Spying Challenge 2018

Write-Up

www.spyingchallenge.com

I. Introduction

Conformément à l'ordre de mission N° 502-NXH-857, la centrale de l'organisation « Société d'Investigations Spécialisées » a recruté 33 équipes composées d'agents d'élite chargés de mener l'enquête sur une levée de fond en cryptomonnaies s'avérant suspecte.

En effet, certains investisseurs ayant participé à cette levée de fond émettent des doutes quant à la légitimité des objectifs de SupremIoT et demandent à obtenir le maximum d'informations sur cette entreprise et ses employés.

Votre centrale vous met donc à disposition une partie des archives concernant cette affaire (le reste étant toujours classé) . Vous trouverez néanmoins d'excellents rapports émanant des autres équipes qui précisent certains points.

Bien évidemment, ce dossier classifié TRÈS CONFIDENTIEL est tamponné - double tamponné et tente de respecter les termes techniques du vocabulaire souverain.

Pour plus de réalisme et pour respecter la confidentialité de chacun durant les phases de filature, le staff s'est abstenu de prendre des photos et s'est permis d'en récupérer quelques-unes dans les rapports des équipes afin d'illustrer au mieux les épreuves.

II. L'entreprise

1. La présence de SupremIoT sur la Toile d'Araignée Mondiale

SupremIoT paraît être une organisation présente sur plusieurs fronts. En effet, à l'aide de l'outil checkusernames.com ainsi que de moteurs de recherche, bien que quelques faux positifs sortent, il apparaît que l'organisation se trouve sur les réseaux Facebook, Twitter, Linkedin, Vimeo, Github ainsi que Telegram.

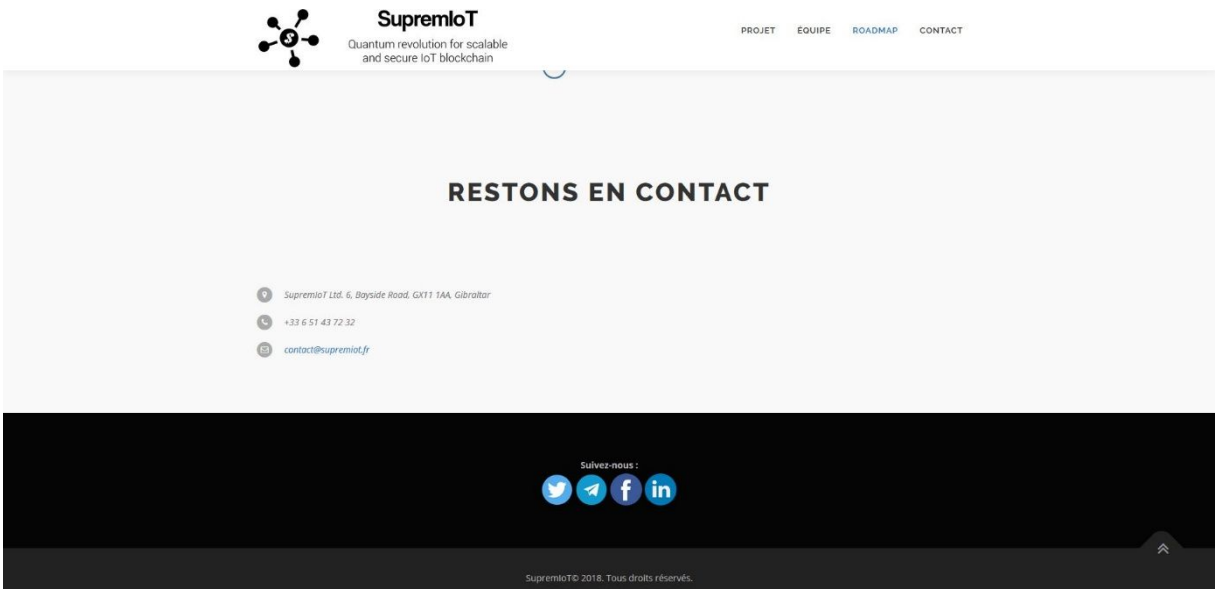
A. Le site Internet

L'organisation possède un site Internet (www.supremiot.fr) de haute qualité graphique, mais celui-ci paraît bien récent.

Il est en effet à remarquer que l'organisation a déposé le nom de domaine le 30/01/2018 chez l'hébergeur OVH.

En parcourant ledit site, nos agents repèrent directement un organigramme permettant de mettre plusieurs noms et visages derrière l'organisation.

Le pied de page du site permet également d'obtenir l'adresse des locaux, le numéro de téléphone du standard, l'adresse courriel de contact ainsi que pléthore de réseaux sociaux tels que Telegram permettant aux collaborateurs de répondre de manière instantanée aux questionnements des investisseurs.



À l'aide d'une simple recherche, il apparaît que les locaux de SupremIoT se trouvent dans un centre d'affaires situé à Gibraltar (lieu géographique connu pour être favorable à certaines organisations travaillant dans le monde de la chaîne de blocs [*blockchain*]).

Avec quelques recherches supplémentaires, il est facile de récupérer le numéro d'accueil du centre d'affaires, de les contacter, et de s'apercevoir qu'aucune entreprise du nom de SupremIoT ne siège dans ces locaux.

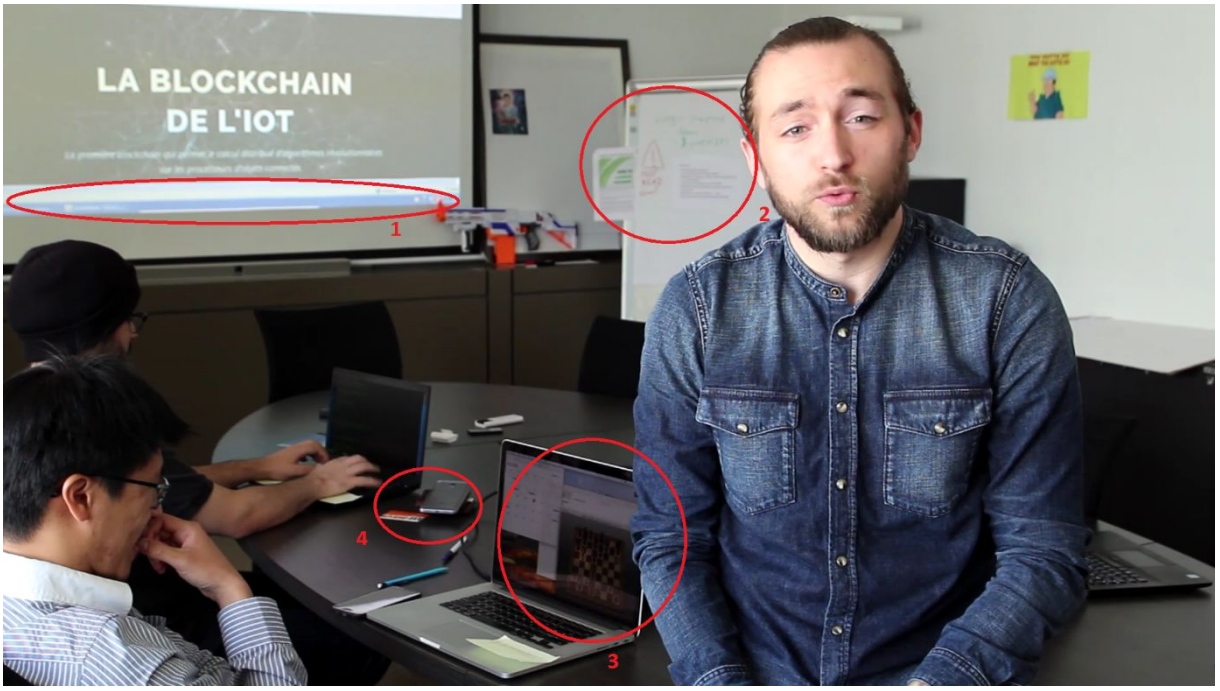
B. La vidéo de présentation

Une vidéo de présentation du projet est mise en ligne sur le site, hébergée chez Vimeo et postée le 23 mai 2018.

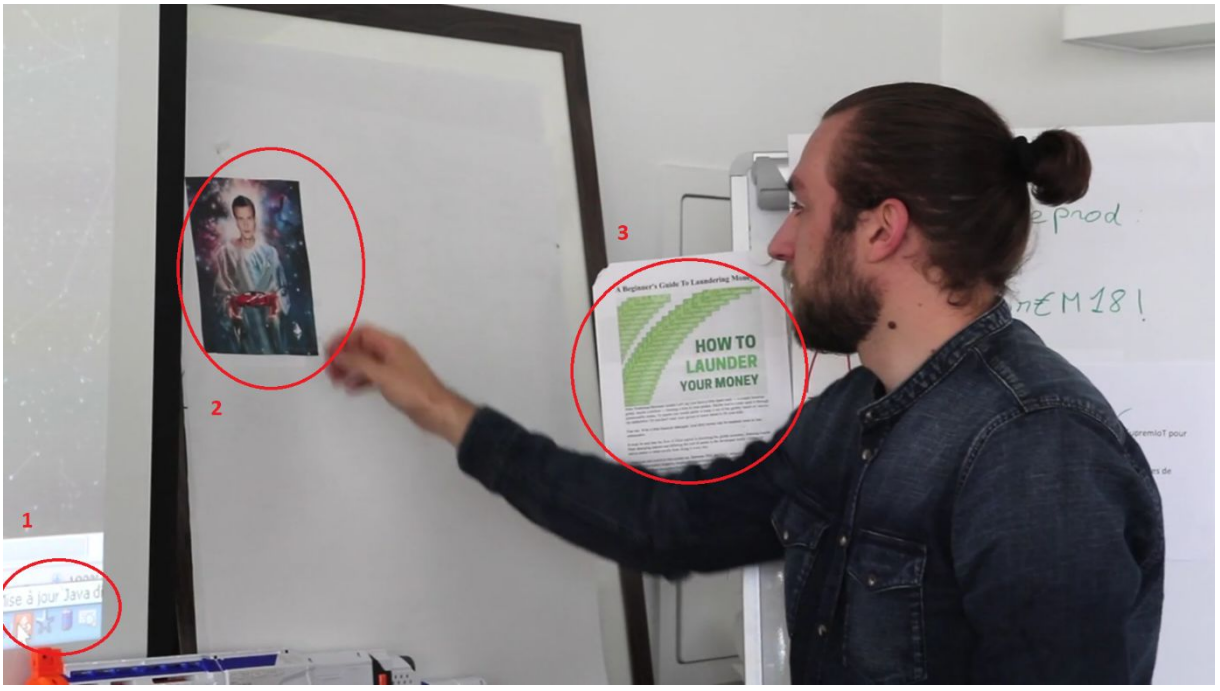
En plus de nous apprendre la date de publication, et que l'équipe derrière le projet est très familière avec le management de communautés sur les Nouvelles Technologies de l'Information et de la Communication, nous pouvons remarquer que le mot-dièse « #shitcoins » a été utilisé.

Ce terme est régulièrement utilisé dans la communauté des cryptoactifs afin de désigner un projet avec une technologie et une pérennité douteuse, mais permettant un haut taux de rentabilité en cas d'investissement. Suspect.

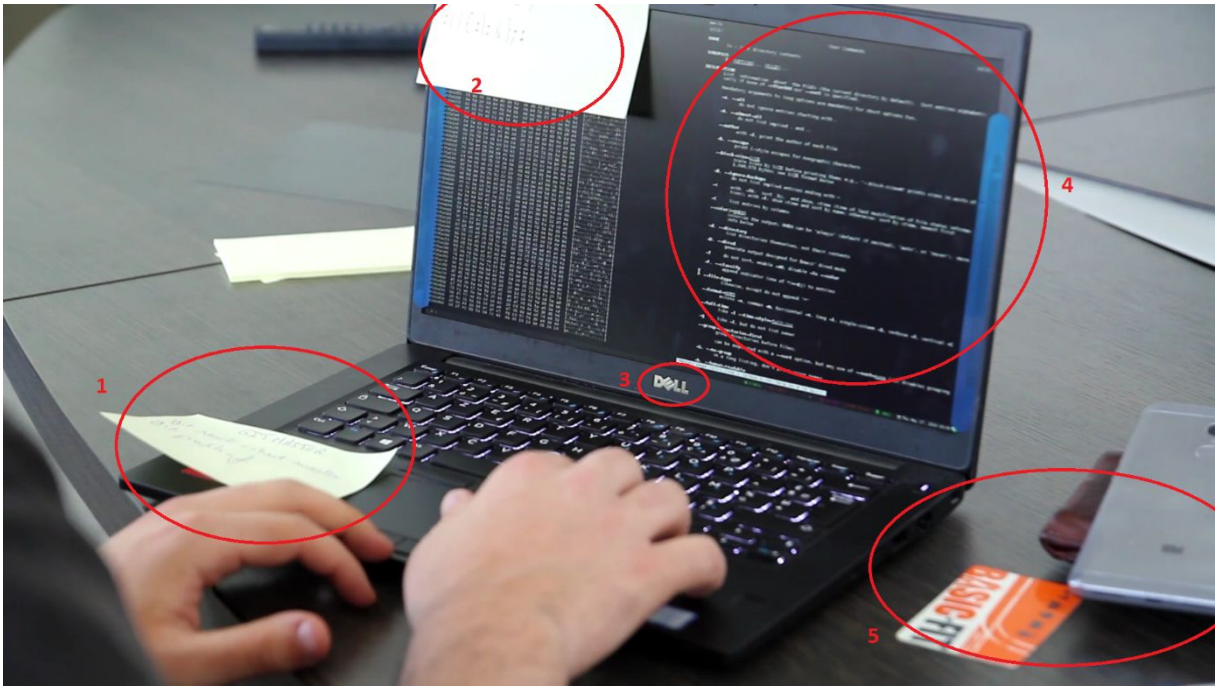
Le contenu de la vidéo, quant à lui, nous apprend énormément de choses tant sur les collaborateurs que sur l'environnement technique :



1. *L'OS du pc utilisé pour vidéoprojeter ressemble à un Windows XP*
2. *Le tableau contient moult informations*
3. *Lan semble être concentré au maximum sur son travail, mais surtout sur sa partie d'échecs et son agenda vide, sur son Macintosh…*
4. *Umberto en plein travail semble avoir laissé des informations intéressantes sur les moyens de télécommunication qu'il possède ainsi que sur ses activités sportives*

