Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 30 mai 2016
N° CERTFR-2016-ACT-022

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-022

1 - Mise en garde contre l'extorsion de fonds sous la menace d'attaques DDoS

Au cours des derniers mois, des attaques par déni de service distribué (ou "DDoS" pour "Distributed Denial of Service"), revendiquées par différents groupes d'attaquants ("DD4BC", "Lizard Squad" ou encore "Armada Collective"), ont fait l'actualité en paralysant les services d'acteurs majeurs appartenant à des secteurs d'activité variés, à travers le monde. Ces actions, souvent très médiatisées, ont été accompagnées d'une demande de rançon, avec la menace de subir des attaques de plus grande ampleur en cas de refus de paiement et la hausse de la rançon en cas de retard de versement des fonds.

Des signalements de menaces semblables ont récemment été transmis au CERT-FR mais, bien qu'étant revendiquées par ces mêmes groupes, celles-ci n'étaient pas pour la plupart précédées d'attaques. Pour tenter d'intimider leurs cibles et les inciter à verser des fonds, les auteurs de ces menaces profitent ainsi de la médiatisation des attaques majeures qui ont déjà été orchestrées.

Phénomène observé : la réception de courriels de menace

Dans les menaces récentes qui ont pu être observées par le CERT-FR, la cible reçoit un courriel dans lequel l'émetteur prétend appartenir à l'un des groupes d'attaquants cités plus haut. Il informe son destinataire que son site Web ou son réseau informatique va être visé par la prochaine attaque DDoS du groupe, à partir d'une date qui lui est précisée.

Pour renforcer l'effet d'intimidation, l'auteur du courriel invite alors le lecteur à effectuer une recherche sur Internet pour prendre connaissance des précédentes actions du groupe et l'avertit des conséquences d'une telle attaque (indisponibilité des services, perte de profit, notoriété entâchée, référencement impacté sur les moteurs de recherche...).

La cible est ensuite incitée à payer une rançon (en bitcoins) avec la menace que la somme augmente pour chaque jour de retard du paiement : une adresse Bitcoin lui est ainsi communiquée avec les explications pour effectuer le paiement.

La rançon demandée s'élève généralement à quelques bitcoins, sachant qu'un bitcoin vaut environ 400 euros actuellement. Exemple d'un courriel observé :

```
Objet : DDoS Attack Imminent - Important information

PLEASE FORWARD THIS EMAIL TO SOMEONE IN YOUR COMPANY WHO IS ALLOWED TO MAKE
IMPORTANT DECISIONS!

We are the Lizard Squad and we have chosen your website/network as target for
our next DDoS attack.

Please perform a google search for "Lizard Squad DDoS" to have a look at some
```

```
of our previous "work".  All of your servers will be subject to a DDoS attack
starting at Tuesday the 3rd of May.

What does this mean?

This means that your website and other connected services will be unavailable
for everyone, during the downtime you will not be able to generate any sales.
Please also note that this will severely damage your reputation amongst your
users / customers as well as strongly hurt your google rankings (worst case =
your website will get de-indexed).

How do I stop this?

We are willing to refrain from attacking your servers for a small fee. The
current fee is 5 Bitcoins (BTC). The fee will increase by 5 Bitcoins for each
day that has passed without payment.

Please send the bitcoin to the following Bitcoin address: [ADRESSE BITCOIN]

Once you have paid we will automatically get informed that it was your payment.
Please note that you have to make payment before Tuesday the 3rd of May or the
attack WILL start!

How do I get Bitcoins?

You can easily buy bitcoins via several websites or even offline from a
Bitcoin-ATM. We suggest you to start with localbitcoins.com or do a google
search.

What if I don't pay?

If you decide not to pay, we will start the attack at the indicated date and
uphold it until you do, there's no counter measure to this, you will only end
up wasting more money trying to find a solution. We will completely destroy
your reputation amongst google and your customers and make sure your website
will remain offline until you pay.

This is not a hoax, do not reply to this email, don't try to reason or
negotiate, we will not read any replies. Once you have paid we won't start the
attack and you will never hear from us again!

Please note that Bitcoin is anonymous and no one will find out that you have
complied.
```

A noter toutefois que ce courriel n'est qu'un exemple et, bien que représentatif d'un certain nombre de menaces d'extorsion récentes, il ne l'est pas forcément pour l'ensemble des menaces rencontrées. En particulier, certains signalements très récents (datant de mai 2016) rapportés au CERT-FR font en effet état d'une attaque DDoS "de démonstration" au moment de la réception du courriel, afin de renforcer la pression exercée sur la victime.

Une menace qui ne serait pas suivie des faits

Ce phénomène, également détecté par d'autres organismes, a notamment fait l'objet d'un rapport publié par CloudFlare le 25 avril 2016 (cf. Documentation). D'après celui-ci, ces menaces s'apparentent à une escroquerie dans la mesure où aucune de celles observées n'a été mise à exécution et donc suivie d'action en cas de non-paiement.

