WANNACRY, MAIS OÙ SONT DONC PARTIS LES BITCOINS ?

Table des matières

I. Genèse de l'histoire

WannaCry c'est quoi ?

Pour rappel, WannaCry est un logiciel malveillant qui exploite une faille dans le protocole SMBv1 pour s'installer, ensuite il recherche les hôtes proches. S'il en trouve, il les infecte aussi. Une fois cette première étape effectuée, il va alors chiffrer des documents bien spécifiques. Après le chiffrement de vos fichiers, il vous est demandé de vous acquitter du paiement d'une rançon d'un montant de 300$ (environ 267€) si vous payez dans les 3 jours. Passé cette échéance, le montant double pour 600$ (environ 535€).

Bitcoin ?

Cette rançon est exigée en Bitcoin, une monnaie numérique réputée anonyme. Un guide est disponible pour vous expliquer comment en acquérir et payer la rançon directement sur la fenêtre du logiciel malveillant. De nombreuses victimes ont payé cette rançon, mais n'ont pas reçu le précieux sésame permettant de déchiffrer leurs données.

Si vous voulez en savoir plus sur WannaCry, j'ai déjà publié un gros article dessus disponible à cette adresse :

https://swithak.github.io/

II. Les Bitcoins des victimes

A l'origine, ils étaient trois :

Comme dit ci-dessus, de nombreuses victimes ont payé la rançon et n'ont rien obtenu en échange. Les rançons étaient payées aux trois adresses Bitcoin suivantes :

Portefeuilles	Adresses Bitcoins	Solde
Portefeuille 1	115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn	14.41067602 BTC
Portefeuille 2	12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw	17.77113037 BTC
Portefeuille 3	13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94	19.74510304 BTC

Mouvements de fonds

Le matin du 03 Août 2017, les portefeuilles où reposaient les rançons payées (un peu plus de $142,000.00 USD) subissent des retraits successifs.

03H06 :

- 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
  - - 0.01227173 BTC
  - - 8.71529348 BTC

03H07 :

- 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
  - - 0.01511375 BTC
  - - 7.32042682 BTC

03H13 :

- 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
  - - 9.02796322 BTC

03H14 :

- 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
  - - 10.05800019 BTC
- 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
  - - 7.05953352 BTC

03H25 :

- 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
  - - 0.10287428 BTC
  - - 9.56285137 BTC

Les mécanismes de blanchiment d'argent sale

Les auteurs de l'attaque WannaCry ne peuvent pas retirer l'argent de ces portefeuilles virtuels directement, c'est impensable car les transactions seraient très facilement traçables. Mais comme dans la vie réelle, le blanchiment d'argent sale existe sur Internet. Prenons un court instant pour entrer dans le monde de la Finance et voir comment ça se passe de l'intérieur :

Le blanchiment d'argent existe depuis un certain temps déjà et ses techniques sont éprouvées. Par divers moyens tels que la complicité bancaire, les entreprises de transfert de fonds et bureaux de change, l'achat de biens au comptant, les transferts électroniques de fonds, les fameux mandats-poste, Casinos, etc.

Le blanchiment d'argent fonctionne en trois étapes :

a) Placement, l'argent d'origine criminelle est introduit dans le système financier ;
b) Empilement, durant laquelle on accumule de nombreuses transactions pour réduire la traçabilité des fonds ;
c) Récupération, consistant à intégrer les fonds dans des secteurs variés sous forme d'investissements.

Mais le bitcoin c'est anonyme ! je l'ai entendu de partout, alors pourquoi ils ont besoin de blanchir leur argent ?

Non, le Bitcoin n'est absolument pas anonyme, il est pseudonyme. Le Bitcoin ne garantit pas l'anonymat car tout le monde peut voir toutes les transactions.

Mais pourquoi est-ce tant utilisé alors ?