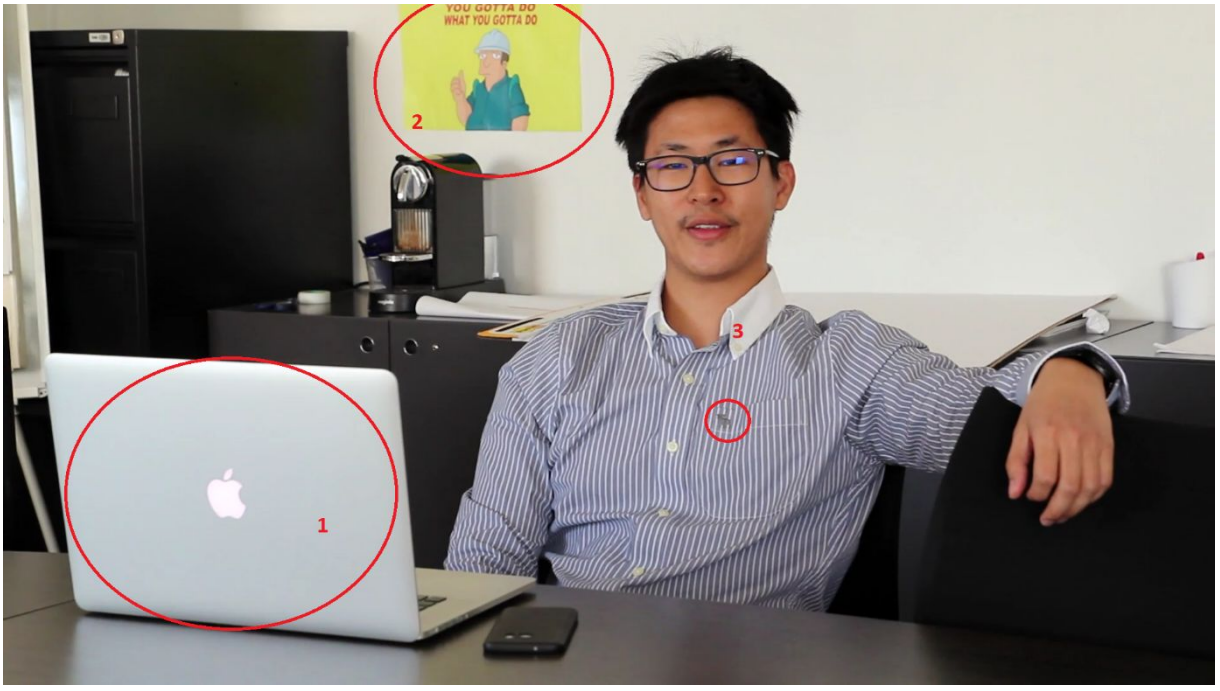


1. *Le pc de présentation semble attendre l'installation d'une mise à jour Java*
2. *Advei est en admiration devant Vitalik Buterin (Fondateur d'Ethereum), des mains duquel émane miraculeusement une Lamborghini. On peut en déduire son aspiration pour le profit*
3. *L'équipe de SupremIoT semble ne pas vouloir participer à l'effort fiscal demandé par notre bon gouvernement*

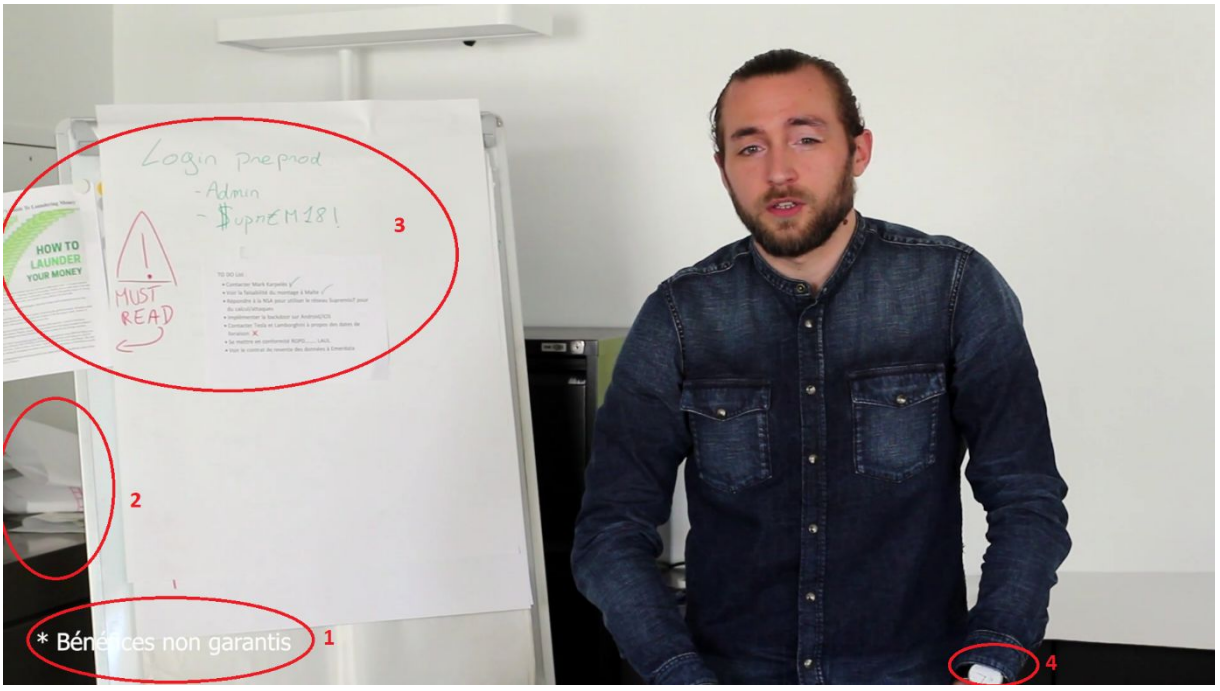


1. *Les agents possédant un écran 4K ou des yeux bioniques peuvent voir apparaître un mémo de commandes git*
2. *https://bit.ly/SSrJ6j*

3. *Umberto utilise un PC de marque Dell. Cette information peut s'avérer utile afin de mener une action de vishing*
4. *Le développeur semble utiliser la commande man ls. Qu'en déduire de ses compétences ?*
5. *La cible possède une carte d'abonnement à une salle de sport Basic Fit ainsi qu'un téléphone avec un logo ressemblant à celui de Xiaomi*



1. *IAN possède un MACINTOSH*
2. *Les locaux sont décorés avec des slogans ne faisant pas montre d'un engouement professionnel exceptionnel, provenant de la série Futurama*
3. *Ian semble aimer la sapologie*



1. *Les bénéfices non garantis peuvent éveiller l'inquiétude de certains investisseurs*
2. *Des brouillons de feuilles se trouvent dans les locaux. Certaines informations sensibles peuvent s'y trouver et être récupérées par nos agents si une action d'intrusion physique dans les locaux de la cible est envisagée*
3. *Des informations de connexion pour une plateforme de préproduction et ne liste d'actions à faire :*
    a. *« contacter Mark Karpeles » (ancien dirigeant d'une plateforme d'échanges de crypto monnaies ayant connue une disparition soudaine des actifs des clients). Cette tâche est indiquée comme réalisée, on peut imaginer que SupremIoT souhaite se volatiliser avec les finances de leurs investisseurs*
    b. *« Voir la faisabilité du montage à malte ». Cette tâche réalisée nous indique que SupremIoT cherche vraisemblablement à mettre en place une amélioration continue de ses mécanismes d'évasion fiscale*
    c. *« Répondre à la NSA pour utiliser le réseau SupremIoT pour du calcul/attaques »*
    d. *« Implémenter la backdoor sur Android/iOS »*
    e. *« Contacter Tesla et Lamborghini à propos des dates de livraison »*
    f. *« Se mettre en conformité RGPD.... LAUL »*
    g. *« Voir le contrat de revente des données à Emerdata »*
4. *Nous pouvons supposer que Advei porte une montre ressemblant à une Daniel Wellington. Peut s'avérer utile pour une attaque de phishing/vishing.*

C. Smart contract

L'agent Martin nous indique l'adresse du SmartContract (https://fr.wikipedia.org/wiki/Contrat_intelligent) utilisé pour l'ICO de SupremIoT, celui-ci gérant le token SHIOT :

https://ropsten.etherscan.io/address/0x3e33c9a96b39a1484bff0de0a9cceb4e6e8a7426

En gage de transparence, les auteurs du contrat en ont publié son code.

Les variables membres suivantes sont y sont déclarées:

```
13  contract SupremIOTToken {
14      string  public constant _name = "Suprem IOT Token";
15      string  public constant _symbol = "SHIOT";
16      uint256 public constant _totalSupply = 2000000 * 10**uint(_decimals);   // WOW, 2,000,000 tokens !
17      uint8   public constant _decimals = 18;                                 // OMFG that's 2,000,000.000000000000000000 tokens now !
18
19      address public owner;                                                   // that's us
20      address public trustedThirdParty;                                       // that's not us
21      uint    public deposited;                                               // the real money
22      mapping (address => uint) public balances;                              // the SHIOT balances
23      uint256 public availableSupply = 2000000 * 10**uint(_decimals);         // SHIOTs that still hasn't been sold
24      uint    public tokenRate = 100000;                                      // SHIOT rate
25      uint[]  public quanticBlockchainBigData;                                // the quantic blockchain big data
```

Les constantes principales du contrat sont donc:

- Nom du token (_name): Suprem IOT Token

- Symbole du token (_symbol): SHIOT

- Total de tokens distribuables (_totalSupply): 2 millions

- Nombre de décimales (_decimals): 18

Les variables suivantes sont initialisées à la création du contrat:

- Propriétaire du contrat (owner): 0xaEC197365EFAdfc671A3eca279b9cdFeb5B67DA5

- Tiers de confiance (trustedThirdParty): 0x3288d807dB0642Ac177F762fdaAD4b3dbeFdfc97

Les méthodes exposées par le contrat sont les suivantes:

function SupremIOTToken(address _trustedThirdParty) public
function name() public pure returns (string)
function symbol() public pure returns (string)
function totalSupply() public pure returns (uint256)
function decimals() public pure returns (uint8)
function deposit() public payable
function balanceOf(address tokenOwner) public view returns (uint balance)
function transfer(address _to, uint _value) public
function withdraw(uint amount) public onlyTrustedThirdParty
function entangleQuanticCloudIOTData(uint IOTData) public
function detangleQuanticCloudIOTData() public
function modifyQuanticCloudIOTData(uint index, uint IOTData) public
function killItWithFire() public onlyTrustedThirdParty

Rien d'anormal ici, pour un token suivant le standard ERC20.

Les fonctions entangleQuanticCloudIOTData, detangleQuanticCloudIOTData, modifyQuanticCloudIOTData et killItWithFire sont spécifiques à SupremIOT.

Analysons ce qu'il s'est passé à partir de la création du contrat.

Nous constatons tout d'abord que plusieurs adresses ont participé à l'ICO, chacune ayant "investi" 1 ETH:

- 0xf47184c95B9Cceae20aaE37C489C1694DBBD58C9
- 0x333C2358bDF6b7d5C9a78aB902E52353f31F9bdd
- 0x39699800d5635499f34B22c893177B1fA35D47bF
- 0x72920E21A6ba67aF6200323d05BAcC0406dD6d05
- 0xb56e6e05BfC831bB99FE66bec0A3d7008EEC984E
- 0x6d86B93E3a9dCCF90A28961dD617428509372C15
- 0xf4C857Ed0CA27e4B829CBa92a3Dd1Bb2450bbfea
- 0xd09c5CA4885203d74a81251Aa279f38D1903dF41
- 0xFE9DeaB67bAd15Dd084faA8df8ab29bc48dB68dD
- 0xd75e16A25bFeA144363C766a9CC88A710E994d43
- 0xd5c9C8c36ae9De6Da646C4587E6a861232d184b6
- 0xF50Cd7F400d3698040DC07e1CdD4a057a32386e6
- 0xdB07D516B79361AA38b8b95b09C880709C000095
- 0xf793E5C5ba8787feBcC1c5CddCCF2c0aAE786f19
- 0xfdC24fFAa8eBC4FD402C5a9d095F311E6330c01B
- 0x6Af075883cE81a10914A80b6c2DEE189E96a98a9
- 0x01Ce252c4d64bf2c2BB679115169BBF8faF58A77

Ensuite, trois transactions suspectes sont effectuées par l'adresse 0xe3291e1ed38a6c05dfb48bc974aaf0004dd67974 (dénommé dans la suite de ce write-up, Haxor), qui entraînent la disparition des Ethers possédés par le contrat.

Comment cela est-il possible ? D'après le code, seul le tiers de confiance était en mesure de procéder au retrait des Ethers.

Voyons en détail ce qu'il s'est passé lors de ces transactions.

La dernière transaction effectuée par Haxor est un appel à la fonction withdraw():

https://ropsten.etherscan.io/tx/0x1ea257bf0e45b08c8a36f3d0edf358c713082f67f83e1de11d153c5bbf4589ec

Bien que l'auteur ne soit pas le tiers de confiance, la transaction est réussie et les 17 Ethers possédés par le contrat ont été transférés à l'adresse de Haxor.

Le 'modifier' onlyTrustedParty appliqué à la fonction withdraw() dont le code ci-dessous aurait du empêcher cette transaction de fonctionner:

```
40      // Very trusted
41      modifier onlyTrustedThirdParty {
42          require(msg.sender == trustedThirdParty); // trusted third party is very trusted
43          _;
44      }
```

Nous en déduisons qu'au moment de l'appel, trustedThirdParty avait la valeur de l'adresse de Haxor sinon cette transaction aurait échoué.

Voyons en détail les deux autres transactions effectuées par Haxor afin de comprendre comment cela a pu se produire.

La première transaction (https://ropsten.etherscan.io/tx/0x8c373c0951889f370dc9560a02b6e7f5aa25d77b7af1a5f7a695b0c5a05a9813) est un simple appel à detangleQuanticCloudIOTData() qui ne dispose pas de paramètres.

A première vue, rien de prodigieux à vouloir désintriquer des particules de données de l'Internet des objets dans le cloud quantique:

```
97      // Detangle quantic cloud IOT data from quantic blockchain big-data
98      function detangleQuanticCloudIOTData() public {
99          require(quanticBlockchainBigData.length >= 0);
100         quanticBlockchainBigData.length--;
101     }
```

Le tableau quanticBlockchainBigData[] étant vide, sa taille initiale est donc naturellement 0.

Cependant, la comparaison à l'aide de l'opérateur ">=" fait que cette fonction va décrémenter la taille du tableau bien que celle-ci soit déja à 0.

La taille du tableau passe donc à 0xa0ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff

Rien de plus pour cette transaction.

La deuxième transaction (https://ropsten.etherscan.io/tx/0x5055233b7886d217ee71786d173a688362eb15af7a76e47543cefad41eed6cf9) va nous aider à comprendre plus en détail ce qu'il s'est passé.

Il s'agit d'un appel à modifyQuanticCloudIOTData(). Cette fonction permet de modifier le tableau quanticBlockchainBigData[] en plaçant le contenu de IOTData à l'index "index".

```
103     // Modify quantic blockchain big-data
104     function modifyQuanticCloudIOTData(uint index, uint IOTData) public {
105         require(index < quanticBlockchainBigData.length);
106         quanticBlockchainBigData[index] = IOTData;
107     }
```

Les paramètres suivants sont passés lors de l'appel:

- uint256 index = 0x09addddcec1d7ba6ad726df49aeea3e93fb0c1037d551236841a60c0c883f2c2

- uint256 IOTData = 0x0000000000000000000000000e3291e1ed38a6c05dfb48bc974aaf0004dd67974

Tiens donc ! Nous remarquons l'adresse de Haxor (0xe3291e1ed38a6c05dfb48bc974aaf0004dd67974) dans le paramètre IOTData.

Nous comprenons donc ici le pourquoi de l'appel précédent à detangleQuanticCloudIOTData(). Celui-ci avait pour but d'entraîner un soupassement de capacité d'entier (coucou l'ANSSI) ou "integer underflow" permettant ainsi d'accéder à un index plus grand que prévu du tableau quanticBlockchainBigData[].

L'emplacement en mémoire de quanticBlockchainBigData[0x09addddcec1d7ba6ad726df49aeea3e93fb0c1037d551236841a60c0c883f2c2] serait ainsi la variable trustedThirdParty ?

Voyons comment l'on arrive à calculer celle-ci.

Le tableau quanticBlockchainBigData est la 7ème variable déclarée et est ainsi au slot 6.

