Fake CDC Flu Pandemic Warning delivers Gandcrab 5.2 ransomware

web.archive.org/web/20190331091056/https://myonlinesecurity.co.uk/fake-cdc-flu-pandemic-warning-delivers-gandcrab-5-2-ransomware/

By 13 March 2019 5:12 am

A somewhat interesting and slightly alarming malware campaign, spreading worldwide but supposed to be targeting the USA that pretends to be an urgent message from the CDC (Centre for Disease Control) warning about a flu outbreak. This delivers Gandcrab 5.2 ransomware that currently does not have free decryption available yet.

They are using email addresses and subjects that will scare, shock, persuade or entice a recipient to read the email and open the attachment.

Remember many email clients or webmail services, especially on a mobile phone or tablet, only show the Name in the From: and not the bit in **<**domain.com **>.** That is why these scams and phishes and malware deliveries work so well.

To confuse the issue even more the subject line was written in what looks like a mix of cyrillic & western characters & encoded in UTF8 format so a computer will automatically translate / decode it. When I first tried to post this, I got a garbled mess of characters in the url to this post where the Copy & pasting from the email picked up the utf8 format

```
Subject: =?utf-8?B?Rmx1IHDQsG5k0LVtaWMgd9Cwcm5pbmcu?=
```

You can now submit suspicious sites, emails and files via our Submissions system

The CDC has not been hacked or had their email or other servers compromised. They are not sending the emails to you. They are just innocent victims in exactly the same way as every recipient of these emails. These came from numerous different email addresses & domains on the same server

The email looks like:

From: Centers for Disease Control and Prevention. <Peter@eatpraynope.com>

Date: Tue 12/03/2019 22:52

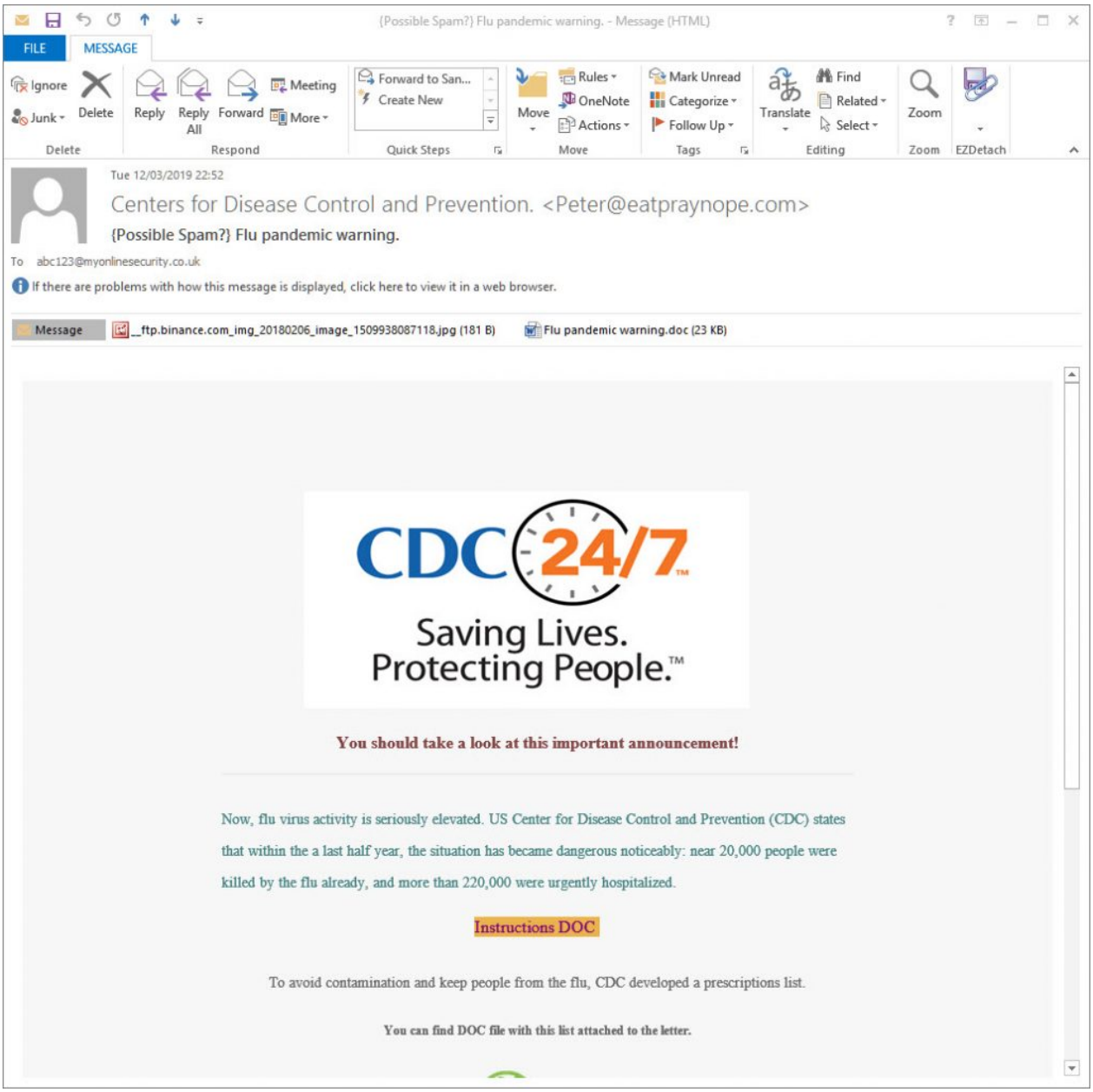
Subject: Flu pandemic warning.

