



My PC has 32,539 errors:
how telephone support scams *really* work

David Harley, ESET
Martijn Grooten, Virus Bulletin
Steve Burn, Malwarebytes
Craig Johnston, Independent

Dramatis Personae

(and how we got onto the same stage)

- David Harley
ESET Senior Research Fellow
- Martijn Grooten
Virus Bulletin Anti-Spam Test Director
- Steve Burn
MalwareBytes Research Engineer
- Craig Johnston
Independent Consultant

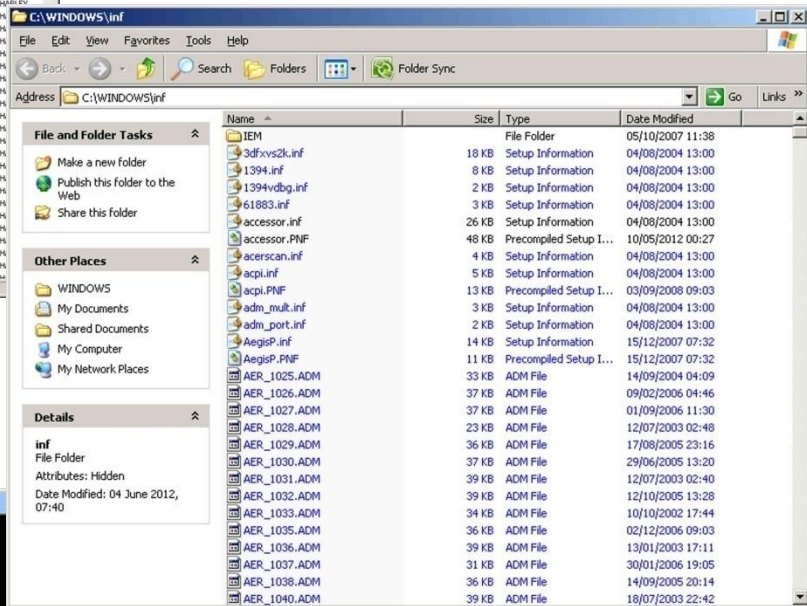
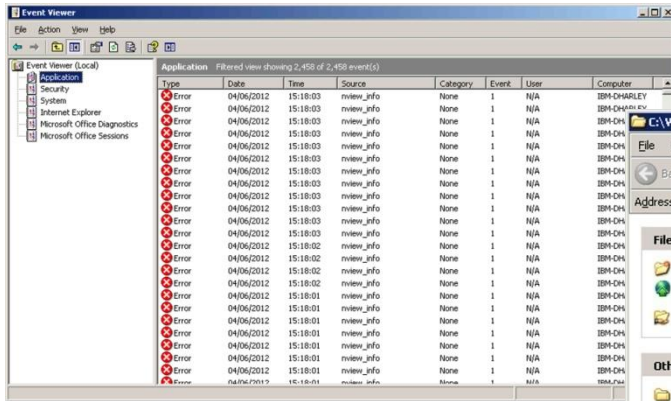


The Basic Scam

- Something is wrong with your PC, but I can help you fix it.
 - A ‘demonstration’ the problem using Event Viewer, ASSOC/CLSID, INF, PREFETCH, Task Manager...
 - Remote installation of ‘appropriate’ utilities and additional ‘diagnosis’
 - Transfer of funds and ‘fix’



