mais **deux certificats** qui ont été utilisés. Le premier ayant **expiré** au milieu de l'année dernière, il a été remplacé par un autre en cours de route. Autant de faisceaux qui indiquent que les pirates avaient **un accès en profondeur** à au moins une partie du réseau d'ASUS ❻.

**Une première étape avant la frappe chirurgicale**

Tout aussi intéressant, cette attaque d'envergure n'était que la première étape d'une frappe chirurgicale ciblant « *seulement* » 600 ordinateurs, identifiés par leur adresse MAC ❼. Ces dernières étaient codées en dur dans les plus de 200 échantillons de l'application étudiés par Kaspersky.
Prudents, les chercheurs ajoutent tout de même que d'autres listes pourraient avoir été mises en place dans d'autres versions de l'utilitaire. Kaspersky a mis en ligne une site dédié afin de savoir si votre adresse MAC a été spécialement ciblée par ShadowHammer.
Pour le moment, les lieux, l'identité des machines et/ou des personnes visées ne sont pas précisés. Les chercheurs n'ont pas réussi à analyser en détail le fonctionnement de la seconde phase de cette attaque. En effet, le **serveur de contrôle a été fermé en novembre dernier**, avant que l'attaque ne soit découverte ❽. **Impossible** donc pour le moment de dire quel était le **but de cette seconde étape**.

**Après avoir fait l'autruche, ASUS réagit**

Kaspersky affirme avoir contacté ASUS le 31 janvier, bien avant que cette attaque ne soit rendue publique. Vitaly Kamluk, un des directeurs de Kaspersky, affirme à Motherboard qu'un employé a ensuite rencontré ASUS le 14 février, mais la société n'aurait pas vraiment réagi depuis et n'aurait « *même pas informé ses clients de ce problème* » ❾.

Pire encore, ASUS aurait **continué à utiliser l'un des certificats compromis** pour signer ses propres fichiers un mois après en avoir été informé par Kaspersky. Si elle a depuis cessé, elle n'aurait par contre **toujours pas révoqué ❿** les deux certificats en question. Contactée, ce matin, elle promettait un communiqué, qui vient d'être publié.
Elle y précise que « *les Menaces Persistantes Avancées (APT) sont des attaques à l'échelle nationale généralement perpétrées par certains gouvernements visant des organisations ou entités internationales plutôt que les utilisateurs grand public. «* ASUS Live Update *» est un logiciel propriétaire intégré aux notebooks ASUS pour maintenir les pilotes et firmwares ASUS à jour. L'attaque APT sur nos serveurs Live Update a permis aux pirates informatiques de placer un code malveillant dans certains de nos ordinateurs pour cibler un groupe spécifique et limité d'utilisateurs* ».
Une manière de minimiser le problème pour le grand public qui ne devrait ainsi pas se considérer comme visé, malgré l'ampleur de la faille. Le constructeur ajoute avoir pris contact avec les utilisateurs concernés et mis à jour **Live Update** (v3.6.8) ⓫ « *en y introduisant notamment de multiples mécanismes de vérification sécuritaire empêchant toute manipulation malveillante sous la forme de mises à jour logicielles ou autre* ».
Du **chiffrement de bout en bout** est également de la partie, ce qui ne semble **pas très utile** dans une situation où les certificats de la société et ses serveurs ont été **compromis ⓬**. ASUS incite ses clients à la contacter pour toute question et promet avoir « *mis à jour puis renforcé l'architecture logicielle de nos serveurs pour empêcher toute nouvelle tentative d'attaque* », sans plus de détails. Un outil de diagnostic a été créé, pour vérifier les systèmes impactés.

**Plus de détails à venir**
Kaspersky indique de son côté qu'il donnera plus de détails lors de son « *Kaspersky Security Analyst Summit* » qui se déroulera du 8 au 11 avril prochain à Singapour.
Dans tous les cas, « *cette attaque montre que la confiance que nous accordons, basée sur des noms connus et sur la validation par des signatures numériques, ne peut garantir une protection contre les logiciels malveillants* » ⓭, affirme Vitaly Kamluk en guise de conclusion.