Attachment: Flu pandemic warning.doc

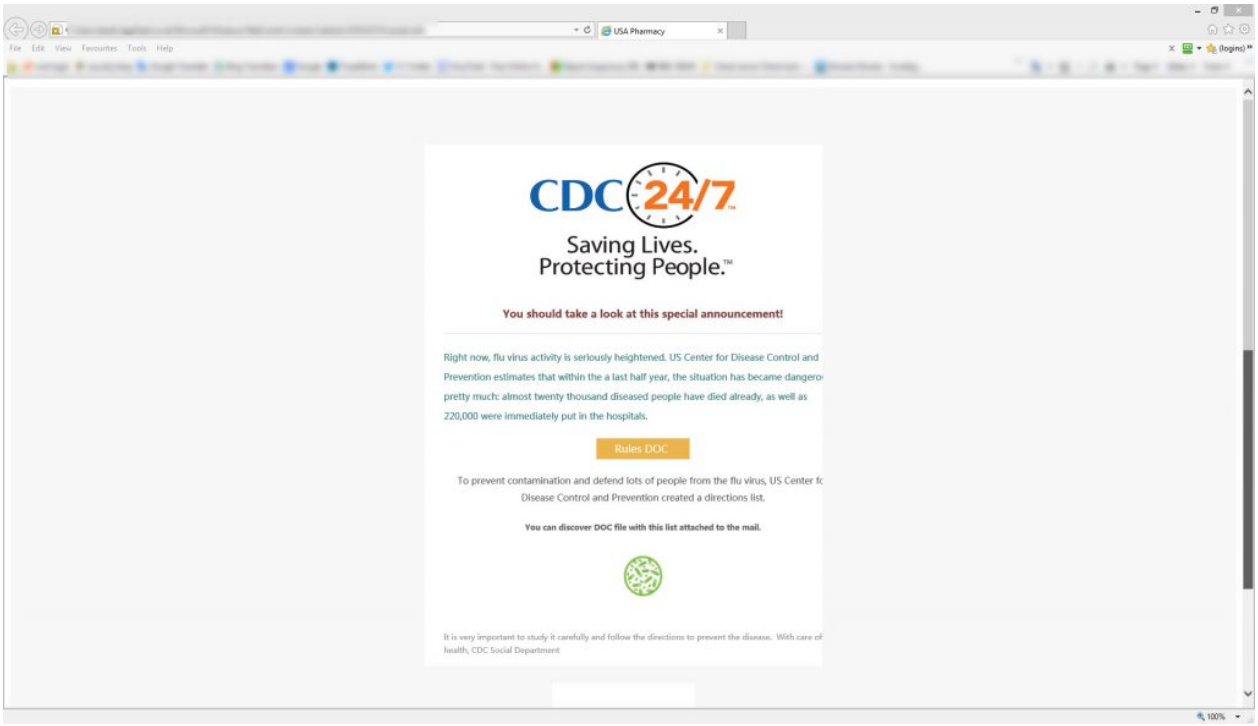
Body content:

> **You should take a look at this important announcement!**
>
> Now, flu virus activity is seriously elevated. US Center for Disease Control and Prevention (CDC) states that within the a last half year, the situation has became dangerous noticeably: near 20,000 people were killed by the flu already, and more than 220,000 were urgently hospitalized.
>
> Instructions DOC
>
> To avoid contamination and keep people from the flu, CDC developed a prescriptions list.
>
> **You can find DOC file with this list attached to the letter.**
>
> It is strongly recommended to study it with care and follow the directions to avoid the disease. With care of your health, CDC Communication Department
>
> Not interested anymore? Unsubscribe
> B© 2001вЂ“2019 All rights Reserved.

Screenshot:

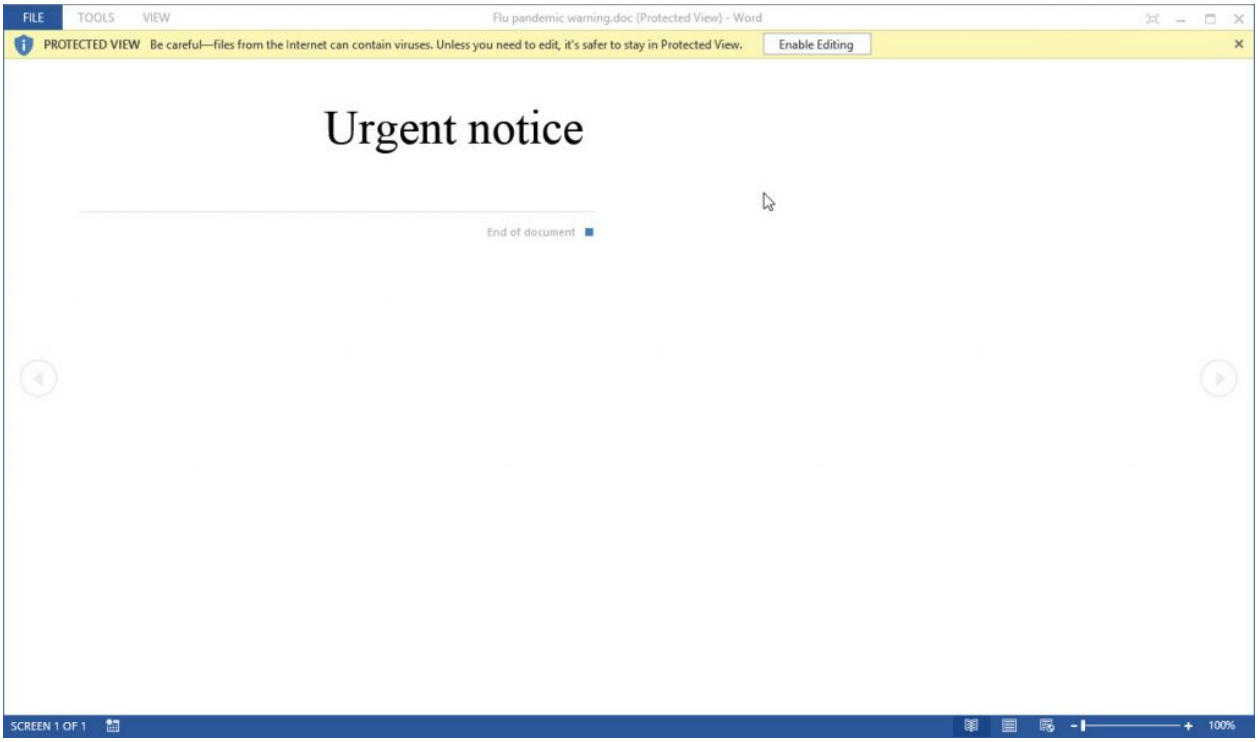


Fake CDC email



Fake CDC email

The Word doc attachment is almost empty with just an Urgent Notice Heading. The scumbags trying to compromise you are hoping that you will enable content & editing to enable the macros that let this run.