De plus, les attaquants n'auraient pas la possibilité de distinguer les victimes ayant versé la rançon de celles ayant ignoré l'extorsion. Les raisons sont que le Bitcoin assure l'anonymat des transactions et qu'une même adresse Bitcoin est souvent réutilisée dans plusieurs courriels destinés à des cibles différentes. D'ailleurs, CloudFlare signale également que certaines victimes ont reçu, à plusieurs reprises et à intervalle de temps proche, un courriel de

menace présentant une demande de rançon du même montant, confirmant ainsi l'incapacité des escrocs à identifier les payeurs.

Cette pratique aurait toutefois permis aux escrocs d'amasser plusieurs centaines de milliers de dollars auprès des victimes du chantage. Bien que cette campagne d'extorsion ne soit semble-t-il pas suivie des faits, il faut cependant souligner que d'autres menaces peuvent quant à elles être accompagnées d'attaques.

Recommandations du CERT-FR

De manière générale, le CERT-FR recommande de ne pas céder au chantage et donc de ne pas verser la rançon exigée, quelle que soit la méthode d'extorsion utilisée par l'attaquant (DDoS, rançongiciel...). Plus spécifiquement, en ce qui concerne les menaces d'attaques DDoS, les raisons sont les suivantes :

- rien ne garantit que le versement de la rançon permette effectivement d'éviter ou de stopper une attaque ;
- rien ne prouve que les escrocs ont effectivement les capacités à mettre leur menace à exécution, d'autant plus si aucune attaque n'a été menée au moment de la demande de rançon ;
- cela encourage le développement de ce type d'escroquerie, en particulier envers les victimes qui ont accepté de payer par le passé et qui accepteront potentiellement encore si une nouvelle menace se présente ;
- cela contribue à financer les groupes à l'origine de l'escroquerie et ainsi à renforcer leurs infrastructures pour exécuter des attaques de plus grande ampleur par la suite.

De même, le CERT-FR déconseille de répondre aux courriels de menace et aux éventuelles relances qui suivraient. En effet, cela confirmerait la validité de l'adresse de messagerie ciblée et pourrait inciter les auteurs à renforcer la pression exercée sur leur victime.

La cible d'une telle menace pourra en revanche se préparer à l'éventualité d'une attaque imminente en mettant en oeuvre les mesures adéquates pour se protéger. Un guide disponible sur le site Internet de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) rappelle les mesures à prendre pour se protéger et réagir face à une attaque DDoS (cf. Documentation).

Documentation

- Rapport de CloudFlare "Empty DDoS Threats: Meet the Armada Collective" : https://blog.cloudflare.com/empty-ddos-threats-meet-the-armada-collective/
- Guide "Comprendre et anticiper les attaques DDoS" par l'ANSSI : http://www.ssi.gouv.fr/uploads/2015/03/NP_Guide_DDoS.pdf

2 - Teslacrypt

Les auteurs du rançongiciel TeslaCrypt ont rendu publique la clé privée qui permet de déchiffrer les fichiers de leurs victimes.

Cryptographie asymétrique

Les rançongiciels se servent souvent de la cryptographie asymétrique pour chiffrer les fichiers d'un ordinateur. Ce système cryptographique utilise deux clés différentes : une de ces clés sert à chiffrer, la clé dite `publique`, tandis que l'autre est utilisée pour déchiffrer, la clé dénommée `privée`. Ce couple de clés est généré sur un serveur contrôlé par les auteurs du rançongiciel. Ils y confinent la clé privée, seul secret capable de déchiffrer les données qui ont été chiffrées avec la clé publique. En revanche, la clé publique est embarquée dans chacun des exécutables responsables de l'infection. Elle est utilisée dans le processus de chiffrement des fichiers de la victime. S'il n'y a pas de faille dans le protocole cryptographique mis en place pour chiffrer avec la clé publique, le seul moyen de déchiffrer les données de la victime est de connaître la clé privée en possession des auteurs du code malveillant.

Le secret de TeslaCrypt révélé

Le CERT-FR a pu vérifier que la clé privée dévoilée est bien associée à la clé publique utilisée dans certaines versions du code malveillant TeslaCrypt. Elle permet donc de recouvrer les données originales pour tous les incidents qui concernent ces versions. Il existe actuellement des outils gratuits qui procèdent au déchiffrement de tous les fichiers d'un poste compromis par TeslaCrypt, pour peu que la version soit concordante avec le secret dévoilé.

Prévention contre les rançongiciels

Les rançongiciels sont de plus en plus nombreux et la divulgation de clé privée est un phénomène exceptionnel. La meilleure solution pour se protéger est de respecter les recommandations contre les rançongiciels, que vous pouvez retrouver sur notre précédent bulletin d'actualité (1)

Documentation

- (1) Rançongiciels : état des lieux
  http://cert.ssi.gouv.fr/site/CERTFR-2016-ACT-016/index.html

3 - Rappel des avis émis

Dans la période du 23 au 29 mai 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-179 : Vulnérabilité dans VMware vCenter Server
- CERTFR-2016-AVI-180 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2016-AVI-181 : Multiples vulnérabilités dans phpMyAdmin
- CERTFR-2016-AVI-182 : Multiples vulnérabilités dans Juniper Junos Space

Gestion détaillée du document

30 mai 2016 version initiale.