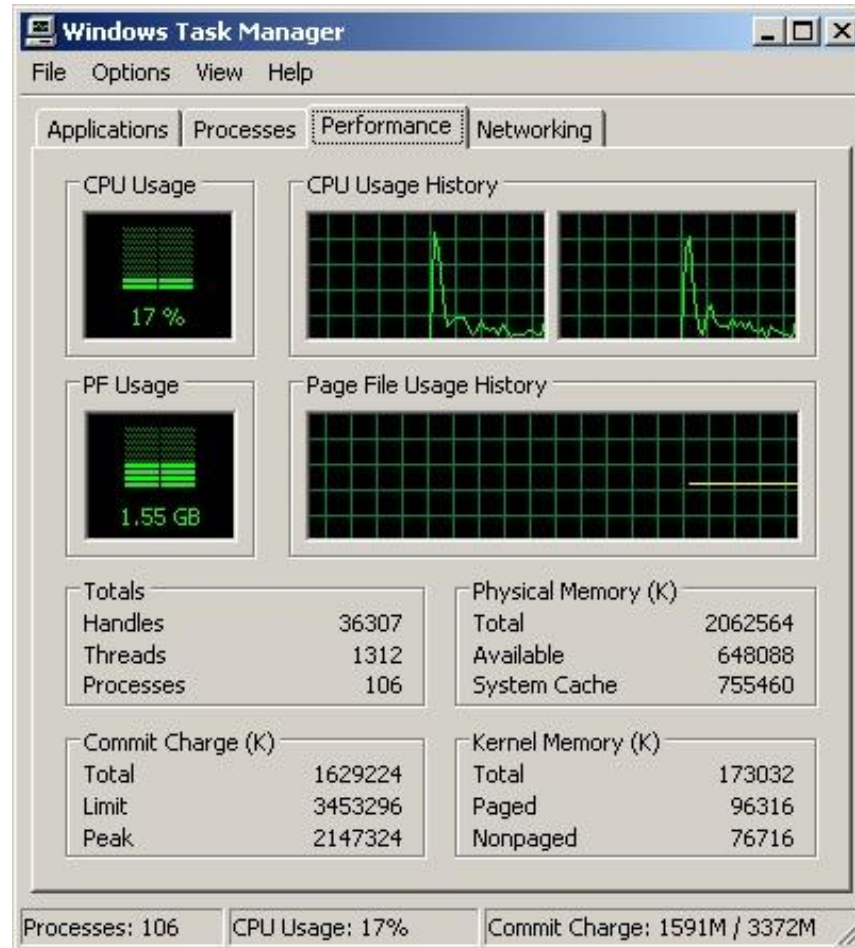
Event Viewer, ASSOC, INF



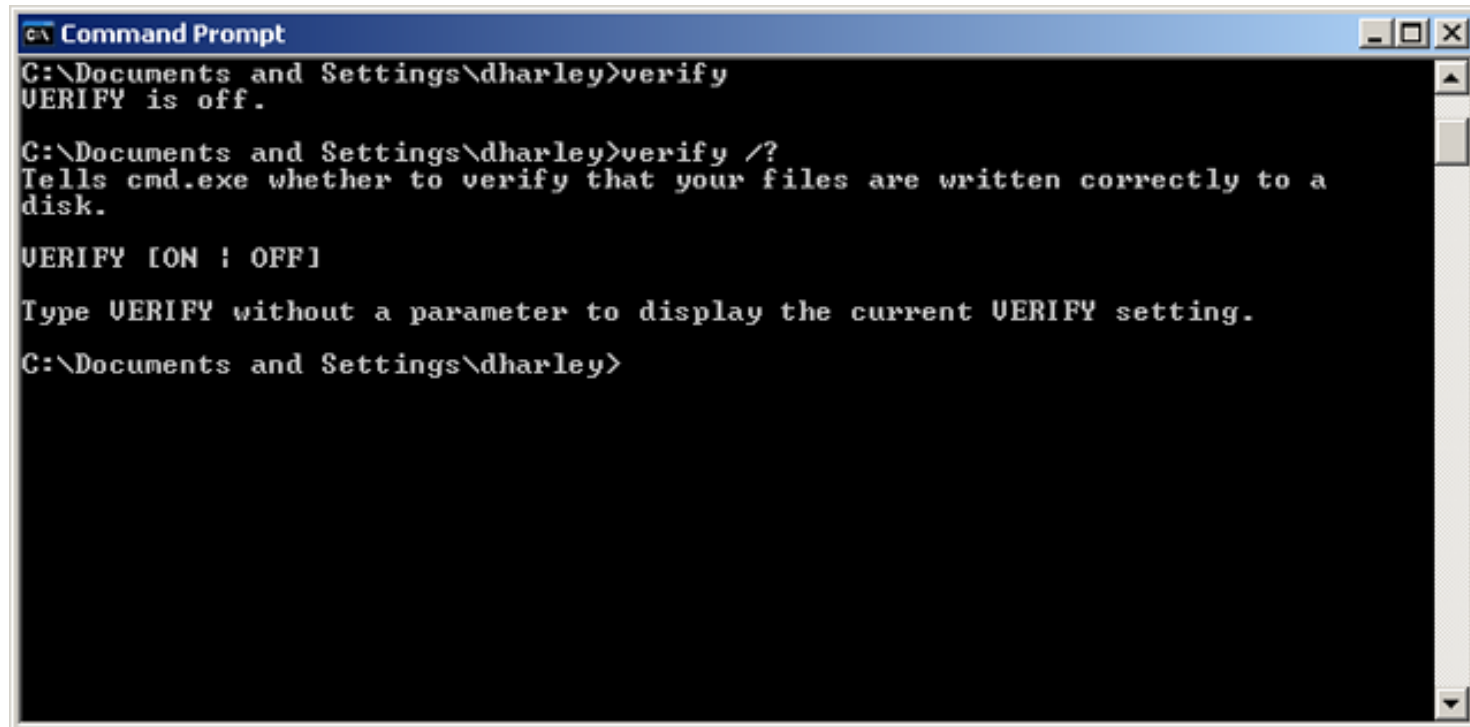
```
cmd Command Prompt
.\xlsn=Excel.SheetMacroEnabled.12
.\xlshhtml=Excel.HtmHtmlFile
.\xlx=Excel.Sheet.12
.\xlt=Excel.Template.8
.\xlthtml=Excel.HtmTemplate
.\xltm=Excel.TemplateMacroEnabled
.\xltx=Excel.Template
.\xlw=Excel.Workspace
.\xlxml=Excel.xmlss
.xml=>.xml file
.xps=XPSViewer.Document
.xsl=xsifile
.xslt=xsifile
.xst=PSIFile
.xxe=IZArcXXE
.yz1=IZArcYZ1
.z=IZArcZ
.z96=
.zap=zapfile
.ZFSendToTarget=CLSID\{888DCA60-FC0A-11CF-8F0F-00C04FD7D062}
.zip=IZArcZIP
.zon=OmniPage.ZoneTemplate
.zoo=IZArcZOO
C:\Documents and Settings\dharleley\assoc
```



Taken to task



Verily, Verify



```
c:\ Command Prompt
C:\Documents and Settings\dharley>verify
VERIFY is off.

C:\Documents and Settings\dharley>verify /?
Tells cmd.exe whether to verify that your files are written correctly to a
disk.

VERIFY [ON | OFF]

Type VERIFY without a parameter to display the current VERIFY setting.
C:\Documents and Settings\dharley>
```