Fake CDC word doc Urgent Notice

Flu pandemic warning.doc Current Virus total detections: Anyrun|

This malware doc downloads from **http://205.185.125.109/samanta.exe** (VirusTotal)

The C2 for this is a well known site **https://www.kakaocorp.link/static/tmp/eshe.png** where the ransomware posts encrypted / encoded details about the compromised computer.

As usual this still drops a text file in each folder that it has encrypted and changes the desktop background

The ransom note looks like this (I have blurred out a lot of the content) the computer data section is the same as the details sent to the C2

```
---=    GANDCRAB V5.2    =---

**********************UNDER NO CIRCUMSTANCES DO NOT DELETE THIS FILE, UNTIL ALL YOUR DATA IS RECOVERED**********************

        *****FAILING TO DO SO, WILL RESULT IN YOUR SYSTEM CORRUPTION, IF THERE ARE DECRYPTION ERRORS*****

Attention!

All your files, documents, photos, databases and other important files are encrypted and have the extension: .VGCHVRLY

The only method of recovering files is to purchase an unique private key. Only we can give you this key and only we can recover your files.


The server with your key is in a closed network TOR. You can get there by the following ways:

--------------------------------------------------------------------------------

| 0. Download Tor browser - https://www.torproject.org/

| 1. Install Tor browser
| 2. Open Tor Browser
| 3. Open link in TOR browser:   http://gandcrabmfe6mnef.onion/5124d7737cd9e0e6
| 4. Follow the instructions on this page

--------------------------------------------------------------------------------


On our page you will see instructions on payment and get the opportunity to decrypt 1 file for free.


ATTENTION!

IN ORDER TO PREVENT DATA DAMAGE:

* DO NOT MODIFY ENCRYPTED FILES
* DO NOT CHANGE DATA BELOW

---BEGIN GANDCRAB KEY---
lAQAAMwfybZVSLFbLQOdE1cSzKRWaNVSDEMDyOZvffbFwUa
+mEE9bGZNRhOHGMhmPJOTSuQ7vuZrmd62k9OqcMJCh4Ln3O/jcgGnm5vdyYvn4rUJeKY8x8qi76v0e3cyQlpIgqC36CCsq3Zm0q2c9Q6XCjkvGcZAvW512mOU3ZwJHOkaPXbEAOgFmsxmVAv8zLB
                                                                                                                                                    Jr+3E3xSbYpLTsSlHm/ZdVoBWkULKfNlgVU
                                                                                                                                                    /zhvD+ddfj/LOJ5JZoNVLVaOJM
                                                                                                                                                    TN61PWZAHwdgELy8wKSYePVV/QnBqQo0oQKT2pd
                                                                                                                                                    gcP79puLGckpM4fABSr0VY2iRivWLsV5p/v
                                                                                                                                                    JMLY
                                                                                                                                                    clZGfXUlV6RacnDQqB+iCt0PSTerF
                                                                                                                                                    SzUkcDnoyQ8DeZgpLAgOVzQnGIW2J5TMzwJhGH7+R6BlL
                                                                                                                                                    /DpoOuOy9NxiD
                                                                                                                                                    /vqKuFA7Jjruedl6hKsMjsh3ltP1PhVRD
                                                                                                                                                    vhn1W5ZiBzJcQ50BIUe/0xutwHOyOObkaybyVLML2IbFVw
                                                                                                                                                    /uVH0qnOuTtpvAuc0dcHUC7zglIK/P
+/VrsnQAdjs6uQEINlaYwemFGguJ7bAK3Jfm2HOXtm10D8gjab2GQy5Pf0WEVn74NzQRgdiPcWdHTPg4TApVGRsDgrc6XK3lAi3A4hHKIrHss3Fb7beEXevz+ZsjMMji+CtbC
+BpmGWddj1K2N/eKTNcp/lck9WAq+TO4/smDM0fPxCeoDuzIWLuAGieRVmfBxJA1oHYzXiMX2HAoalWZA4WCwww9l
+1dgpaugmoGdOxpnIBX7dxsDFM4DiqXLURpCUSEFSVdGGMEcBSkd0iylqvXYhgy2jjPoel2/I2eGwlM=
---END GANDCRAB KEY---

---BEGIN PC DATA---
7ftDEgLb/ZS0lcmZbHM61IDJ6AOtD78KkA7absMgUXYxWLsC+5+UYF9xVmDr9M/JOZDIAomVteDDRQ3IfHQEQwea5LPnzpQSSOggau
                                                                                                                                                    2igEn2up2xUzR73t
+WDkyMD58TsGXvLA6j6/1AWA/1nZUGKK1g1o2eWKH+bAK8vD11y4EUErtE91NgAiAnm9QY1EV1TKGZyY6MP51B1K8/OeRMeZEE1XTLCPPN9CUPA==
---END PC DATA---
```