Nous en calculons l'empreinte sha3

```
>>>web3.sha3("0x0000000000000000000000000000000000000000000000000000000000000006", { encoding: 'hex' })
"0xf652222313e28459528d920b65115c16c04f3efc82aaedc97be59f3f377c0d3f"
```

La variable trustedThirdParty est la 2ème variable, donc située au slot 1.

```
>>> hex(2**256 - 0xf652222313e28459528d920b65115c16c04f3efc82aaedc97be59f3f377c0d3f + 1)
'0x9addddcec1d7ba6ad726df49aeea3e93fb0c1037d551236841a60c0c883f2c2'
```

Et voilà, nous retrouvons l'emplacement de la variable trustedThirdParty par rapport au tableau quanticBlockchainBigData.

Nous voyons par la suite qu'un autre agent (0xAd3692c2Ba9bDECfdcc663FBdb7a942427D71dBB) a interagit avec le contrat et l'a exploité avec succès afin de le "suicider" lors de la transaction suivante avec l'appel de killItWithFire():

https://ropsten.etherscan.io/tx/0x81559bc0caaf2a9a88b02fc47ebbaa4898c617a4b2a8b8ac68fe5801f9fed8e8

Les Ethers sont eux, en revanche, perdus dans la nature ;)

Cette vulnérabilité a été exposée par Doug Hoyte lors de sa soumission au concours Underhanded Solidity Coding Contest et a gagné la 4ème place avec mention honorable:

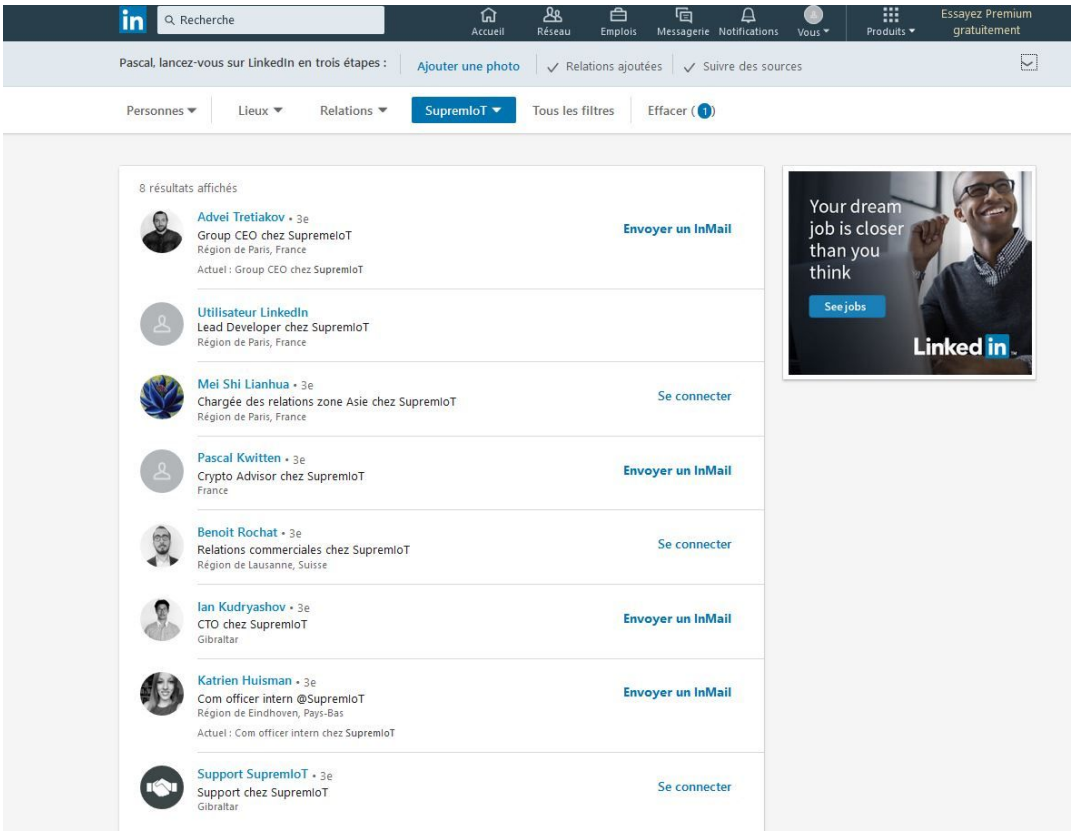
https://medium.com/@weka/announcing-the-winners-of-the-first-underhanded-solidity-coding-contest-282563a87079

Nous vous conseillons vivement de consulter l'ensemble des soumissions à ce concours, celles-ci, très intéressantes également, sont disponibles sur le dépôt suivant:

https://github.com/Arachnid/uscc/

III. Les collaborateurs

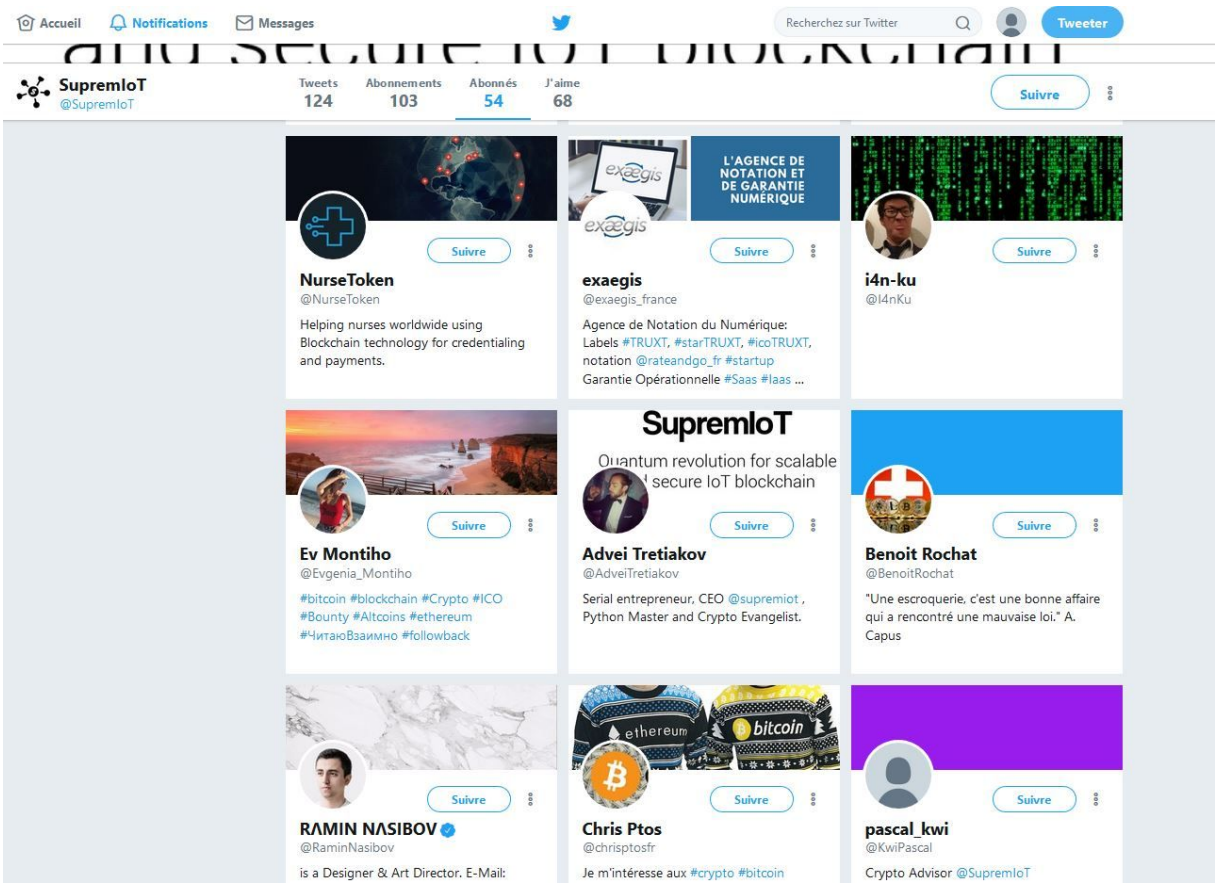
Bien que le site nous donne le nom et les fonctions de 4 collaborateurs, une recherche sur le réseau social professionnel LinkedIn nous indique d'autres collaborateurs travaillant chez SupremIoT.

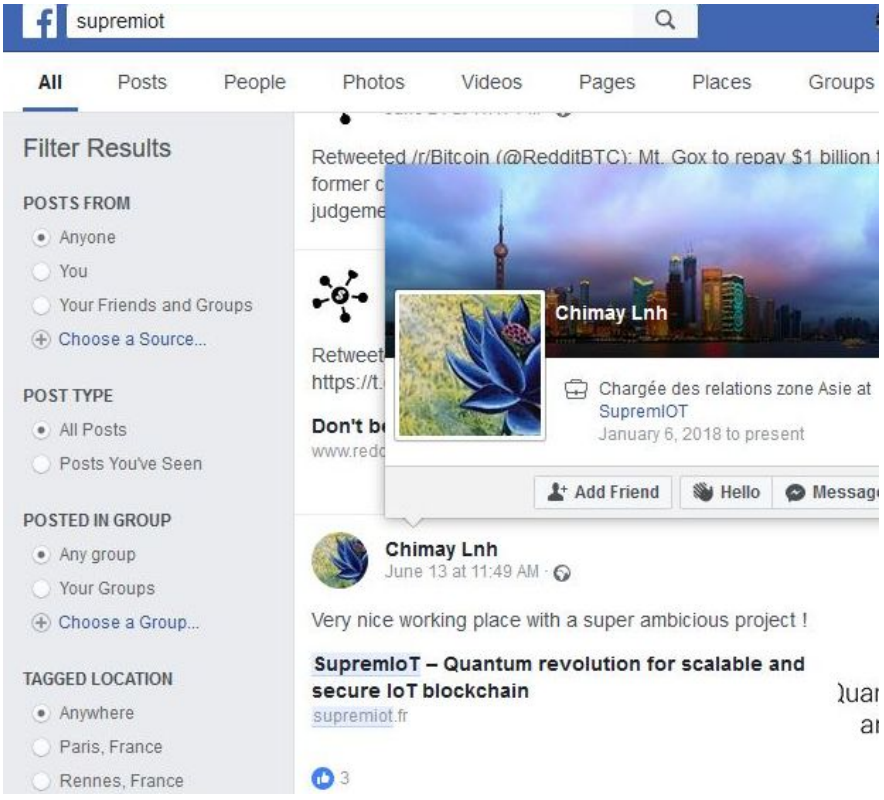


Pascal Kwitten, effectivement collaborateur de SupremIoT, ne possède normalement pas de compte LinkedIn ! La centrale a pu remarquer qu'une équipe a créé ce faux profil afin d'entourlouper certains compétiteurs.

Bien évidemment, les profils professionnels des collaborateurs sont intéressants, mais les profils personnels (Twitter, Facebook...) le sont encore plus pour apprendre à connaître nos cibles.

Il est relativement facile de trouver une liste de collaborateur en regardant, par exemple, les abonnés Twitter de SupremIoT ou en vérifiant qui a aimé les publications de la page de l'entreprise.

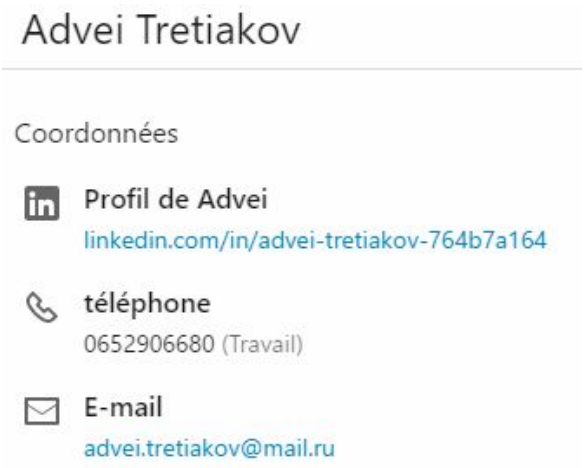

Accueil
Notifications
Messages
Recherchez sur Twitter
Tweeter
SupremIoT
@SupremIoT
Tweets 124
Abonnements 103
Abonnés 54
J'aime 68
Suivre
NurseToken
@NurseToken
Helping nurses worldwide using Blockchain technology for credentialing and payments.
exaegis
L'AGENCE DE NOTATION ET DE GARANTIE NUMÉRIQUE
@exaegis_france
Agence de Notation du Numérique: Labels #TRUXT, #starTRUXT, #icoTRUXT, notation @rateandgo_fr #startup Garantie Opérationnelle #Saas #Iaas ...
i4n-ku
@I4nKu
Ev Montiho
@Evgenia_Montiho
#bitcoin #blockchain #Crypto #ICO #Bounty #Altcoins #ethereum #ЧитаюВзаимно #followback
SupremIoT
Quantum revolution for scalable
secure IoT blockchain
Advei Tretiakov
@AdveiTretiakov
Serial entrepreneur, CEO @supremiot , Python Master and Crypto Evangelist.
Benoit Rochat
@BenoitRochat
"Une escroquerie, c'est une bonne affaire qui a rencontré une mauvaise loi." A. Capus
RAMIN NASIBOV
@RaminNasibov
is a Designer & Art Director. E-Mail:
ethereum
bitcoin
Chris Ptos
@chrisptosfr
Je m'intéresse aux #crypto #bitcoin
pascal_kwi
@KwiPascal
Crypto Advisor @SupremIoT


supremiot
All
Posts
People
Photos
Videos
Pages
Places
Groups
Filter Results
POSTS FROM
Anyone
You
Your Friends and Groups
Choose a Source...
POST TYPE
All Posts
Posts You've Seen
POSTED IN GROUP
Any group
Your Groups
Choose a Group...
TAGGED LOCATION
Anywhere
Paris, France
Rennes, France
Chimay Lnh
Chargée des relations zone Asie at SupremIOT
January 6, 2018 to present
Add Friend
Hello
Chimay Lnh
June 13 at 11:49 AM
Very nice working place with a super ambicious project !
SupremIoT – Quantum revolution for scalable and secure IoT blockchain
supremiot.fr
3

1. Advei TRETIAKOV

Le grand patron de SupremIoT paraît très peu actif sur Linkedin, où nous n'apprenons pas grand-chose de lui à part sa dernière formation au sein de l'Université Pierre et Marie Curie et le fait qu'il suit les activités de la chambre de commerce et d'industrie franco-russe.

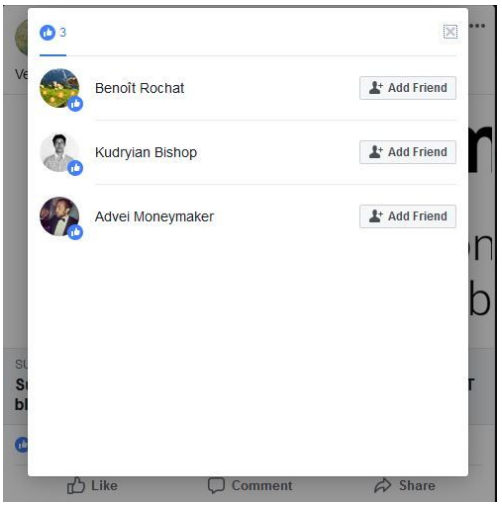
En revanche, si les agents s'étaient connectés avec cette personne, ils auraient pu récupérer son adresse mail ainsi que son numéro de téléphone.