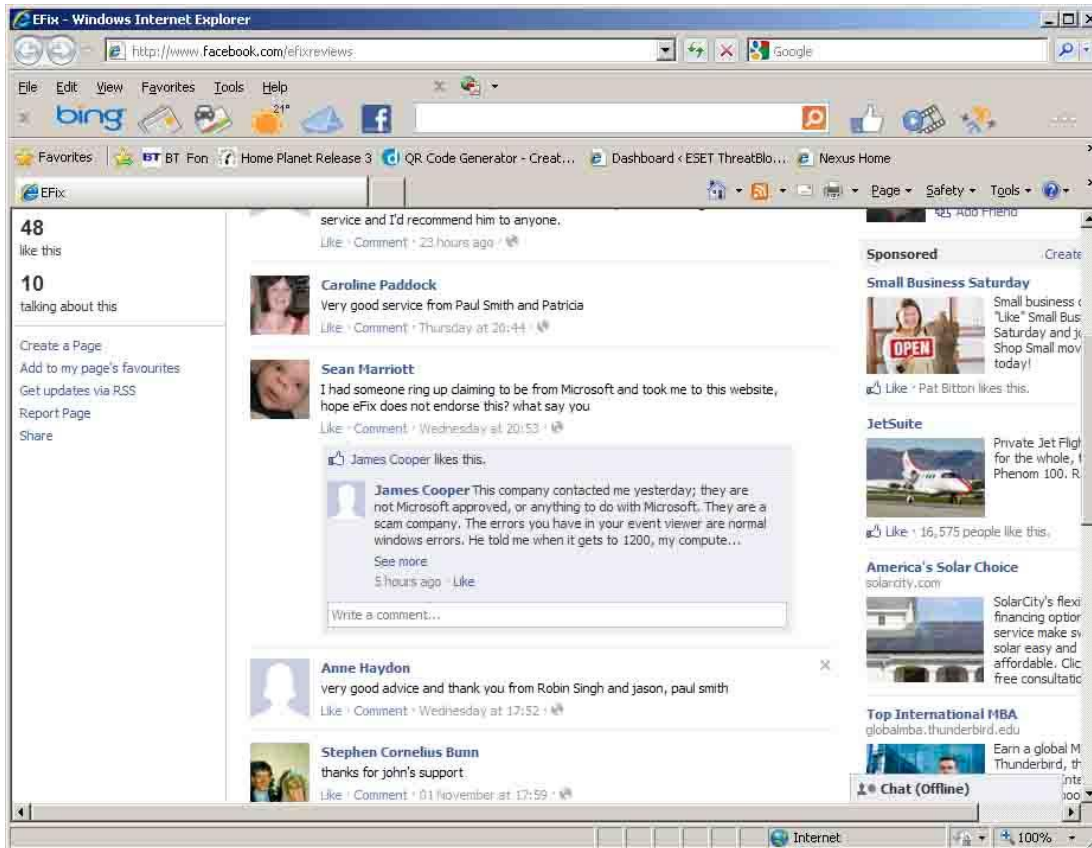


There's more to this than phone calls

- <http://blog.eset.com/2011/11/09/facebook-likes-and-cold-call-scams>
- eFIX Ltd, at 8901 Marmora Road, Glasgow, D04 89GR
- MR ANTHONY SCOTT CALLED ME TODAY TO OFFER THE E FIX SERVICE, WHICH has been fully explained to me and Mr Scott has been very helpful and patient. Thanks



At Your Service



The Problem: Telescammers

- Estimated 350,000 call center agents in India (New York Times)
- @ estimated 5% = 17,500 rogue call agents
- 17,500 @ 100 calls p/d = 1,750,000 calls per day
- 1,750,000 cpd @ 0.1% est conversion (avg \$200 p/v x 1750) = \$350,000 per day



Fighting the Telescammers today

- Takedown process
- Biggest obstacle = Indian LE
- We need Banks, credit card companies to get involved



What can I do? Get involved!

- One main issue, is we estimate that the amount of victims that have come forward to report this, are far lower than those actually taken in.
- We need more victims to feel comfortable enough to come forward and report this.
- We need more law enforcement involvement
- More collaboration between security companies

What can I do? Get involved!

Steven Burn

Email: sburn@malwarebytes.org



Introducing... PC-Optimizers

Select your Country:  

 **Annual PC Support**
for only £ 119 per year

  **Technical Support**
+44 808 234 8670

HOME ABOUT US PRICING & PLAN WE SUPPORT REMOTE SUPPORT CLIENTS REVIEW FEEDBACK CONTACT US

GET TECH SUPPORT IN ONE PHONE CALL
Support for PC, MP3s, Cameras, Wireless and more.