Le Bitcoin n'est pas anonyme, mais les criminels ont toujours trouvé comment rendre une technologie neutre malveillante. Et ils se sont inspirés d'une vieille technique : Le Schtroumpfage (ou smurfing)

On part d'une somme X et on va la partager en de petites sommes que l'on va transmettre à un grand nombre de personnes afin de perdre les contrôles de flux monétaires dans des milliers de petites transactions. De plus, du fait de leur petit montant, elles ne tombent pas dans les contrôles automatiques pour les transactions de montants élevés.

Appliqué aux Bitcoins, ça ressemble dans notre cas à :

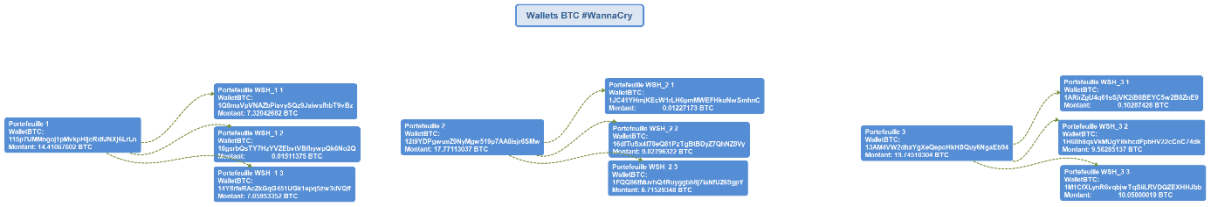

Figure 1: Portefeuilles BTC WannaCry, 20170308@8h00

Premier niveau, on voit trois portefeuilles où se trouvent les Bitcoins. Deuxième niveau, ils transfèrent l'intégralité de ces trois portefeuilles en distribuant les Bitcoins sur 9 autres portefeuilles.

Nous n'avons désormais plus 3 adresses à surveiller mais 9 :

Portefeuilles	Adresses Bitcoins	Solde
Portefeuille 1	115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn	0 BTC
Portefeuille 2	12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw	0 BTC
Portefeuille 3	13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94	0 BTC
Portefeuille WSH_1 1	1Q8maVpVNAZbPiavySQz9JaiwsfhbT9vBz	7.32042682 BTC
Portefeuille WSH_1 2	18gsrbQsTY7HzYVZEbvtVBfhywpQk6No2Q	0.01511375 BTC
Portefeuille WSH_1 3	14Y8rfeRAcZkGqG451UGk1epq5zw3dVQif	7.05953352 BTC
Portefeuille WSH_2 1	1JC41YHmjKEcW1rLH6pmMWEFHkoNwSmhnC	0.01227173 BTC
Portefeuille WSH_2 2	16dfTuSx4f78eQ81PzTgBtBDyZ7QhNZ8Vy	9.02796322 BTC
Portefeuille WSH_2 3	1FQQ86tMuvhQ4Ruyggbb8j7iaNfUZ69gpY	8.71529348 BTC
Portefeuille WSH_3 1	1ARirZgU4q61sSjVK2iB8BEYC5w2B8ZnE9	0.10287428 BTC
Portefeuille WSH_3 2	1H68h8qsVkMUgY8khcdFpbHV22cCnC74dk	9.56285137 BTC
Portefeuille WSH_3 3	1M1CfXLynR6vqbjwTqSiiLRVDQZEXHHJbb	10.05800019 BTC

Et ce n'est que pour le premier niveau, car pour la troisième étape, ils partagent encore, mais il n'y a plus de suite logique dans ces derniers. C'est là où intervient la phase d'Empilement :