Celui-ci se dévoile un peu plus sur Twitter en répondant à des collègues sur les petits plaisirs de la vie :

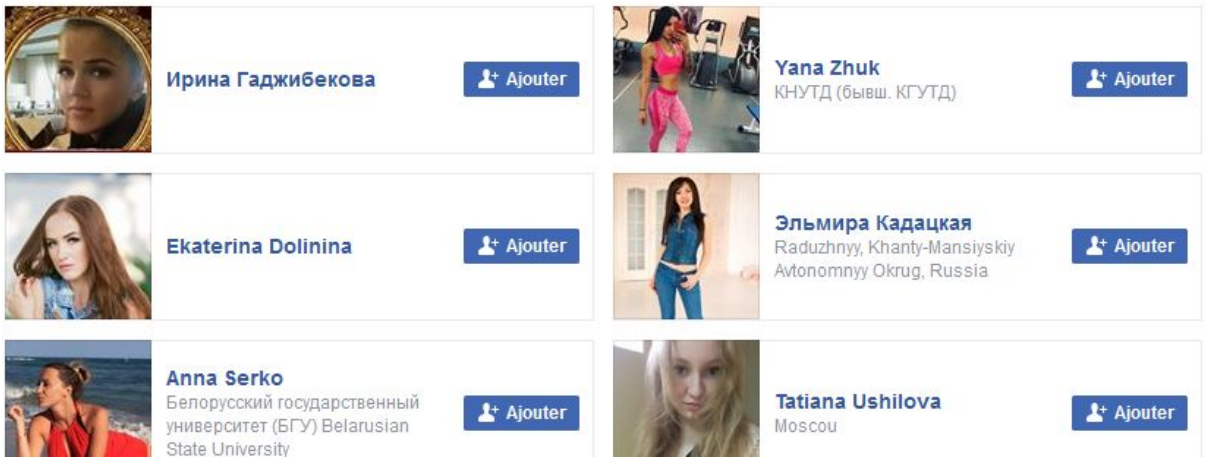
En revanche, c'est sur Facebook que le bougre se dévoile vraiment.

Bien qu'il utilise un pseudonyme, nous remarquons qu'il aime une publication concernant SupremIoT. Nous reconnaissons tout de go son visage !



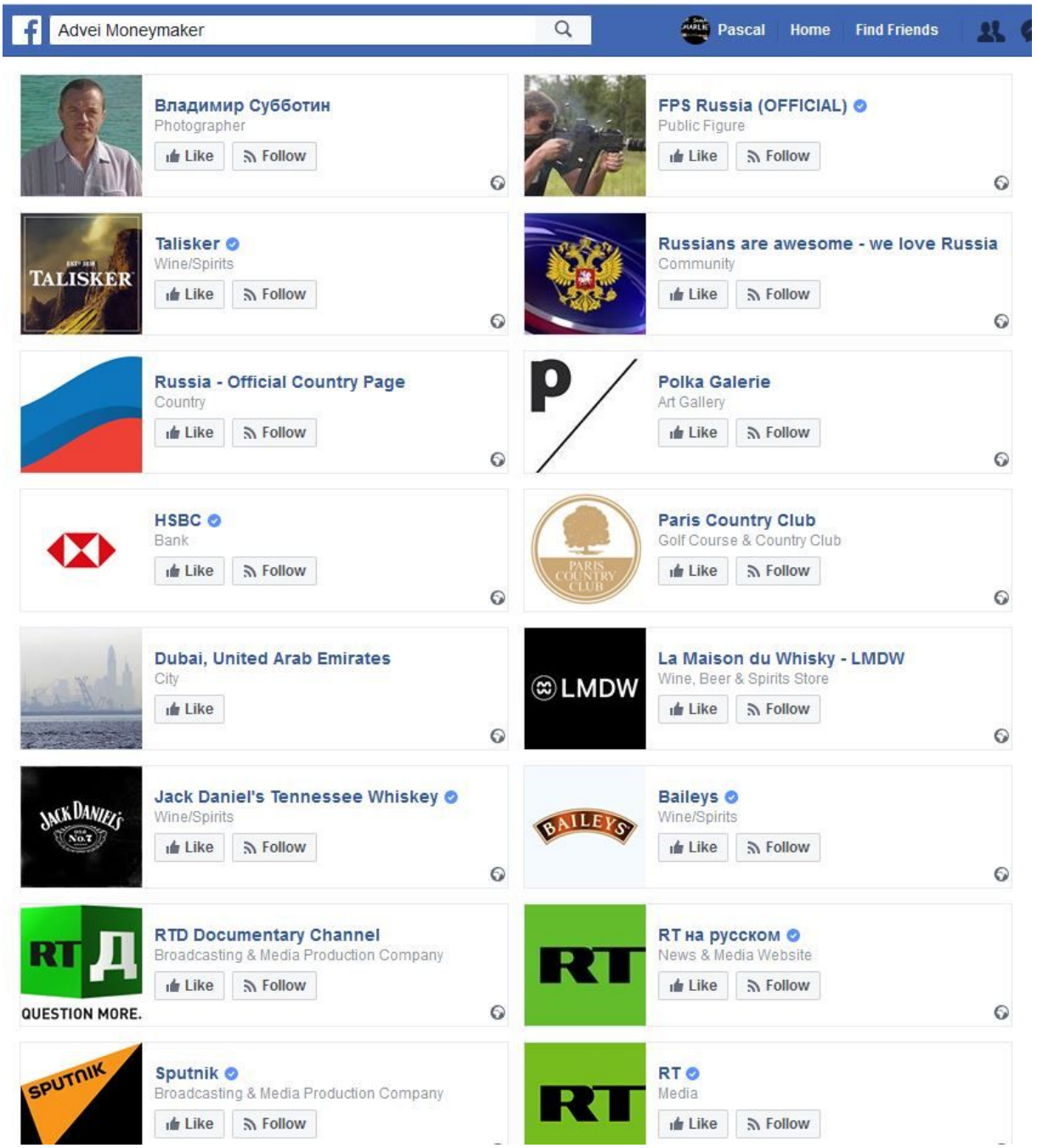
Se pensant introuvable avec son pseudonyme, le coquin se permet de chercher des femmes faciles acceptant des crypto-actifs et n'hésite pas à laisser apparent son mail professionnel.

Son goût prononcé pour les femmes est aisément décelable sur son profil, notamment par le fait qu'une grande partie de ses amis est du beau sexe, ou que les vidéos et pages qu'il aime portent à douter du sérieux de son engagement dans les liens sacrés du mariage.

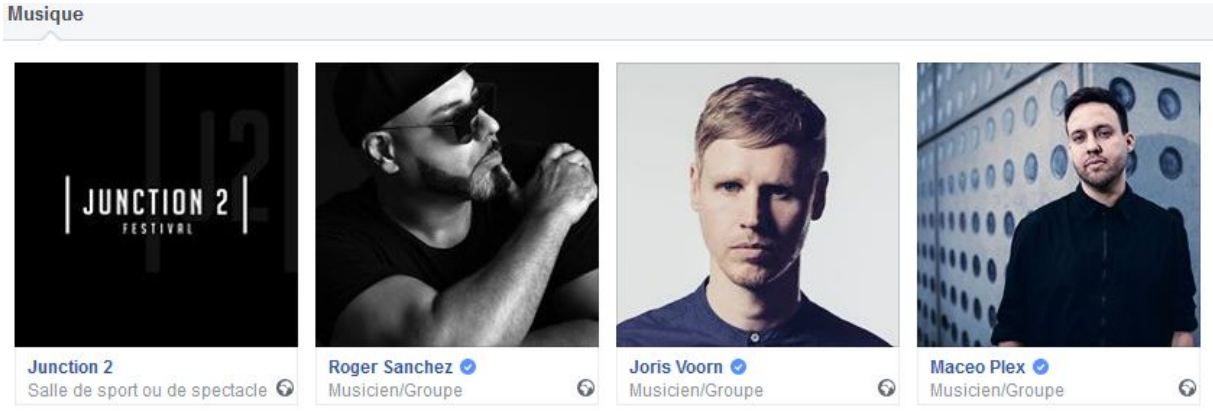


Advei reste néanmoins une personne proche de sa patrie russe et semble avoir d'importants moyens financiers.

Cet extrait des pages aimées par Advei permet de deviner sa banque ainsi que le club où il pratique certaines de ses activités sportives.



Il est également possible de l'approcher suivant ses goûts musicaux ou durant des événements auxquels il a indiqué avoir participé.



Ces informations peuvent une nouvelle fois encore utiles pour du vishing, du spear-phishing ou pour mettre en place une filature de qualité.

Enfin, la photo de couverture de ce filou au volant d'une voiture nous dévoile, à travers la vignette du contrôle technique, son goût pour les MG MGB Tourer 1,8 Cabriolet 96cv.


BQ-309-AJ
29 12/18

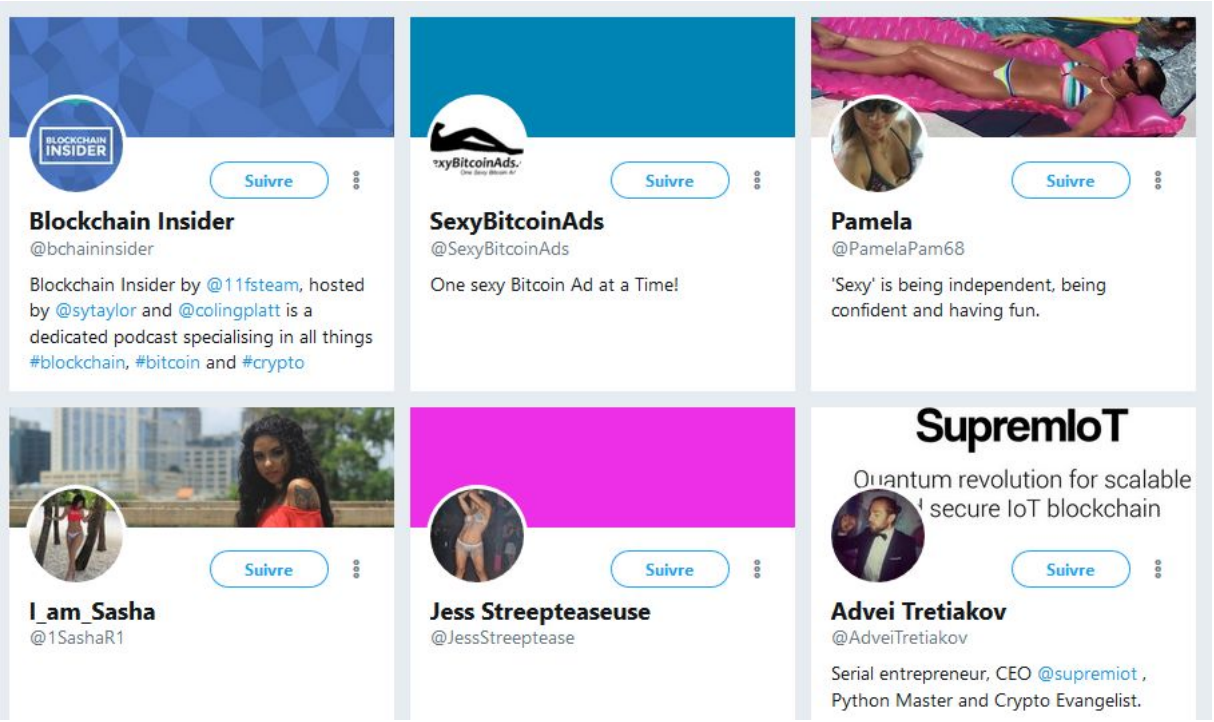
2. Ian KUDRYASHOV

Ian a l'air d'être une personne faisant attention à son image comme nous avons pu le remarquer dans la vidéo de présentation de la société. En effet, il est l'un des rares à suivre la sapologie et à porter une chemise confectionnée en véritable tissu.

Son profil LinkedIn ne nous apprend pas énormément de choses, à part son adresse mail et son expérience précédente chez IBM, en Russie.

En revanche, il est possible de trouver son compte Twitter sous pseudonyme en regardant les suiveurs du compte SupremIoT.

Voilà que nous découvrons Ian, ou plutôt « **@I4nKu** ». Son dernier tweet est bien prometteur, tout comme la typologie de profils qu'il suit.



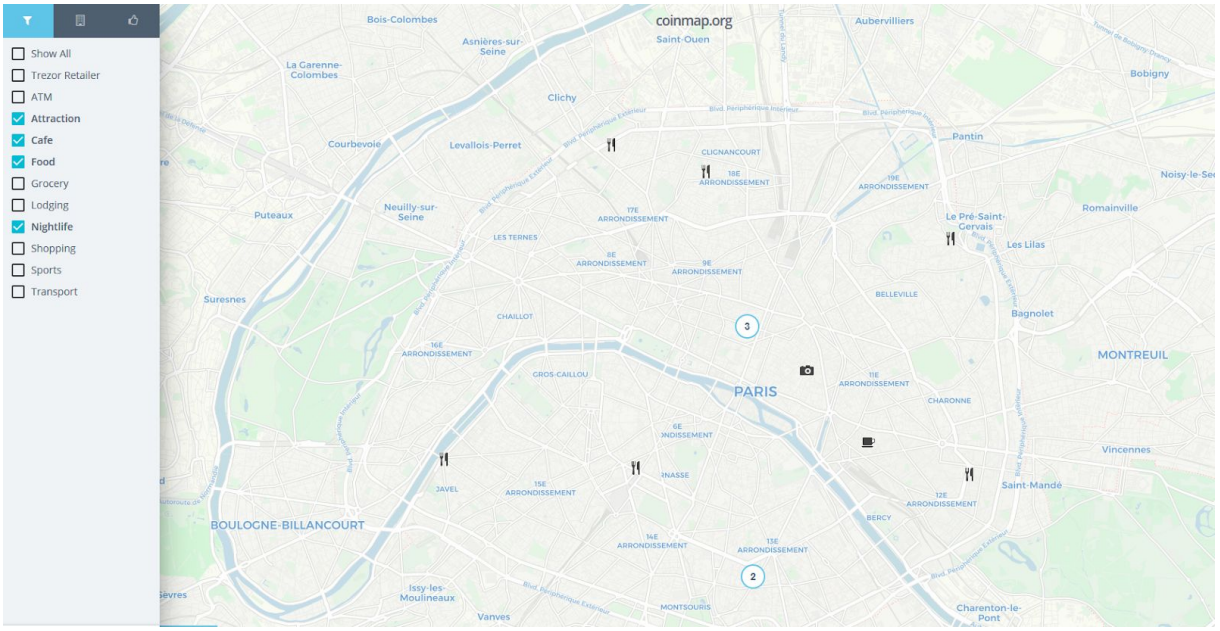
Ian a également l'habitude de partager ses aventures, ses voyages...

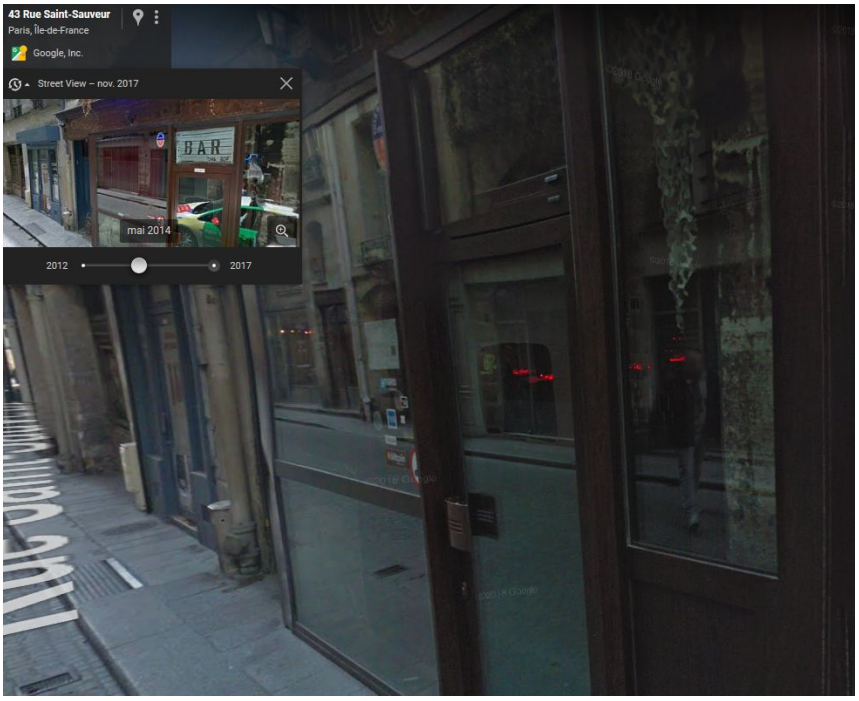
Le 17 juin, Ian visite un bar afin de dépenser ses Bitcoins.