Gandcrab 5.2 ransomware note

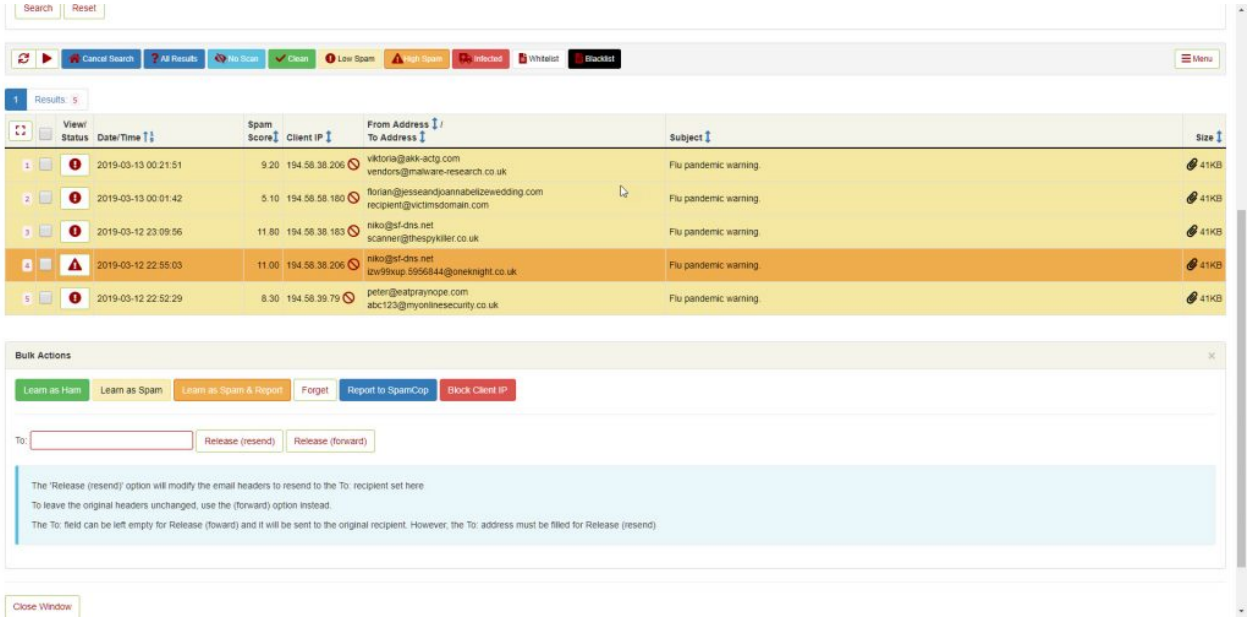
Email Headers:

IP	Hostname	City	Region	Country	Organisation
194.58.39.79	eatpraynope.com			RU	AS197695 Domain names registrar REG.RU, Ltd

```
Received: from eatpraynope.com ([194.58.39.79]:53462)
        by my emnail server with esmtp (Exim 4.91)
        (envelope-from <Peter@eatpraynope.com>)
        id 1h3qFp-0006zX-2T
        for abc123@myonlinesecurity.co.uk; Tue, 12 Mar 2019 22:52:13 +0000
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; s=mail; d=eatpraynope.com;
 h=Message-ID:From:To:Subject:Date:MIME-Version:Content-Type;
i=Peter@eatpraynope.com;
 bh=au57B5AjAYA8CV51N8wUPa2oKbcn4cMHOk1pSWI+wPw=;
 b=ajb75+gP8xkU82j754wURfAVH+pizwP+dJ+PymiMQRD/i68Ebvm4ek9aYCdjMNUIHtaZNN1S6GjZ
   rttgYhdZ0PHEVi8ZCfnYwmw4GTHy8RTLzp5rW3iWleJeFP32X2ysR7pEKYyZcKj07u/D3UA5nNvQ
   mUqaWOgSrMQpix47/hM=
Message-ID: <069ddf0efa09cdeac937c192994d4599ba6f4a88ef@eatpraynope.com>
From: "Centers for Disease Control and Prevention." <Peter@eatpraynope.com>
To: <abc123@myonlinesecurity.co.uk>
Subject: =?utf-8?B?Rmx1IHDQsG5k0LVtaWMgd9Cwcm5pbmcu?=
Date: Tue, 12 Mar 2019 15:51:31 -0700
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="ab513f7da27658eb37327bf5d105001304f7"
```

The other emails I saw were all from same IP & server 194.58.39.79

viktoria@akk-actg.com
florian@jesseandjoannabelizewedding.com
niko@sf-dns.net
peter@eatpraynope.com



fake CDC email list

All the alleged senders, companies, names of employees, phone numbers, amounts, reference numbers etc. mentioned in the emails are all innocent and are just picked at random. Some of these companies will exist and some won't. **Don't try to respond by phone or email, all you will do is end up with an innocent person or company who have had their details spoofed and picked at random from a long list that the bad guys**

have previously found . The bad guys choose companies, Government departments and other organisations with subjects that are designed to entice you or alarm you into blindly opening the attachment or clicking the link in the email to see what is happening.

This email attachment contains what appears to be a genuine word doc or Excel XLS spreadsheet with either a macro script or an embedded OLE object that when run will infect you.

Modern versions of Microsoft office, that is Office 2010, 2013, 2016 and Office 365 should be automatically set to higher security to protect you.

By default protected view is enabled and macros are disabled, UNLESS you or your company have enabled them. If protected view mode is turned off and macros are enabled then opening this malicious word document will infect you, and simply previewing it in windows explorer or your email client might well be enough to infect you. **Definitely DO NOT follow the advice they give to enable macros or enable editing to see the content**.

Most of these malicious word documents either appear to be totally blank or look something like these images when opened in protected view mode, which should be the default in Office 2010, 2013, 2016 and 365. Some versions pretend to have a digital RSA key and say you need to enable editing and Macros to see the content. **Do NOT enable Macros or editing under any circumstances**.

What can be infected by this
At this time, these malicious macros only infect windows computers. **They do not affect a Mac, IPhone, IPad, Blackberry, Windows phone or Android phone**. The malicious word or excel file can open on any device with an office program installed, and potentially the macro will run on Windows or Mac or *any other device with* ***Microsoft Office*** *installed.* BUT the downloaded malware that the macro tries to download is windows specific, so will not harm, install or infect any other computer except a windows computer. You will not be infected if you do not have macros enabled in Excel or Word. These Macros do not run in "Office Online" Open Office, Libre Office, Word Perfect or any other office program that can read Word or Excel files.

Please read our How to protect yourselves page for simple, sensible advice on how to avoid being infected by this sort of socially engineered malware. Also please read our post about word macro malware and how to avoid being infected by them

Be very careful with email attachments. All of these emails use Social engineering tricks to persuade you to open the attachments that come with the email. It might be a simple message saying “look at this picture of me I took last night” that appears to come from a friend. It might be a scare ware message that will make you open the attachment to see what you are accused of doing. Frequently it is more targeted at somebody (small companies etc.) who regularly receive PDF attachments or Word .doc attachments or any other common file that you use every day, for example an invoice addressed to sales@victimcompany.com.