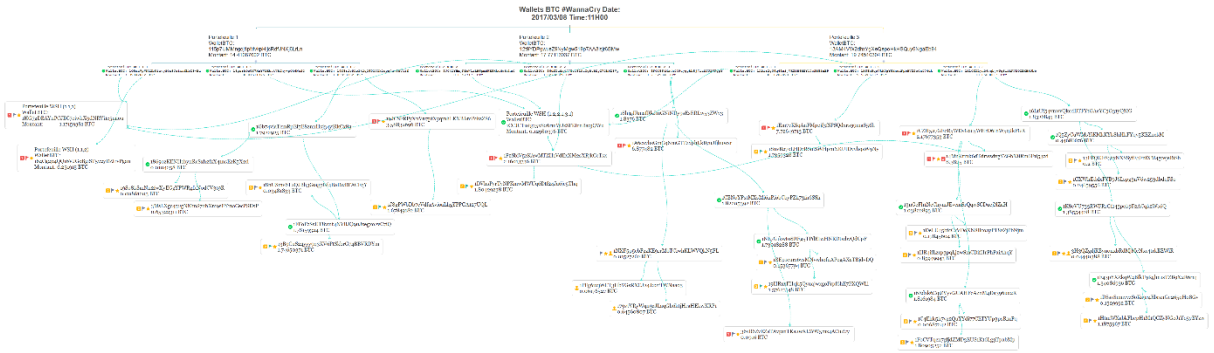

Figure 2:Portefeuilles BTC WannaCry, 20170308@13H00

Malgré le fait qu'il n'y ait pas de suite logique, j'ai tout de même remarqué des schémas intéressants :

Divisions successives

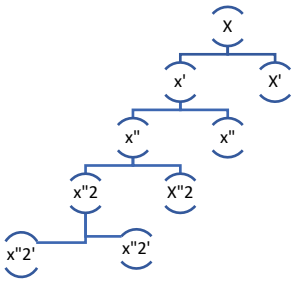

Figure 3: Partage BTC WannaCry, divisions successives

Chaque fois que le montant est divisé par 2, une grosse partie (>90%) va dans une adresse et le reste va dans une autre, l'adresse ayant les 90% passant une nouvelle fois au partage jusqu'à ce que le portefeuille d'origine soit vide. On peut résumer cela à des divisions successives.

Éclatement

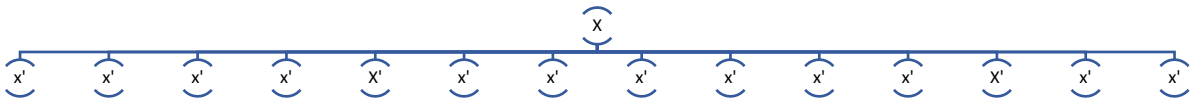

Figure 4: Partage des Bitcoins WannaCry, éclatement

J'ai observé l'éclatement d'un portefeuille en plusieurs dizaines de petites transactions. Cette méthode permet de multiplier exponentiellement le nombre d'adresses à suivre, la destination de ces nouvelles adresses était bien souvent ce que j'ai considéré comme des adresses de mixers.

Mix, mix mixers

J'ai continué de suivre les transactions jusqu'à ce que je considère les adresses Bitcoin comme étant les mixers où j'ai trouvé des milliers de transactions de très petits montants.

Jusqu'à présent, on était sur des modèles où le portefeuille était sans transactions apparentes au préalable et lorsqu'il recevait la transaction, il vidait par la suite tout le portefeuille. Ce qu'on a vu jusqu'à présent était simple à suivre. Mais là où je me suis arrêté c'est quand je suis parvenu sur des portefeuilles ayant déjà des milliers de transactions, des bitcoins sur le solde et ne sortant pas le même montant. Mes compétences s'arrêtant ici, je n'ai pas pu suivre plus en détails et j'ai donc perdu leurs traces.

Mixers	Adresses Bitcoins
Mixer 1	3MsLXgc452gNMmS7uhXm9sEYmaCecPSDsP
Mixer 2	38ZPoQUW7A6hj6ZsCGqWPk3X77qQXGspVx
Mixer 3	1BvTQTP5PJVCEz7dCU2YxgMskMxxikSruM
Mixer 4	1NXF5p5cbPgzKE9rrMbTCiwhKLWVQkN5FL
Mixer 5	36vB6ZvEZaTAvpmTKa2wXLWW5mz4ACuZ7y