En analysant bien la photo, nous remarquons un panneau d'interdiction de fumer écrit en français.

Nous savons également que Advei vit à Paris. Il y'a de grandes chances que ce bougre de Ian soit également installé dans cette ville.

Une recherche croisée entre Coinmap (avec les bons filtres) et Google Street View nous permet de conclure que l'individu se trouve au « Sof's Bar » à Paris.

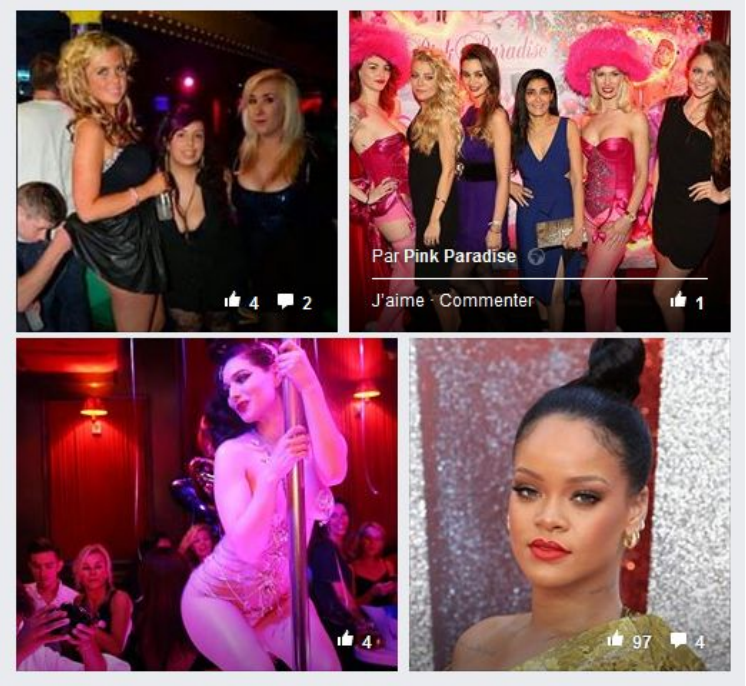




Son profil Facebook avec pseudonyme se trouve facilement en étudiant plus en détail les amis d'Advei.

À première vue, l'individu a l'air de bien gérer la confidentialité de ses publications sur Facebook.

En revanche, le résultat est tout autre avec quelques requêtes Facebook Graph Search.

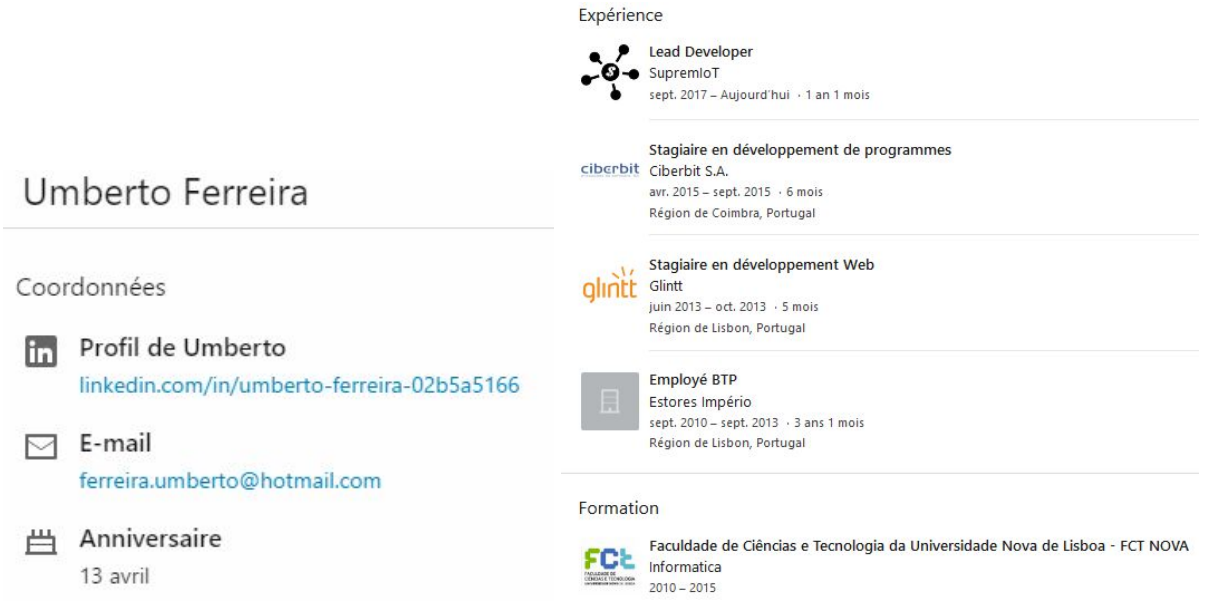


Pages et photos aimées par Ian (Ce petit fripon aime les photos d'un fameux club de strip-tease parisien).

3. Umberto FERREIRA

Umberto apparaît sur le site de l'entreprise comme étant le développeur en chef.

En parcourant son profil LinkedIn après être entrés en relation avec lui, les agents obtiennent les informations suivantes :



On remarque notamment que Umberto semble assez jeune dans le milieu de la télématique pour être développeur en chef de SupremIoT, lui qui a connu une reconversion du BTP vers l'informatique.

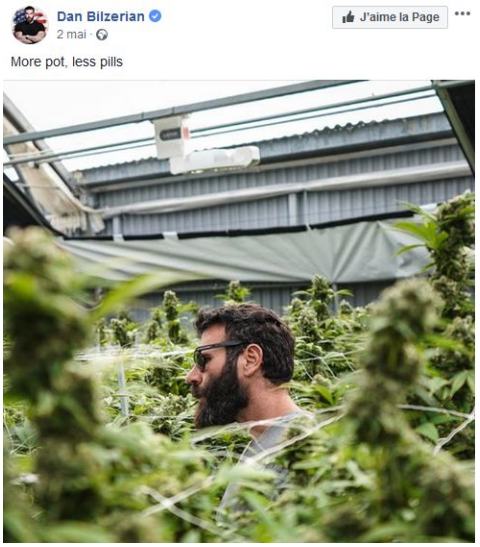
Son twitter nous indique une passion pour CR7 (Cristiano Ronaldo), ainsi que pour le monde du football en général.

Les comptes qu'il suit nous confirment des origines portugaises, une passion pour les crypto-actifs ainsi que pour les jeux vidéo.

Son profil Facebook est également saturé de photos de Cristiano Ronaldo et nous indique publiquement qu'il vit à Saint-Cloud.

Quelques requêtes nous permettent de deviner qu'Umberto est nostalgique de son pays.

Certes, monsieur Ferreira a comme passion le Portugal et le football, mais ses centres d'intérêt ne semblent pas s'arrêter ici, puisque cet étrange énergumène ne cherche même pas à dissimuler sa consommation de stupéfiants (envoi de messages publics, mention j'aime sur des photos explicites).



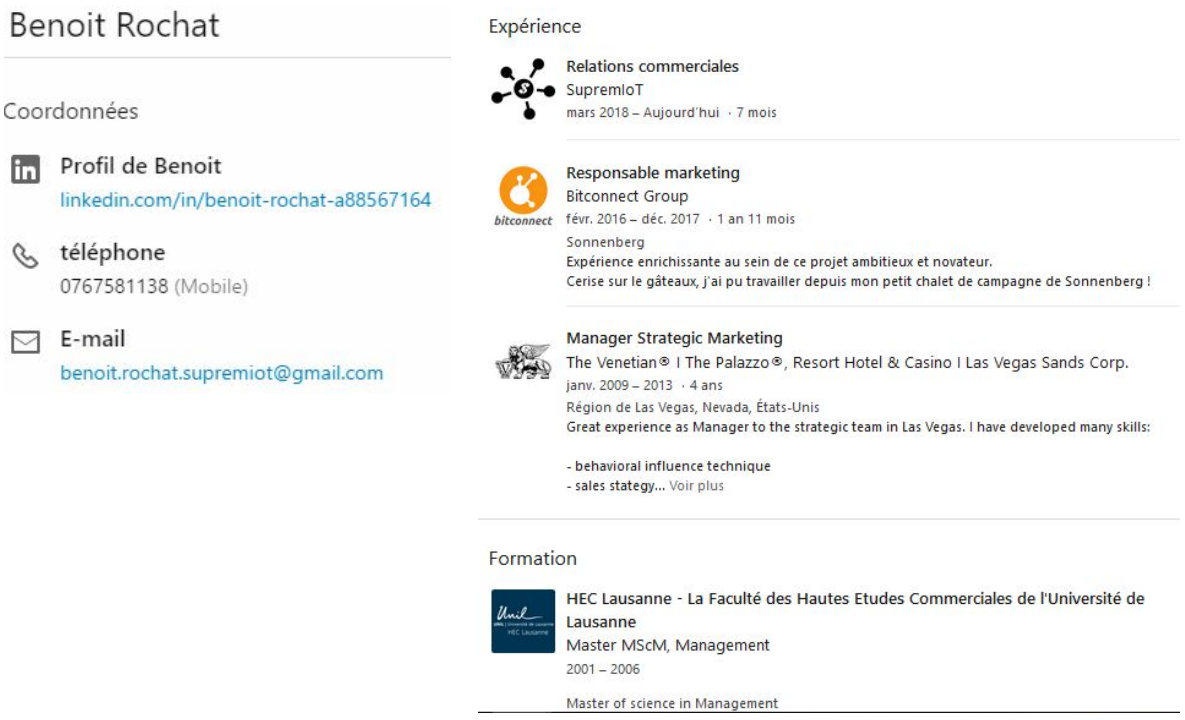
Enfin, un rapide tour sur les événements passés et futurs auxquels Umberto participe nous permet de remettre en question ses compétences en termes de rédaction de contrats intelligents.

4. Benoît ROCHAT

Si vous cherchez une définition d'entourloupeur, n'aller pas plus loin, la voici.

Benoît a tout pour plaire : une tête sympa, un cursus au sein de HEC Lausanne, un précédent poste prestigieux au sein d'un palace de Las Vegas, un cercle de relations linkedin très étoffé, ce qui fait de lui un personnage influent sur la place...

Une connexion avec son profil permettait de récupérer une profusion de moyens de le contacter.



Mais après quelques recherches plus approfondies, tout cela n'est pas très reluisant.

A l'évidence, sa fonction passée chez Bitconect, une organisation connue pour avoir été une pyramide de Ponzi, est de mauvais augure.

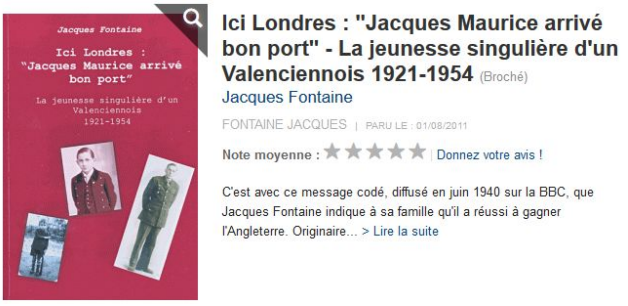
Mais autant vous dire que cela n'est rien en comparaison de son profil Twitter et de ses abonnements. Cette citation, c'est le pompon sur la Garonne !

On devine facilement que monsieur Rochat est un escroc de nationalité suisse.

Benoît, de par ses fonctions, voyage énormément, comme il l'indique dans ses tweets. Mais il semble également se moquer grandement du monde.

En effet, celui-ci indique partir de Russie pour retourner en Suisse, et n'a pas de honte à réutiliser la même photo qu'un tweet précédent, tout en laissant la géolocalisation activée, géolocalisation qui le positionne dans un bar de Saint-Pétersbourg.

On peut également supposer que notre cible helvétique soit un fanatique d'histoire, et plus particulièrement de la seconde guerre mondiale avec cette référence à Jacques Fontaine.



Bien que nous ayons déjà une abondance d'informations sur notre cible, un profil Facebook ne serait pas de trop. Une simple recherche sur Facebook permet de distinguer relativement simplement le profil de la cible, malgré les homonymes.

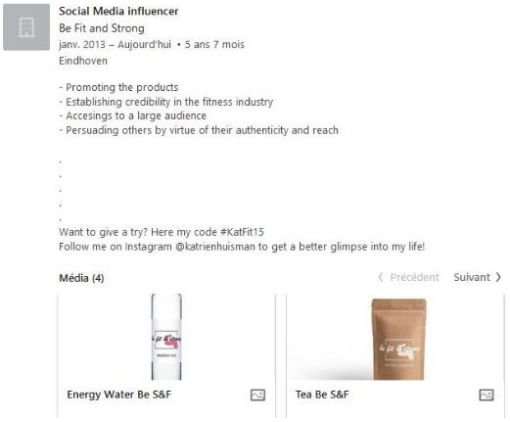
Sur Facebook, il y'a dans l'ensemble assez peu d'informations sur Benoît.

En revanche, les pages aimées permettent d'apprendre quelques renseignements utiles.

5. Katrien HUISMAN

Katrien est une personne non indiquée sur le site, mais référencée comme employé sur LinkedIn, au poste de stagiaire communication.