**Questions :**

a. Quelles **garanties** apportent la signature numérique ❶ d'un programme diffusé par un constructeur sur les ordinateurs qu'il a fabriqué ? *(1pt)*

b. Qu'est ce qu'un « *cheval de Troie* » ❷ ? Pourquoi est-ce justifier dans le cas de l'attaque ShadowHammer ? *(1pt)*

c. Comment est-ce possible que l'attaque puisse faire « *de gros dégâts* » ❸ ? *(1pt)*
Est-ce que le système d'exploitation Windows 10 peut protéger contre ce genre d'attaque ?

d. Décrivez **comment**, à votre avis, cette attaque a été réalisée et comment les attaquants ont réussi à utiliser des « *certificats légitimes* » ❹ ? *(2pts)*

e. Décrivez comment l'ordinateur de l'utilisateur a pu considérer que les fichiers provenaient d'un hébergement sur des « *serveurs officiels* » ❺. *(2pts)*

f. Comment le certificat a-t-il expiré et pourquoi on soupçonne « *un accès en profondeur* » au réseau d'ASUS ❻ ? *(1pt)*

g. Qu'est-ce que cette adresse MAC ❼ et est-elle facile à récupérer ? Est-ce facile d'effectuer une « *frappe chirurgicale* » ? *(1pt)*

h. Quel rapport entre l'attaque et le « *serveur de contrôle* » ? Pourquoi sa fermeture empêche-t-elle de savoir quel était le but de l'attaque ❽ ? *(1pt)*

i. Est-ce que le comportement d'ASUS est conforme au RGPD ❾ ? Et pourquoi ? *(1pt)*

j. Est-ce que la révocation des certificats est-elle suffisante pour régler le problème ❿ ? *(1pt)*

k. En quoi une mise à jour de « *Live Update* » ⓫ est-elle nécessaire par rapport au changement de certificats compromis ? *(1pt)*
Quels mécanismes logiciels peuvent donner plus de confiance dans les certficats utilisés ?

l. Expliquez pourquoi un « *chiffrement de bout en bout* » n'est « *pas très utile* » en cas de certificats « *compromis* » ⓬ ? N'est-ce pas pourtant une garantie de sécurité ? *(1pt)*

m. Expliquez la remarque finale de Vitaly Kamluk ⓭. *(1pt)*
Quels conseils de sécurité donneriez vous à un usager pour aller au delà du seul « *cadenas vert* » de son navigateur ?

## Protocoles sécurisés – 5 points

**2 – 5pts** On s'intéresse au protocole « *Wide Mouth Frog* ». Il permet à un agent A d'envoyer une clé symétrique $K_{AB}$ à un agent B, via un serveur S.
On suppose que S est toujours honnête.

$A \rightarrow S : A, \{N_A, B, K_{AB}\}K_{AS}$
$S \rightarrow B : \{N_S, A, K_{AB}\}K_{BS}$

a. Donner les **propriétés** de secret, d'authentification (message, agent) et de fraîcheur que l'on peut attendre a priori d'un tel protocole.

b. Trouver une **attaque par rejeu** pour faire accepter une clé $K_{AB}$ par l'agent B bien qu'elle ait déjà servi.

c. Pour réparer le protocole, S enregistre maintenant tous les $N_A$ qu'il reçoit et s'assure qu'ils sont frais. De même, B enregistre tous les $N_S$ qu'il reçoit et s'assure qu'ils sont frais.
   1. **Expliquer pourquoi** cette contre mesure empêche l'attaque précédente.
   2. Montrez une **possibilité de rejeu** pour faire accepter quand même une clé $K_{AB}$ bien qu'elle ait déjà servie.
      *Indication : l'attaque tente de faire accepter la clé par A et non pas par B.*

d. Proposez une **correction** permettant d'empêcher l'attaque évoquée en 2.