

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

Published: 2017-06-29 · Archived: 2026-04-05 16:33:02 UTC

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)


Reply Reply All Forward

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

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

Dear Customer,

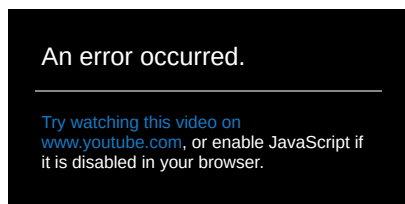
UPS courier was unable to contact you for your parcel delivery.

You can download the shipment label attached!

Yours truly,

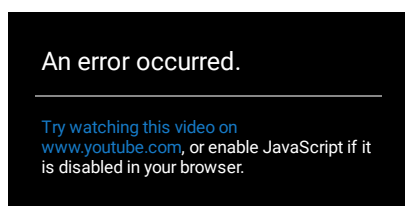
UPS Mail Delivery Agent.

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





## 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](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/?

0000000162citM2mvkp8bEpsLyUchneaUyauzndYZ01260400MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwxpEMyYKM9ghv4vgeQJwKXMCcsTvSGfNW4hF\_NZSEsKYjEn9GUxLPGcW1emZ92jcfllfODcX0Ru18cUUuHFkcH4bzAVAb32DVS6QlhSVKYffqfdzKEXiWKMfEAKmCCBQlaC7me9cOUxchwi9TetRquy4w1SvcAUIL4H8\_IviuKtI7B-jbrkYqTbS5CpyqV1nDKg4xiwW-2MCHBE3yE-TKsOS9G35UwrO99GNcEMX3Ok2eFEEjnipdLjTkYdvt67RkK\_hc\_5YvB7flwIDAQABRR99hCv\_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.iojosecurity.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/149863070/>

<https://www.hybrid-analysis.com/sample/21efa5573721890cdf9481f613ccb7d633733f05bc29cfeae402802e382cc92?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  
vademecca.com.ar  
vinoteka28.ru  
zgqyzjxh.com  
osadakrajenska.pl  
chymeres.org  
www.mecanique-de-precision.net  
winnicemoldawii.pl  
www.agrimixxshop.com  
luxelimo.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  
anthonydavies.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  
infirmierifktmatuziani.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](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:

- o Download Tor Browser here: <https://www.torproject.org/download/download-easy.html.en>
- o Install and run Tor Browser
- o 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/f2281cdabf9498ee754740b69c41d15f3ba91a82eb61d34f2cd857acaeab962/analysis/1500796303/>

<https://www.hybrid-analysis.com/sample/f2281cdabf9498ee754740b69c41d15f3ba91a82eb61d34f2cd857acaeab962?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.businessstowork.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-  
yz3Tp7DD8Ke2HYOg7K48BFetgvryWkHOAMPcieVNXhHY0ScvU5hYFzPbYyeviYtyt1v8TL6kc8i4I0

which when decoded gives

<sitename>/counter/?aY5rzyqa6RhRlp5-  
yz3Tp7DD8Ke2HYOg7K48BFetgvryWkHOAMPcieVNXhHY0ScvU5hYFzPbYyeviYtyt1v8TL6kc8i4I +n where n is 2-4

Analysis reports

<https://www.hybrid-analysis.com/sample/3b60fde281d91cc3e7ea3e343ee5b13a31def564903c0136ae928f70e25c3c02?environmentid=100>

<https://www.hybrid-analysis.com/sample/da40684e0f603ca5bfdc99b958fa39d3b64f5aabb1096ce2570c478259f177e?environmentId=100>

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

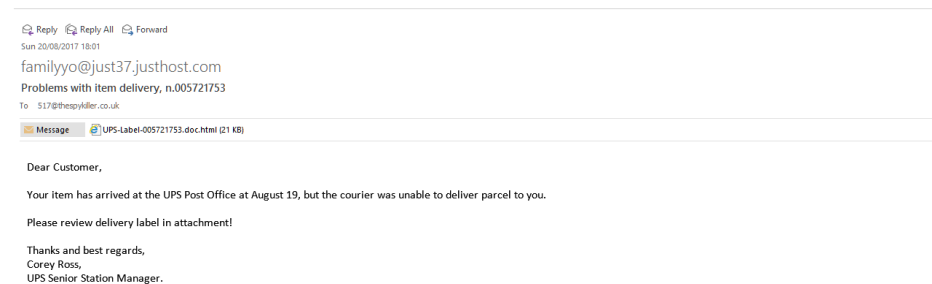
<https://www.hybrid-analysis.com/sample/3b60fde281d91cc3e7ea3e343ee5b13a31def564903c0136ae928f70e25c3c02?environmentId=100>

**Update 20 August 2017:**

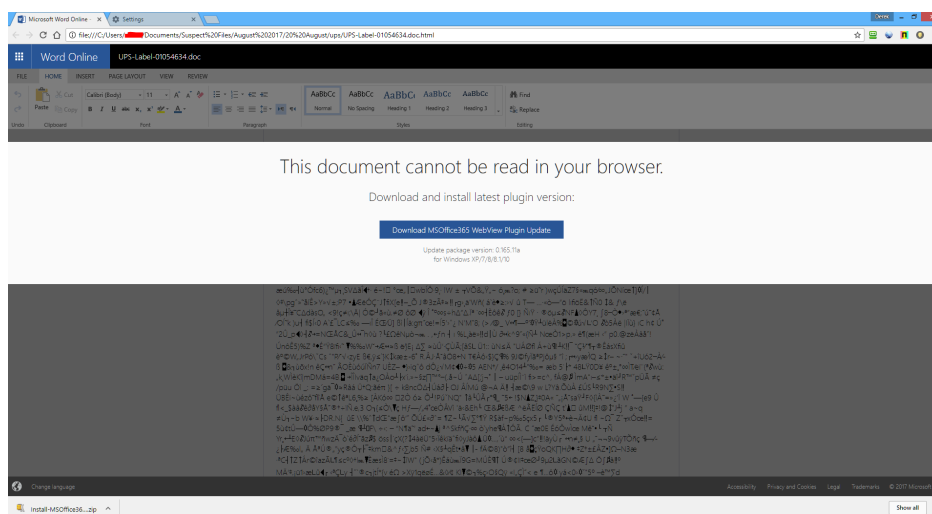
Yet another change to the delivery method this afternoon/evening

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:



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



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/>

---

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