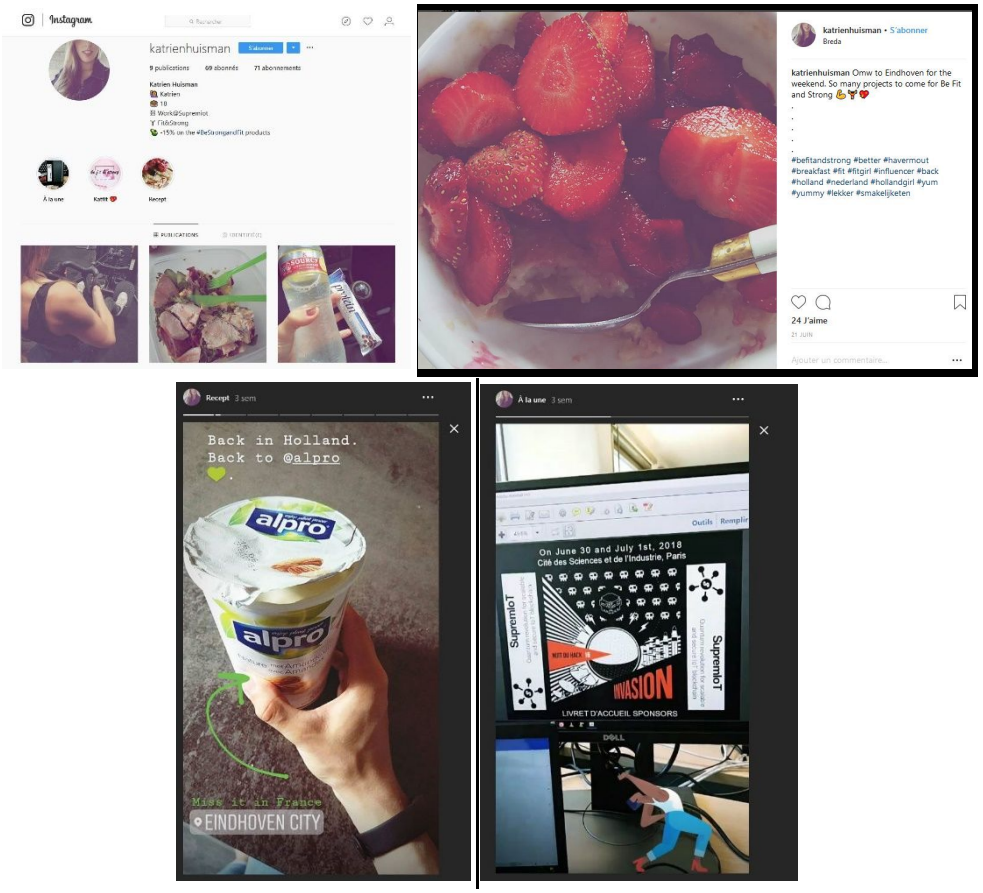
Une mise en relation via ce réseau social permet de récupérer son adresse e-mail dans les coordonnées.



En revanche, l'expérience de cette employée au sein de « Be Fit and Strong » interpelle.

En effet, notre chère amie a créé une marque avec sa réputation de « InstaGirl », influenceuse sportive...

On peut notamment voir sur Instagram les nombreuses publications la montrant en train de faire du sport, de se préparer des repas « sains », etc.



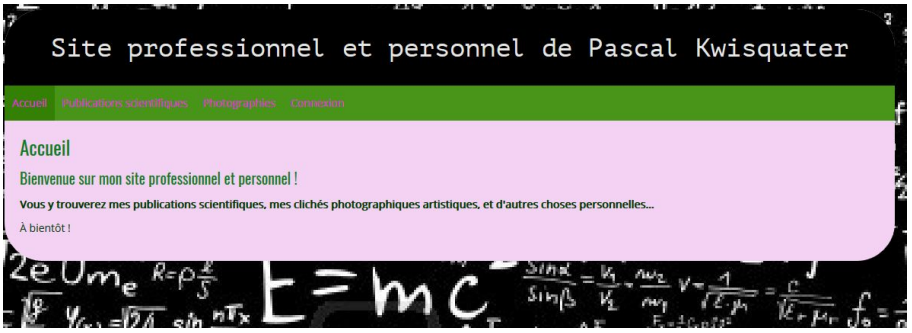
Les différentes « story » nous permet d'apprendre qu'elle travaille régulièrement en France, est sûrement originaire d'Eindhoven, fait extrêmement attention à ce qu'elle mange et possède peut-être un bracelet connecté.

Mais nous voyons également que SupremIoT est sponsor de la Nuit du Hack. On peut distinguer cela grâce à la « story » publiée où l'on distingue son écran d'ordinateur Dell, un lecteur PDF Adobe Acrobat Reader , le logiciel VLC ainsi que le logiciel de correction orthographique Antidote.

On peut supposer que Katrien est une personne narcissique, souhaitant à tout prix avoir un corps galbé et musculeux.

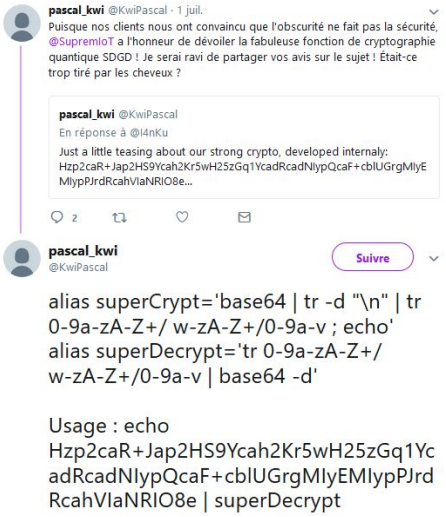
6. Pascal KWISQUATER

En regardant les comptes abonnés à SupremIoT, nous trouvons le compte d'une personne se présentant comme le consultant cryptographique de SupremIoT.



Pascal possède également un site Internet personnel lui permettant de présenter ses travaux en exploitant toutes les potentialités du HTML 5.

Ce site permet de récupérer de nombreuses informations, notamment des indices sur le message chiffré publié auparavant sur Twitter. La technique de chiffrement a notamment été publiée par la suite.



Un accès au document site/data/data.json permet de récupérer les informations ci-dessous :


```
{
  "pascalkwi": {
    "firstname": "Pascal",
    "forgot": 1530033811,
    "group": 3,
    "lastname": "Kwisquater",
    "mail": "pascal.kwikwi@hotmail.com",
    "password": "$2y$10$j9hcd2/eUDpvBRylr3kp4eihQrp52Iu7AZt4YOz6LFva.ve0xvKQa"
  }
}
```

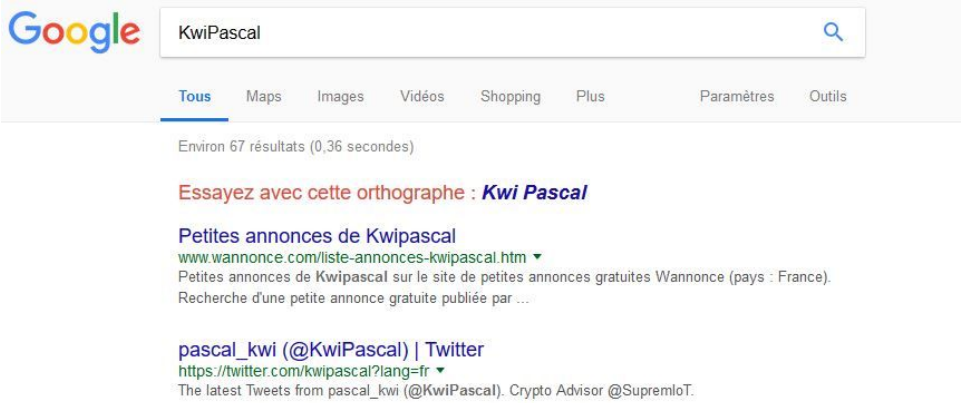

Dans le robot.txt, le « disallow » sur un dossier permet de trouver une « To-do list » où l'on apprend que ce mystérieux personnage vit chez sa mère et utilise Keepass.

On y apprend également, à force de parcourir son site, qu'il aime les smoothies à l'avocat. Information cruciale.

Une librairie photo permet de plus de s'apercevoir que Pascal est adepte du jeu du rond, utilise Tinder ainsi que What's app, mais qu'en revanche il ne maîtrise pas les métadonnées...

http://kwisquater.ovh/site/file/source/gallery/oeuvres/amoureux.jpg
Dans les métadonnées de l'image on y trouve des coordonnées GPS:
GPS Date/Time : 2018:05:10 16:21:01Z
GPS Latitude : 48 deg 50' 59.05" N
GPS Longitude : 2 deg 23' 3.68" E
GPS Position : 48 deg 50' 59.05" N, 2 deg 23' 3.68" E
Localisation : 42 Rue de Chaligny, 75012 Paris, France
Latitude : 48.849736 | **Longitude :** 2.384356

Au demeurant, une recherche plus approfondie nous dévoile un autre aspect du Tanguy Pascal.



Référence de l'annonce : A31372351

Annonce publiée par **Kwipascal** le 20 juin 2018 à 18:39.

Annonce
Informations complémentaires

Pays, Région :	**France, Île-de-France**
Code postal, Ville :	**75019, Paris**
Type d'annonce :	**Recherche**
Type d'annonceur :	**Particulier**

Salut les loulous, moi c'est KwiPascal,

Je recherche principalement un actif performant pour me faire découvrir les plaisirs d'une relation avec un homme.
Je suis de passage à Paris le 30 juin, écrivez moi directement sur pascal.kwikwi chez laposte.net.
Rencontres sérieuses uniquement.

Contacter l'annonceur

Interaction avec cette annonce

Membre hors ligne
Partager l'annonce
n.c.
Envoyer à un ami
Contacter l'annonceur par email
Format imprimable
Ajouter à vos sélections
Signaler un problème

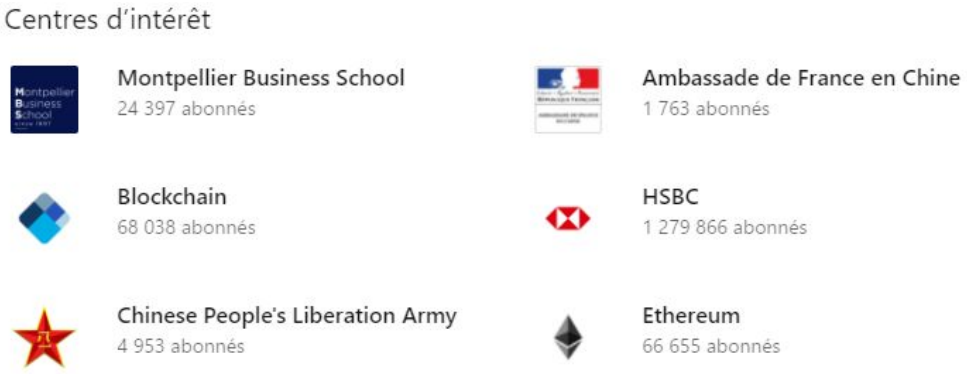
Pour ce qui est du profil LinkedIn, il s'avère que celui-ci en est un faux créé par une équipe d'agents dans le but de désinformer et déstabiliser les autres équipes, comme indiqué plus haut.
Pascal ne possédait donc pas de profil LinkedIn.

7. Mei-Shi LIANHUA

Mei Shi est identifiable facilement via LinkedIn, sur lequel on retrace facilement son parcours. Elle fait ses études dans la filière business en France, à Montpellier, et termine ses deux dernières années d'études à Shanghai. Elle restera en Chine pour travailler à l'Ambassade de France, endroit idéal pour se faire des contacts hauts placés. Elle reviendra 3 ans plus tard en France et mettra à profit ses relations chinoises pour le compte de la société SupremIoT. A priori, tout est normal...

Ses coordonnées sont accessibles sur LinkedIn, nous donnant sa date de naissance, 12 le décembre, et son adresse mail : meishi.lianhua163@gmail.com.

Ses centres d'intérêt la montre Chinoise nationaliste. Elle soutient notamment la Chinese People Liberation Army...



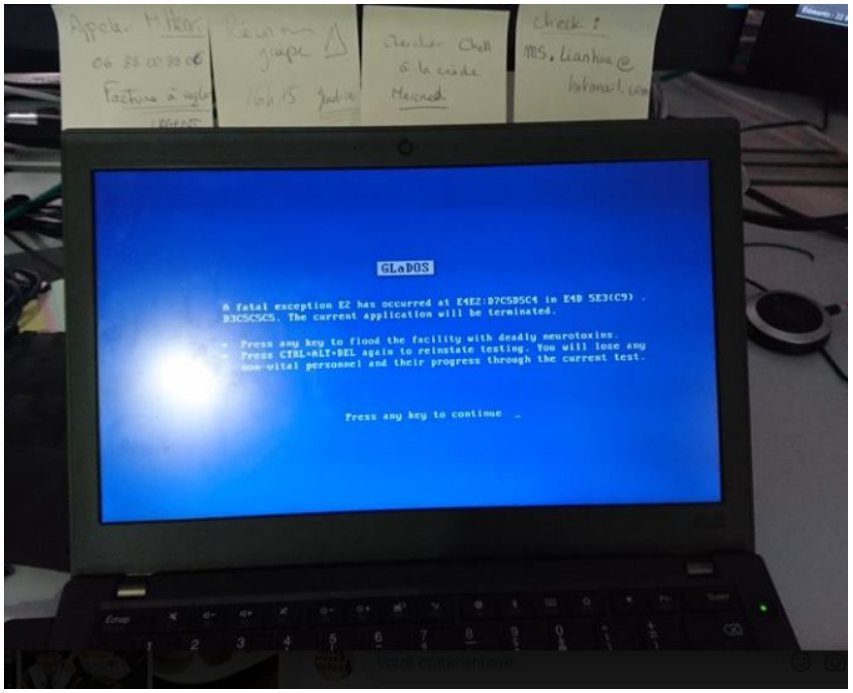
Le profil Facebook de Mei Shi est facilement identifiable malgré son faux nom (Chimay Lnh) : elle est amie avec certains membres de SupremIoT et l'avatar de son profil est l'image d'un Black Lotus, carte emblématique du jeu Magic the Gathering.

On y retrouve son parcours professionnel exposé de manière plus personnelle.

Une photo pour la vente de son Raspberry (avec un OS chinois) nous donne le lien Twitter de ce qui semble être selon toute vraisemblance son compte au vu de l'avatar.

Après une photo d'aurore boréale, on apprend qu'elle est en vacances à Shanghai pour voir sa famille, et elle se plaint du mauvais temps en postant un cliché :

Enfin, une photo de son BSOD nous donne les informations suivantes :
- Mei Shi a une petite fille, en crèche : Chell
- Une adresse mail ms.lianhua@hotmail.com
(- Et le fameux numéro de M. HENRI qui en réalité ne participait pas à la mission :D)



Nous avons maintenant accès à son Twitter. Ses abonnements ciblent particulièrement des médias chinois, des éditeurs d'antivirus connus et des agences gouvernementales. Étrange.

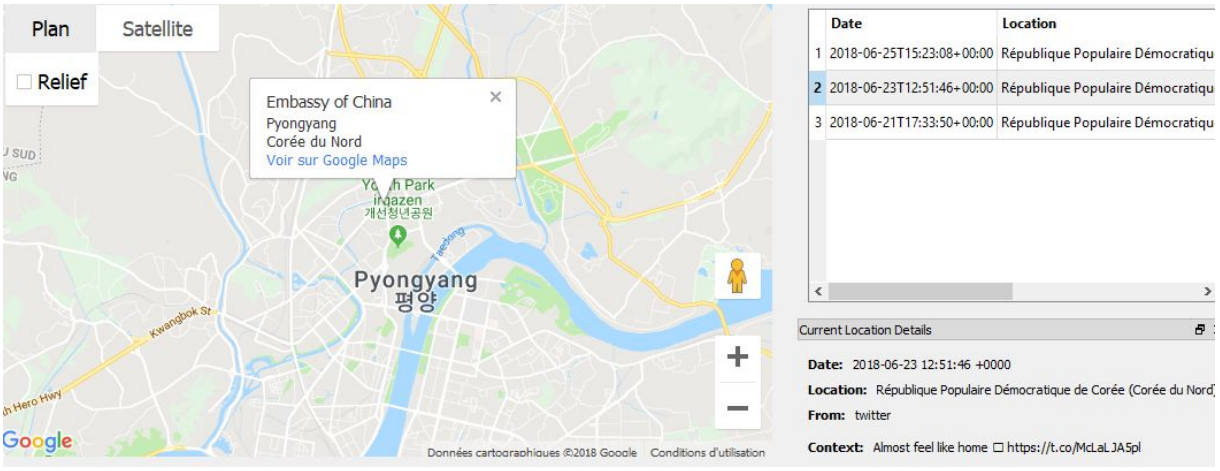
En remontant le fil, nous découvrons un « mot-dièse » revenant souvent, associé à d'obscurs messages : #61398. Cela s'apparente à des dépêches donnant des informations sur des opérations aux noms codées.