CALL **+44 808 234 8670**

 Windows

Services We Offer
We provide almost all gadget support

- PC Maintenance & Technical Support
- Computer Optimization
- Windows Support
- Wireless Internet Support
- Printer and Scanner Support
- Internet Support
- Virus Removal
- Spyware / Adware Removal
- Digital Camera and MP3 Support
- Support for Microsoft Office Setup
- E-mail set up and Support
- Data Back up

 **CONNECT TO TECHNICIAN**

 **FREE PC HEALTH CHECK**

SERVICES PLAN

- 1 Year Plan** **BUY NOW**
- 2 Year Plan** **BUY NOW**
Unlimited Support

Testimonials

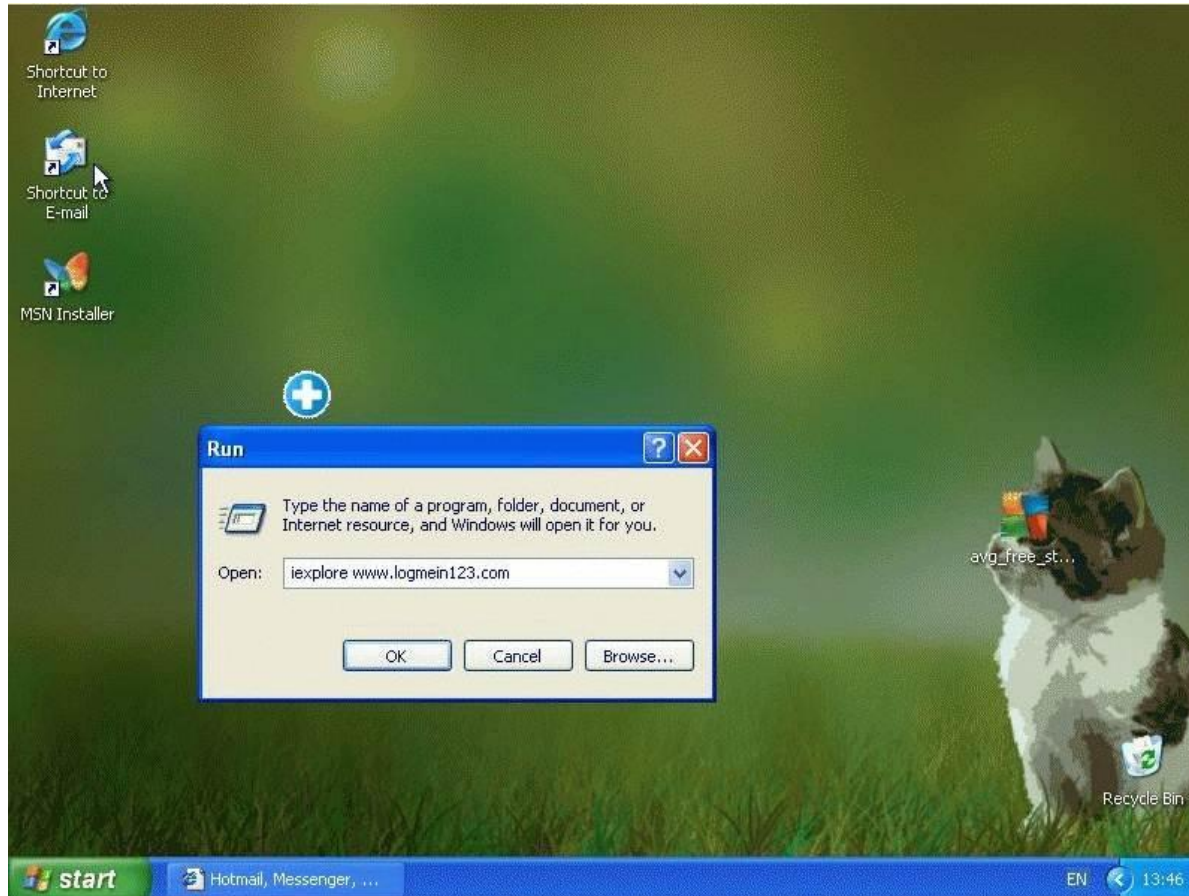
Welcome to Our Website

Photo Not Available **Barbara Johnson**
2011-11-05

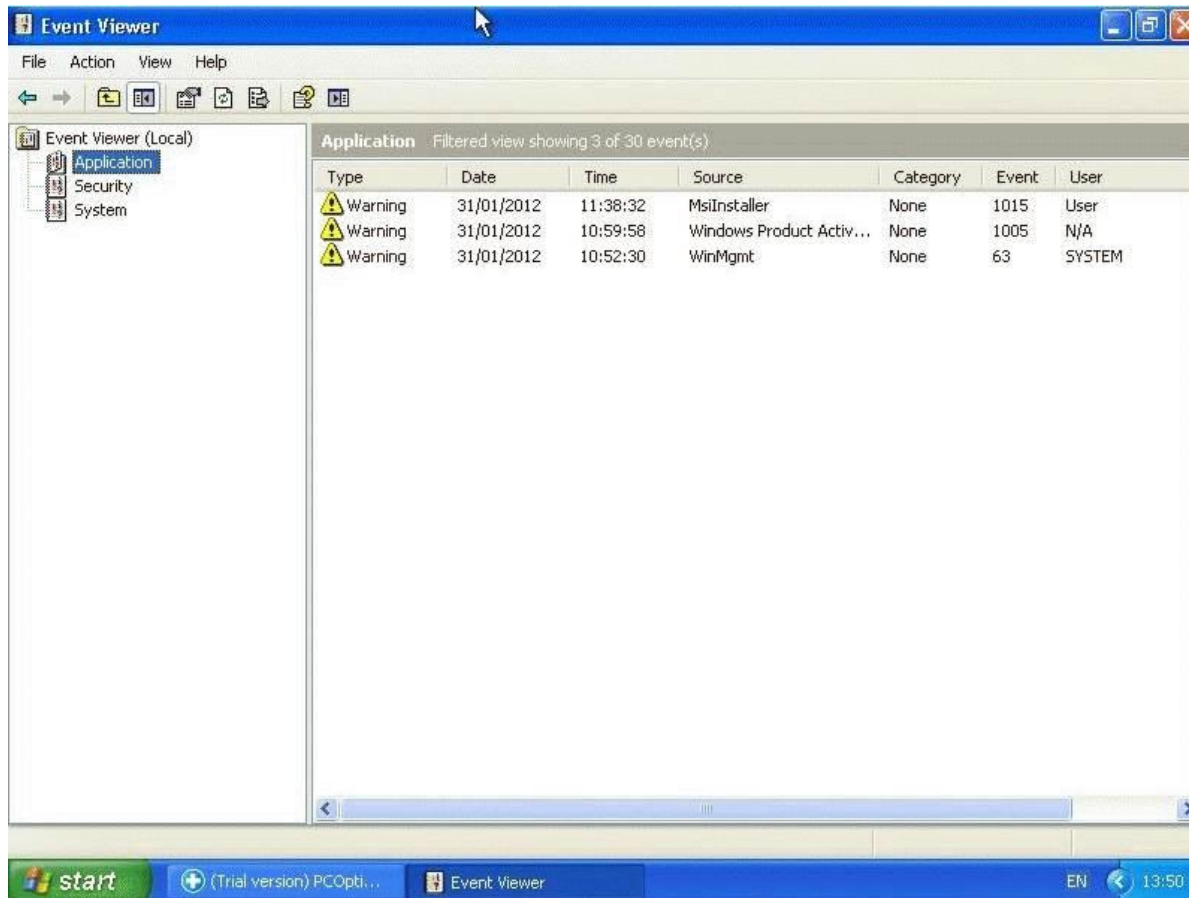
I am very pleased with how quickly you

...What's the common thing that drives Google, Yahoo, MSN and YouTube? You got it right, internet users