Mixer 6	19HRxxFHqk5QyuajwxgoFrpf6hE7FXQWLi
Mixer 7	1BEp1eurz6vsMNvwhofuAPogAXaTBjdvDQ
Mixer 8	1DeLU45bfcCxVDoXN8BcoayPT8xZjPbNjm
Mixer 9	3NpYs1BK6GBYxFMdngJU9LnttAEXn88SwN
Mixer 10	1C4Ehk5h7vg2QuYYdi77CETYUp3psR1aPq
Mixer 11	3H3QZgdjRBynonxbRdMjMeNsx4trkBEWiR
Mixer 12	1ETAeh5y2q9Bh9s7kYDY2DDaNX89jEjW7M
Mixer 13	1KwA4fS4uVuCNjCtMivE7m5ATbv93UZg8V

Carte finale des transactions suivies

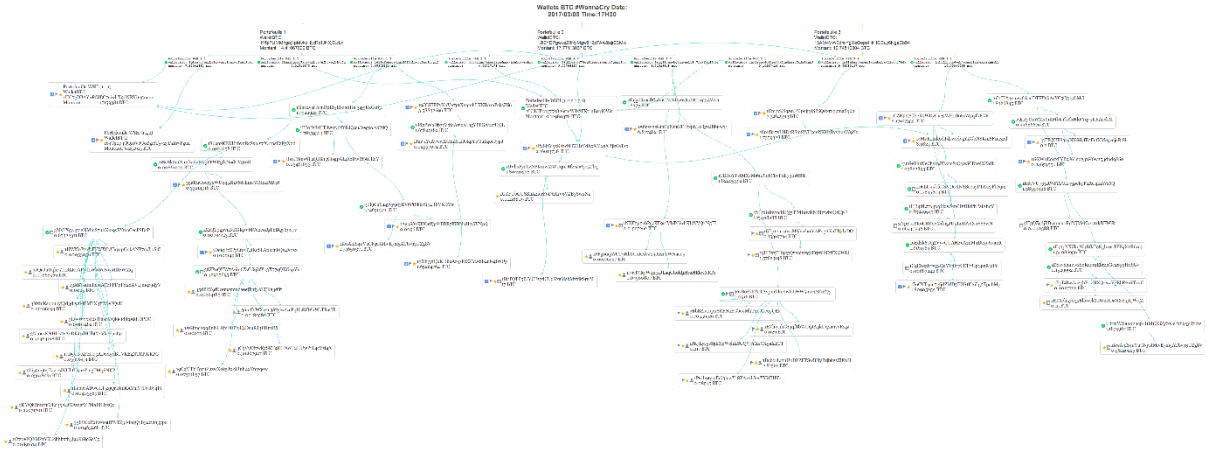

Figure 5: WannaCry Bitcoin, FINAL, 2010308@17H30

III. Commentaire

J'avais personnellement beaucoup entendu parler de Bitcoins, que c'était « anonyme » et qu'il était monnaie courante d'utiliser des mixers pour obscurcir leur destination. J'ai décidé de voir le résultat de mes propres yeux, de suivre le processus jusqu'à ce que je ne le puisse plus. Ce fût intéressant même si je pense ne pas être allé très loin dans le mécanisme de blanchiment d'argent. Selon Alberto Ornaghi, Directeur Technique de Neutrino, il semblerait que les Bitcoins ont été convertis en Monero, qui est connu pour être encore plus difficile à suivre.

Merci à @x0rz et @msuiche pour les conseils avisés !

Le mystère des Bitcoins des rançons de WannaCry reste entier, du moins pour le moment.

Swit**H**ak

IV. Webographie :

- https://fr.wikipedia.org/wiki/Blanchiment_d%27argent
- https://www.cecyf.fr/wp-content/uploads/2016/08/2017-OK-Bortzmeyer-blockchain.pdf
- https://twitter.com/SwitHak/status/892997075113267200
- https://www.cyberscoop.com/wannacry-monero-bitcoin/

A propos de l'auteur

Professionnel de la sécurité informatique, passionné par tout ce qui touche directement et indirectement à ce domaine : Législations (nationales et internationales), logiciels malveillants, actualités, vie privée, géopolitique, etc.

@SwitHak

Carte finale des transactions