On retrouve à nouveau la photo du bâtiment postée sur Facebook concernant ses vacances à Shanghai... Mais cette fois, son commentaire « A daywork like any other... » laisse sous-entendre qu'elle est au travail ?!

Intéressons-nous à cette image. En la cherchant sur Internet, nous nous rendons compte que ce bâtiment est le QG de l'unité 61398, la cyber armée chinoise.... Ce chiffre ne vous rappelle-t-il rien ? ☺

Nous avons donc une forte suspicion que Mei Shi mène une double vie et travail en réalité pour le groupe de hacker APT1.

Par ailleurs, certains tweets semblent la localiser en Corée durant quelques jours... Ces lieux semblent correspondre à un hôtel proche d'établissements politiques stratégiques à Pyongyang... Mei Shi serait-elle en déplacement politique ?



Elle rentrera en Chine le 23 juin, où son tweet la localise à l'aéroport de Pyongyang. Elle écrira sur le mur Facebook d'Advei pour annoncer son retour en France le 26, donnant une indication sur son vol (seule une équipe d'agent pensera à trouver le numéro du vol !).

Pour récupérer cette information, il suffisait d'être ami sur Facebook avec Advei (pas si difficile de faire un profil attirant à ses yeux...) et de rechercher les vols en provenance de Shanghai et à destination de Paris.

Grâce à la photo postée sur le Facebook de Mei Shi, nous obtenons une adresse mail. À partir de cette adresse, les moteurs de recherche nous renvoient sur des liens Pastebin de leak de base de données sur lesquels elle est référencée avec un mot de passe...

Il est alors possible d'accéder à son compte Outlook... (malheureusement, malgré les consignes, l'inévitable est arrivé et certaines équipes se sont amusées à supprimer des messages : heureusement que Mei Shi veillait...). Il était également possible d'obtenir le « .pst » de la boîte mail.

On remarque alors des échanges avec plusieurs correspondants, dont un certain « U.G » qui revenait régulièrement (si vous avez lu le rapport Mandient, il devait vraisemblablement s'agir de Ugly Gorilla :p).

Ces échanges dissipent les doutes sur le fait que Mei Shi travaille pour des entités cybercriminelles, très probablement APT1. On apprend que des opérations ont eu lieu et que d'autres sont à venir. Les payloads sont très probablement échangés via un autre biais (les « packages » dont elle semble faire référence) dans certains mails. En cherchant le nom des opérations, il est facile de se rendre compte qu'il s'agit généralement d'attaques massives via malware souvent étatiques (attribution !).

C'est également au travers de son compte Outlook que l'on parvient à retrouver l'adresse mail de Ian Kudryashov, dans un mail de sa part qu'elle transmettra à ses coéquipiers d'APT1. Elle leur annonce que l'équipe de SupremIOT va bientôt sortir un algorithme révolutionnaire et qu'elle commence à gagner la confiance de son équipe.

Quelques jours avant le 30 juin, elle retransmettra un mail de Ian, lequel lui demande de prendre rendez-vous avec sa masseuse favorite, qui n'est autre qu'une membre d'APT1 infiltrée en vue de soutirer des informations durant ses moments « de détente » avec Ian.

IV. Les méthodes d'approche

Après avoir récolté toutes ces informations, il était possible d'établir pour chaque cible un profil psychologique à peu près complet, et des méthodes d'approche et/ou de récoltes d'informations personnalisées.

Nous ne détaillerons pas ici les meilleures attaques réalisées par nos agents, qui feront sûrement partie d'un DLC. Par ailleurs, les scénarios décrits ci-dessous ne sont que des suggestions ; vous pouvez bien évidemment laisser libre cours à votre imagination. Il y'a de nombreuses approches possibles !

Les attaques peuvent se réaliser par vishing, phishing, Telegram, LinkedIn,....

Il est recommandé d'utiliser des méthodes telles que MICE ou SANSOUCIS, pour une plus grande efficacité.

1. Advei

Un jour, les femmes le perdront... Mais pour l'heure, la centrale n'a pas les moyens nécessaires afin de mener une action de LOVEINT ou de piège à miel. Il est, en revanche, possible de l'aborder par son goût prononcé pour les spiritueux, la musique ou son amour de la patrie, qui sont autant de manière de récolter de l'information ou de le faire mener des actions.

2. Ian

Bien que Ian aime également les femmes, celui-ci n'est, jusqu'à preuve du contraire, pas marié. En revanche, après avoir pris connaissance des lieux de plaisir qu'il fréquente, nous pouvons très bien imaginer une approche IRL par PUR hasard en parlant de sujets pouvant l'intéresser tels que certains mangas, anime, joueurs d'échecs...

Bien évidemment une réflexion quant à une attaque informatique peut s'avérer intéressante en cas de révélations de 0-jours sur le Mac de celui-ci.

3. Umberto

Umberto n'a pas l'air très à l'aise dans le domaine du développement et des cryptomonnaies, comme nous avons pu le constater avec les mémos qu'il que l'on aperçoit dans la vidéo de présentation de l'organisation, mais également grâce à l'événement lui permettant d'apprendre à un développé un

contrat-intelligent en seulement quatre heures. Sa récente conversion du monde du BTP abonde dans le sens de cette hypothèse.

Une invitation à un événement où le Ricard et le football sont présents peut être un gage de réussite pour l'approcher. Un événement organisé autour de la communauté portugaise peut également s'avérer intéressant connaissant la nostalgie qu'il entretient pour son pays.

Enfin, usurper l'identité de la salle de sport qu'il fréquente pour lui offrir des services supplémentaires peut être un bon moyen de récolte d'informations.

4. Benoît

Arnaquer l'arnaqueur. Que lui proposer, à part lui faire miroiter un partenariat exclusif avec les plus grands de ce monde ?

Notons malgré tout que des attaques de phishing usurpant sa banque ou sa plateforme d'exchange préférée peuvent s'avérer efficaces pour un commercial, si tant est qu'il ne s'y connaisse pas trop en informatique et qu'il ait le clic facile.

Ne négligeons pas le fait que Benoît semble être un mythomane (cf. l'utilisation des 2 photos d'avions, les erreurs de géolocalisation...) et désire se mettre en avant en tweetant régulièrement sur son travail alors que ses collaborateurs ne dévoilent pas autant leurs journées de travail.

Peut-être parle-t-il facilement de choses qu'il devrait garder secrètes afin de se rendre intéressant, surtout auprès des femmes (rappelons que notre cible suit la page Facebook de Meetic Suisse.) C'est une piste à étudier plus en détail.

5. Katrien

Eh vas-y que je fais des squats, que je mange du quinoa, que je publie en permanence des stories,...

Rien à dire, Katrien passe pour être la millennial accro aux réseaux sociaux et fière de son apparence. Cela cache sans doute un manque de confiance en elle.

Une approche via le réseau social Instagram parait le plus facile, si l' on possède beaucoup de followers et que l'on est beau gosse.

En revanche, une approche via LinkedIn ne paraît pas inintéressante non plus si l'on montre de l'intérêt pour elle et sa marque. Il ne faut pas oublier également qu'elle est stagiaire au sein de SupremIoT et que son manque d'expérience peut la pousser à révéler malencontreusement des secrets de l'organisation.

6. Pascal

Pascal a tout du gentil Tanguy. Malheureusement, il a également le profil d'un opportuniste ne connaissant pas grand-chose à la cryptographie, mais étant de bonne volonté et passionné par son métier.

En revanche, étant un peu maladroite, sa publication d'annonce avec le même pseudonyme que son compte Twitter peut se retourner contre lui. En effet, nous ne savons pas si la mère de Pascal, bien que partageant son habitation, connaît les préférences sexuelles de son fils.

Si vous souhaitez opter pour une approche moins agressive, rien ne vous empêche d'envoyer une invitation exclusive et tous frais payés pour visiter une entreprise de fabrication de smoothies avocat.

7. Mei-shi

Que dire sur ce profil tant il est complexe et dangereux ?

Pour procéder à une attaque sur ce genre de personne, il est plus que recommandé d'user de tous les moyens techniques à votre disposition pour garantir votre anonymat et ne pas blesser la cible, à moins que vous souhaitiez être dans la ligne de mire de certaines agences gouvernementales aux méthodes éprouvées.

La discrétion est de mise. Pour cela, vous pouvez répondre à la proposition de vente du Raspberry Pi, parler du jeu de cartes Magic ou encore évoquer votre souhait de réaliser le même cursus que Mei-shi tout en ayant une appétence pour la Chine.

Si toutefois l'envie vous prend de jouer avec le feu, rien ne vous interdit d'essayer de procéder à une déstabilisation de la cible en évoquant sa fille ou ses activités au sein des services étatiques.

V. Filature et interactions

Comme remarqué lors de la phase d'OSINT, SupremIoT était présent au sein de la Nuit Du Hack XVI en tant que sponsor et disposait donc d'un stand.

Agents,

La suite de votre mission va consister en une phase de filature qui a déjà été évoquée dans l'ordre de mission #2. Voici des précisions :

Vous ne serez pas seuls durant votre filature : deux agences concurrentes seront sur les traces des employés de SupremIoT en même temps que vous. Vous êtes autorisé à collecter des éléments d'informations sur ces agents.

Vous avez rendez-vous à **14h30** au stand SupremIoT. Vos deux cibles sont le CEO et le responsable commercial. Ils partiront de ce point pour rejoindre leurs rendez-vous. Répartissez vos agents sur les deux cibles. Suivez-les, prenez-les en photos sans vous faire repérer. Récupérez les documents qui pourraient servir.

Vos objectifs :

Pour le CEO :
Après l'échange, vous aurez 5 minutes pour faire pression de la manière qui vous semblera la plus adaptée dans le but de récupérer tout ou partie de l'investissement de nos clients.

Pour le responsable commercial :
Un échange de document doit avoir lieu via boîte morte. Il est impératif que vous ayez connaissance du message, mais que vous n'altériez pas la livraison. Nous soupçonnons M. Rochat de détourner une partie des fonds de l'ICO. Vous aurez 5 minutes pour récupérer des aveux de sa part concernant le détournement de fonds qu'il réalise. Obtenez les indices qui le prouvent.

À noter :
Dans le cadre de la coopération internationale entre sociétés d'investigations spécialisées, merci de respecter ces délais de 5 minutes et de laisser les preuves à leur place pour permettre aux autres agences de récupérer les données. Vous n'avez pas l'autorisation d'interagir avec les cibles si elles sont déjà en contact avec une autre agence.

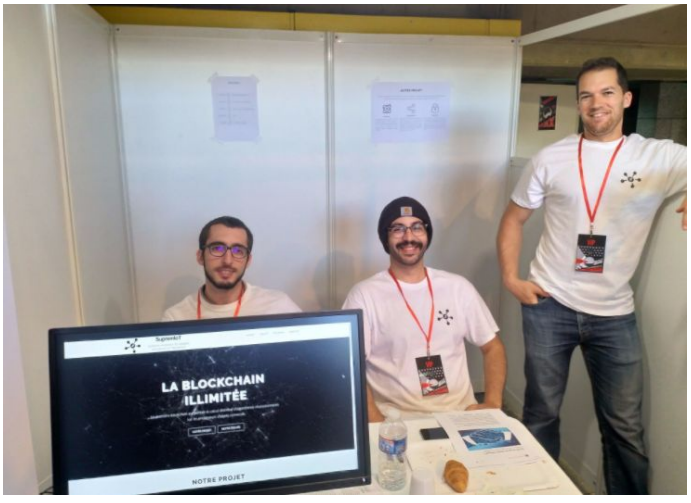
Pendant tout le temps de la filature, des membres de l'équipe SupremIoT seront présents sur le stand : n'hésitez pas à interagir avec eux.

Nous attendons votre rapport pour **17h30 CEST** dernier délais.

Bon courage,

Agent Martin
Pas de N° de mobile.
spying.challenge@gmail.com
Société d'Instigations Spécialisées

Sur ce stand se relayait l'ensemble des collaborateurs de SupremIoT.



Cette phase de repérage et de prise de contact permettait d'obtenir des informations supplémentaires sur les individus et leurs personnalités, de récupérer des documents laissés malencontreusement sans surveillance :

Partenaires principaux	CA	Dans Supremlet
Gazprom	158 000 000 000	1 000 000 €
Boris Antonov	---	600 000,00 €
Rosneft	129 000 000 000	541 854 241,00 €
Lukoil	121 400 000 000	245 000,00 €
Sberbank	58 100 000 000	120 000,00 €
Alexandre Zakhrade	---	545 451,00 €
Dan Bilzerian	---	542 546,00 €
Nabilla	---	50,00 €
John Deere	28 863 000 000	542 164,00 €
Akkuen Energies General Electric	143 260 000 000	4 521 854,00 €
Alibaba	1 433 478 561	545 454,00 €

Liste d'investisseurs

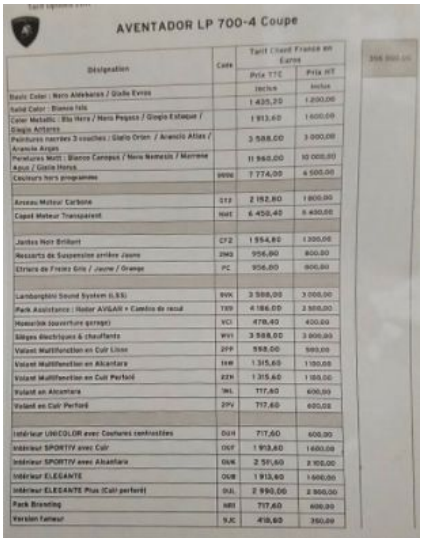
Qu'est-ce qu'un smart contract ?

par AdminDev | 14 Jun, 2018 | Guide du débutant | 0 commentaires

Les smart contracts (ou contrats intelligents) sont également appelés contrats auto-exécutoires, contrats digitaux ou encore contrats Blockchain.
Comprendre le fonctionnement des smart contracts est essentiel pour appréhender les apports de la technologie de chaine de blocs aux différents pans de l'économie réelle.
Si sa mise en oeuvre est récente, l'idée est loin d'être nouvelle. Elle date de 1994, lorsque Nick Szabo, cryptographe de génie, soumet pour la première fois la possibilité d'enregistrer des contrats sous la forme d'un code informatique qui s'activerait automatiquement lorsque certaines conditions seraient réunies.
L'automatisation des transactions et la concrétisation de l'idée de smart contracts on réalise pour la première fois via la technologie de chaine de blocs grâce au réseau Ethereum, créé en 2013 par Vitalik Buterin.