Log me in, please



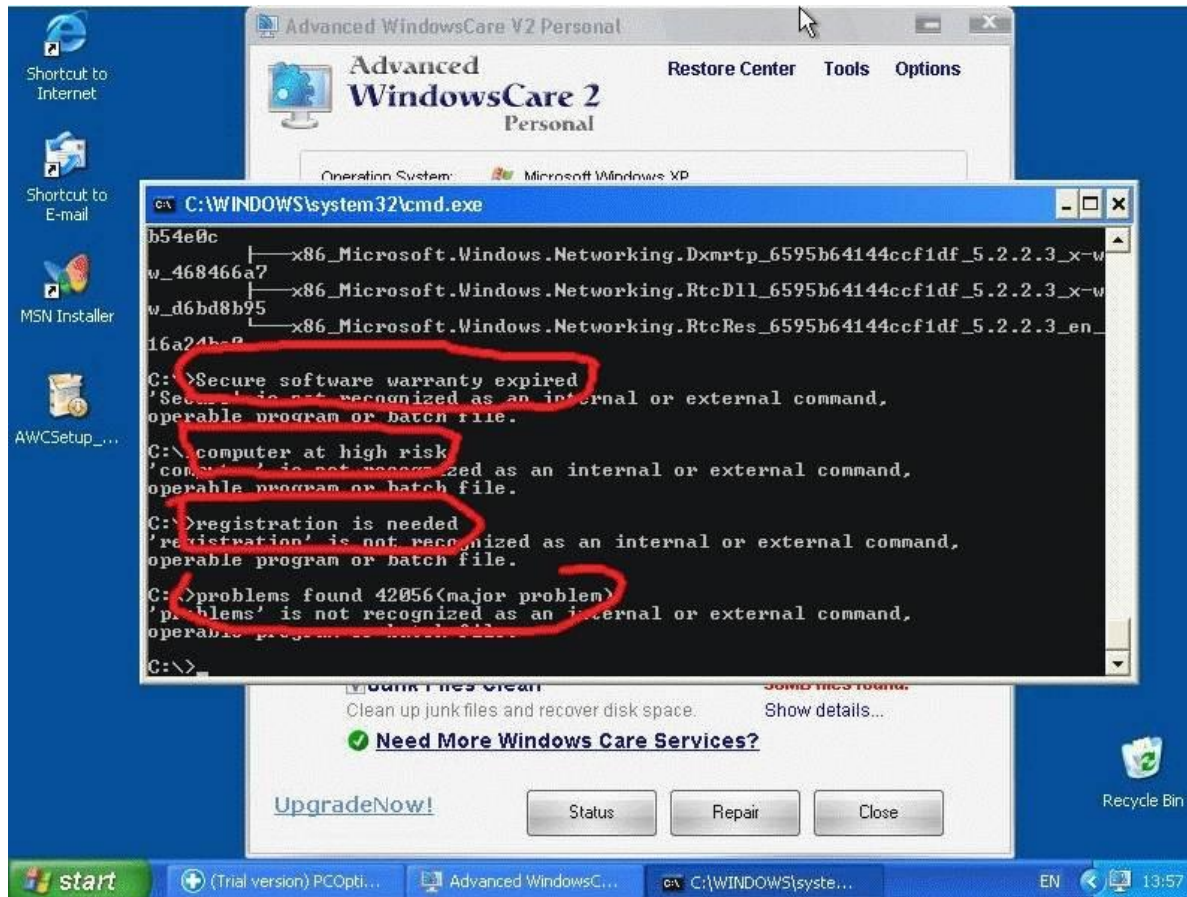
I have a small problem...