The basic rule is **NEVER** open any attachment to an email, unless you are expecting it. Now that is very easy to say but quite hard to put into practice, because we all get emails with files attached to them. Our friends and family love to send us pictures of them doing silly things, or even cute pictures of the children or pets. Many of us routinely get Word, Excel or PowerPoint attachments in the course of work or from companies that we already have a relationship with.

Never just blindly click on the file in your email program. Always save the file to your downloads folder, so you can check it first. A lot of malicious files that are attached to emails will have a faked extension. That is the 3 letters at the end of the file name. Unfortunately windows by default hides the file extensions so you need to **Set your folder options** to “show known file types. Then when you unzip the zip file that is supposed to contain the pictures of “Sally’s dog catching a ball”, an invoice or receipt from some company for a product or service or receive a Word doc or Excel file report that work has supposedly sent you to finish working on at the weekend, you can easily see if it is a picture or document & not a malicious program. If you see **JS or .EXE or .COM or .PIF or .SCR or .HTA .vbs, .wsf , .jse .jar** at the end of the file name **DO NOT** click on it or try to open it, it will infect you.

With these malformed infected word, excel and other office documents that normally contain a vba macro virus, the vital thing is do not open any office document direct from your email client or the web. Always save the document to a safe location on your computer, normally your downloads folder or your documents folder and scan it with your antivirus. Many Antiviruses do not natively detect vba macro-viruses in real time protection and you need to enable document or office protection in the settings. Do not rely on your Anti-Virus to immediately detect the malware or malicious content. **DO NOT enable editing mode or enable macros**

All modern versions of word and other office programs, that is 2010, 2013, 2016 and 365, should open all Microsoft office documents that is word docs, excel files and PowerPoint etc that are downloaded from the web or received in an email automatically in

“protected view” that stops any embedded malware or macros from being displayed and running. Make sure protected view is set in all office programs to protect you and your company from these sorts of attacks and do not over ride it to edit the document until you are 100% sure that it is a safe document. If the protected mode bar appears when opening the document **DO NOT enable editing mode or enable macros** the document will look blank or have a warning message, but will be safe.

Be aware that there are a lot of dodgy word docs spreading that WILL infect you with no action from you if you are still using an out dated or vulnerable version of word. This is a good reason to update your office programs to a recent version and stop using office 2003 and 2007. Many of us have continued to use older versions of word and other office programs, because they are convenient, have the functions and settings we are used to and have never seen a need to update to the latest super-duper version. The risks in using older version are now seriously starting to outweigh the convenience, benefits and cost of keeping an old version going.

I strongly urge you to update your office software to the latest version and stop putting yourself at risk, using old out of date software.

IOC:

Main object- “Flu pandemic warning.doc”
sha256 a1ca75dfdcc8038650c27cbd4f7b3edc2cf5915cd75567c9bd2407ea0d099eba
sha1 7971cd39eee59bf64cc2dfd7610d6f529eafd9df
md5 fae8e6b098eb9ecce2611f1dffc8f7b9
Dropped executable file
sha256 C:\windows\temp\191.exe
73a994e9fa2804afceaf1286e4aba8522eb3c555b85766b03f03106118165736
MD5 27fa5f1ef590ee5e503c3d15f210dab7
SHA-1 6069666610d09085dc7926cde3d242427e67b167
DNS requests
domain www.kakaocorp.link
Connections
ip 107.173.49.208
ip 205.185.125.109
HTTP/HTTPS requests
url http://205.185.125.109/samanta.exe
url http://www.kakaocorp.link/
url https://www.kakaocorp.link/static/tmp/eshe.png

Emails from: (probably loads of other domains & addresses on same server)

viktoria@akk-actg.com
florian@jesseandjoannabelizewedding.com
niko@sf-dns.net
peter@eatpraynope.com
194.58.39.79