Une nouvelle approche de l'accord

Tutoriel appartenant à Umberto



AVENTADOR LP 700-4 Coupe

Désignation	Code	Tarif Client France en Euros Prix TTC	Prix HT
Basic Color : Nero Aldebaran / Giallo Evros		inclus	inclus
Solid Color : Bianco Icis		1 435,20	1 200,00
Color Metallic : Blu Hera / Nero Pegaso / Giallo Estrapue / Giallo Antares		1 913,60	1 600,00
Peinturos nacrées 3 couches : Giallo Orion / Arancio Atlas / Arancio Argos		3 588,00	3 000,00
Peintures Matt : Bianco Canopus / Nero Nemesis / Marrone Agus / Giallo Horus		11 960,00	10 000,00
Couleurs hors programme	WHM	7 774,00	6 500,00
Anneau Moteur Carbone	CF2	2 152,80	1 800,00
Capot Moteur Transparent	HMT	6 458,40	5 400,00
Jantes Noir Brillant	CF2	1 554,80	1 300,00
Ressorts de Suspension arrière Jaune	2M3	956,80	800,00
Etriers de Freins Gris / Jaune / Orange	PC	956,80	800,00
Lamborghini Sound System (LSS)	SVK	3 588,00	3 000,00
Pack Assistance : Hodor AVGAR + Cambio de recul	TX9	4 186,00	3 500,00
Hoserbok (ouverture garage)	VCI	478,40	400,00
Sièges électriques & chauffants	VV1	3 588,00	3 000,00
Volant Multifonction en Cuir Lisse	2FP	598,00	500,00
Volant Multifonction en Alcantara	1M	1 315,60	1 100,00
Volant Multifonction en Cuir Perforé	2ZH	1 315,60	1 100,00
Volant en Alcantara	3KL	717,60	600,00
Volant en Cuir Perforé	2PV	717,60	600,00
Intérieur UNICOLOR avec Coutures contrastées	DLH	717,60	600,00
Intérieur SPORTIV avec Cuir	DCF	1 913,60	1 600,00
Intérieur SPORTIV avec Alcantara	DLN	2 591,60	2 165,00
Intérieur ELEGANTE	DLB	1 913,60	1 600,00
Intérieur ELEGANTE Plus (Cuir perforé)	DJL	2 990,00	2 500,00
Pack Branding	MRI	717,60	600,00
Version Tuteur	9JC	418,80	350,00

Facture pour une Lamborghini

The British Virgin Islands are a self-governing British overseas territory situated in the Caribbean just to the east of the US Virgin Islands.

The BVIs, as they are called, are a popular travel destination for sailors, fishermen, sun worshippers, and other independent travellers, albeit not for the most conscious. Boating among the dozens of tiny, mostly uninhabited, islands is a great trip on any tour of the Caribbean islands.

Understand

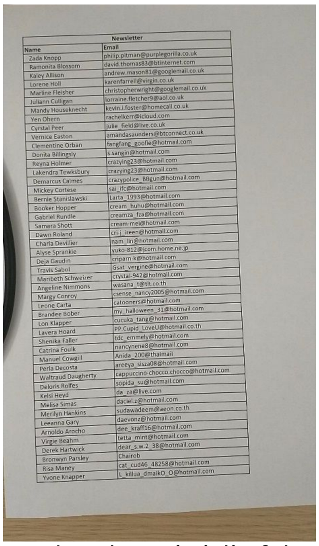
Landscape

The British Virgin Islands comprise 60+ islands and keys, with more than 40 of them being uninhabited islands. The islands fall into two types: the majority are steep volcanic islands (including the outer islands, Tortola and Virgin Gorda), and a small number of relatively flat coral islands (such as Anegada and Sandy Spit). Anegada is referred to as "the drowned island" because its elevation is so low. Many people own it altogether until they sail close to it. The highest point is Sage Mountain on Tortola.

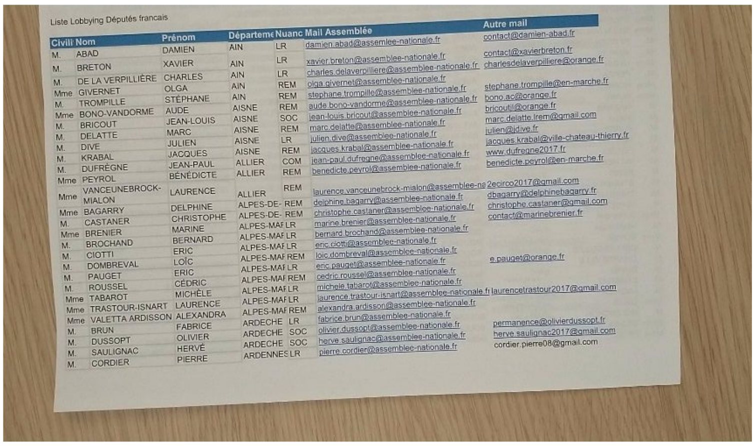
Climate

History

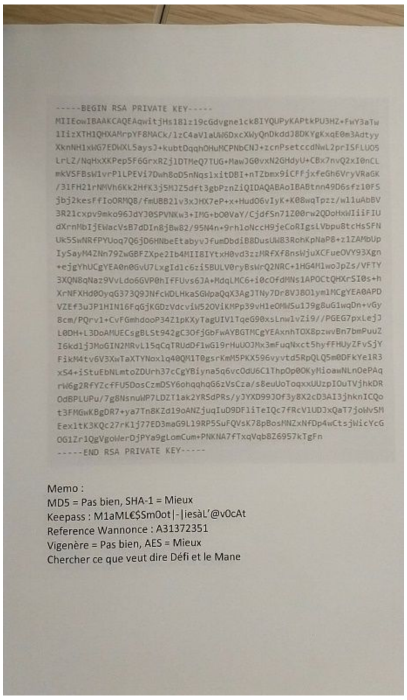
Guide de voyages aux îles vierges britanniques appartenant à Benoît



Listing des abonnés à l’infolettre



Listing de parlementaires afin de réaliser des actions de lobbying



Mémo appartenant à Pascal

Tatouage d’un lotus sur l’avant-bras permettant de repérer qui est Mei-Shi

Il était également nécessaire de mettre à l'épreuve ses talents de pickpocket afin de subtiliser un portefeuille Bitcoin en papier dépassant des poches d'Advei pendant qu'il marchait.

Il est à noter que certains agents ont récupéré sur le stand des cartes de visite SupremIoT.

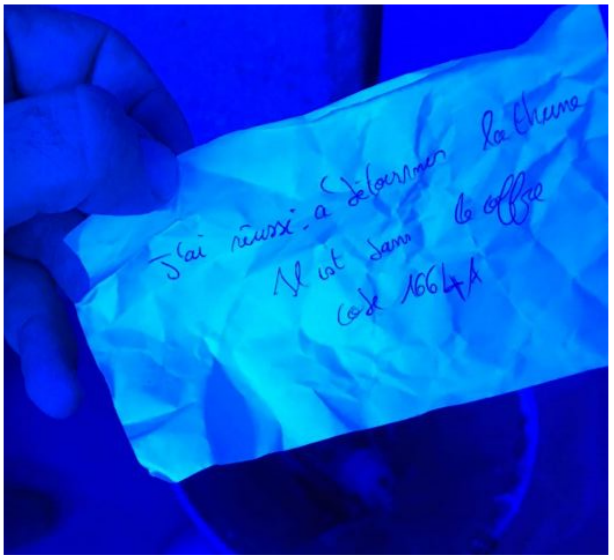
Précisons bien que ces cartes n'ont pas été réalisées par les équipes de SupremIoT. Encore une tentative de déstabilisation réalisée sans doute par une puissante étatique étrangère. Ces cartes menaient vers un faux indice, Zataz n'y ayant rien à voir.

Mais le but principal de la mission était de prendre en filature les cibles Advei et Benoît.

1. Filature de Benoît

La prise en filature de Benoît permettait surtout de remarquer qu'il a utilisé une boîte à lettre morte.

De fait, après un long parcours (sûrement pour essayer de semer des potentielles poursuivants), il s'arrête et écrit sur un papier qu'il jette à la poubelle. Le message inscrit précise qu'il a réussi à détourner l'argent et que celui-ci se trouve dans un coffre.



Nous avons ici même la preuve que Benoît a dupé l'ensemble de l'équipe de SupremIoT.

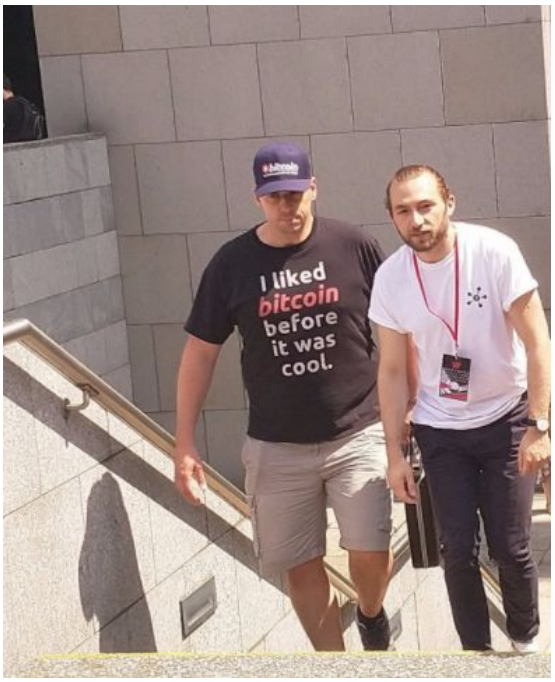
Après cette filature, Benoît se retrouvait seul, ce qui était le moment idéal pour lui parler dans le but d'enregistrer des aveux du détournement d'argent afin d'engager plus tard des poursuites contre lui.

Benoît en train de cracher le morceau

2. Filature d'Advei

La centrale sait qu'Advei doit rencontrer une personne blanchissant ses crypto actifs en euros, et plus si affinités...

Une filature du PDG permet de constater qu'il rencontre un russe avec un attaché-case menotté au poignet.



Réalisation de la transaction

Dès le départ du blanchisseur, les agents devaient aller à la rencontre d'Advei afin de le convaincre par tous moyens (sauf la force) de leur donner une somme d'argent servant à rembourser les infortunés clients.

Attaché-case contenant des portefeuilles Bitcoin, des coupures de 500€ ainsi que des sachets de cocaïne.

VI. L'affaire Mei-shi

Pendant que la quasi-totalité des invités à l'événement vogue à ses occupations, certains services sont sur le pied de guerre.

L'agent Mei-shi des services secrets chinois, qui met en vente son Raspberry Pi avec le système d'exploitation KylinOS, intéresse grandement la centrale, mais pas que...

En effet, la centrale de Mei-shi a exigée qu'elle rende l'ordinateur à un agent de leurs services présent sur place. L'objectif des équipes est de récupérer coûte que coûte le dispositif électronique.

Bonjour,

Pour l'ultime mission, vous devez intercepter le Raspberry détenu par Mei Shi (agent chinois en train de réaliser l'opération Black Panda !)
Le Raspberry doit surement détenir des informations de la plus haute importance !
Les agents SIS vous donnent rendez-vous à **19H15** au stand SupremIoT pour vous fournir plus d'informations ainsi que du matériel.
Vous devrez suivre l'individu.

Une seule personne doit aller rencontrer Mei Shi, se faire passer pour un agent allié de Mei Shi et lui demander de fournir le Raspberry comme convenu.
Le reste de votre équipe devra suivre l'opération à distance.

Une division de soutien vous surveille.
En cas de problèmes, elle interviendra pour vous soutenir

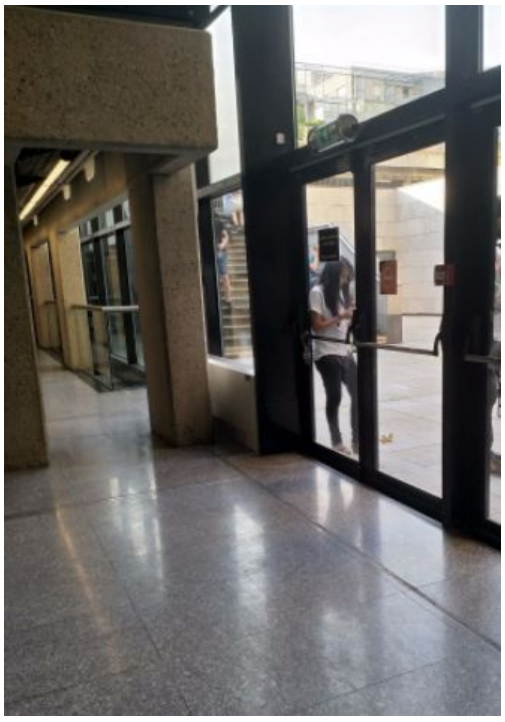
Les vidéos et fichiers son de cette partie sont essentielles.

Vous ne devrez montrer aucun signe de résistance !

Bon courage,

Agent Dupont

Une seule personne dans l'équipe sera autorisée à procéder à la rencontre avec Mei-shi afin de se faire passer pour l'agent légitime devant récupérer le colis. Le reste de l'équipe veillera à la sécurité du récupérateur et aidera à la filature afin de voir où Mei-shi attends son rendez-vous.



La cible attendant son rendez-vous

Échange en cours

Une fois l'échange réalisé, Mei-shi s'en va, mais l'agent de notre centrale se fait intercepté par le contre-espionnage français. Ceux-ci souhaitent en savoir plus sur le Raspberry Pi, mais surtout sur la personne ayant récupéré ce dispositif.

L'agent de notre centrale est emmené dans une salle à part et se trouve menotté en attendant que des agents français viennent l'interroger. Il dispose à ses côtés d'une barre métallique provenant d'un balai d'essuie-glace ainsi que d'une épingle à cheveux pour pouvoir se libérer avant que quelqu'un ne rentre dans la salle où il est enfermé.

La salle est protégée par un accès RFID. Les autres agents de l'équipe dont le malheureux coéquipier s'est fait intercepté ont pour mission d'interpeller les gardes devant la porte ou pendant leurs départs afin de copier depuis leur poche le badge qui leur permettra de rejoindre leur infortuné collègue.

Agent payant une bière à un fonctionnaire des services de contre-espionnage français afin de copier discrètement le badge RFID présent dans la poche

Une fois réunie dans la salle, l'équipe a pour objectif, dans un temps imparti, de :

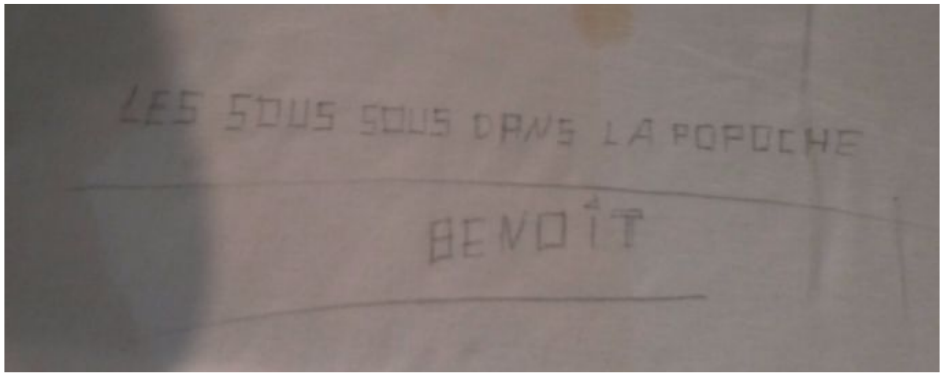
- Se connecter sur un miner Bitcoin et changer l'adresse de réception des Bitcoins ;
- Crocheter un caisson contenant à l'intérieur le coffre ainsi que des documents ;
- Crocheter l'attaché-case afin de récupérer l'ensemble de l'argent, des portefeuilles Bitcoin et de la cocaïne ;
- Procéder à du dumpster diving ;
- Miner une partie de bloc Bitcoin à la main.

Et c’est ainsi que s’achève la mission !

VII. Pour conclure…

Bien que le PDG reparte bredouille, certains employés de SupremIoT continuent de profiter d'une partie des bénéfices arnaqués aux innombrables d'investisseurs ouvertement arnaqués sur les réseaux sociaux et sur la table du stand.

SupremIoT @SupremIoT · 30 juin
Toute l'équipe de #SupremIoT vous remercie pour votre accueil à la #NDH16.
#FarineFrancine



VIII. Remerciements

HZV

L’ensemble des acteurs et contributeurs du challenge

Les participants

“Au service de la France” pour l'inspiration