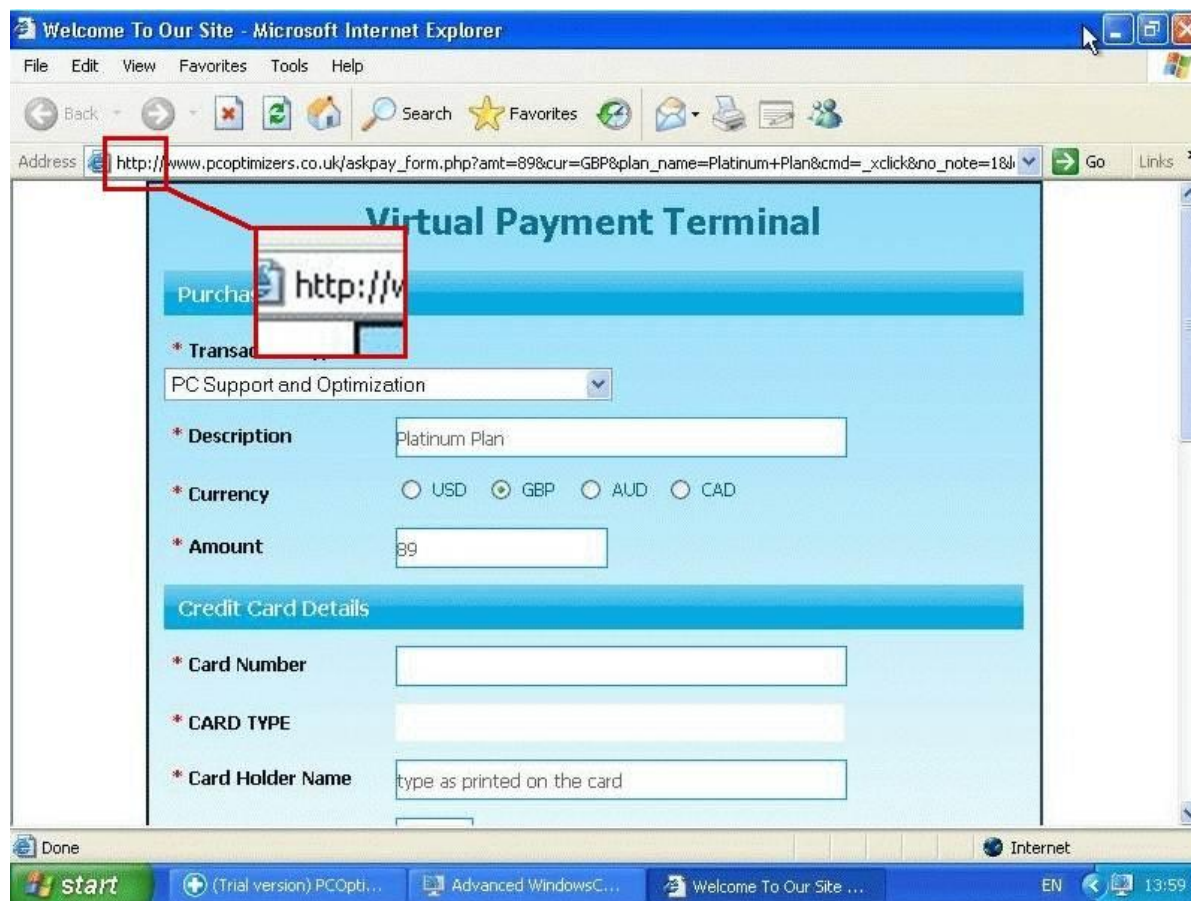
...or, perhaps, a big problem?




Like, a really big problem



A problem worth paying for



Now with added “security”

Date Of Birth	<input type="text"/> [DD-MM-YYYY]
SSN [Last 4 digit only]	<input type="text"/>
* Address	<input type="text"/>
* City/Town:	<input type="text"/>
* State/County:	<input type="text"/>
* Country:	<input type="text"/>
* Zip / POST CODE:	<input type="text"/>
* Best Call Back Time :	Select Time ▾
* Verification:	 Click here to refresh
	<input type="text"/>
<input checked="" type="checkbox"/> I acknowledge the information submitted is accurate to the best of my knowledge	
<input checked="" type="checkbox"/> I have read and agreed to the Terms & Conditions and Privacy Policy	
<input type="button" value="Process Transaction"/> <input type="button" value="Reset"/>	

...and my computer is secure again



But don't forget the T&Cs



The call ends

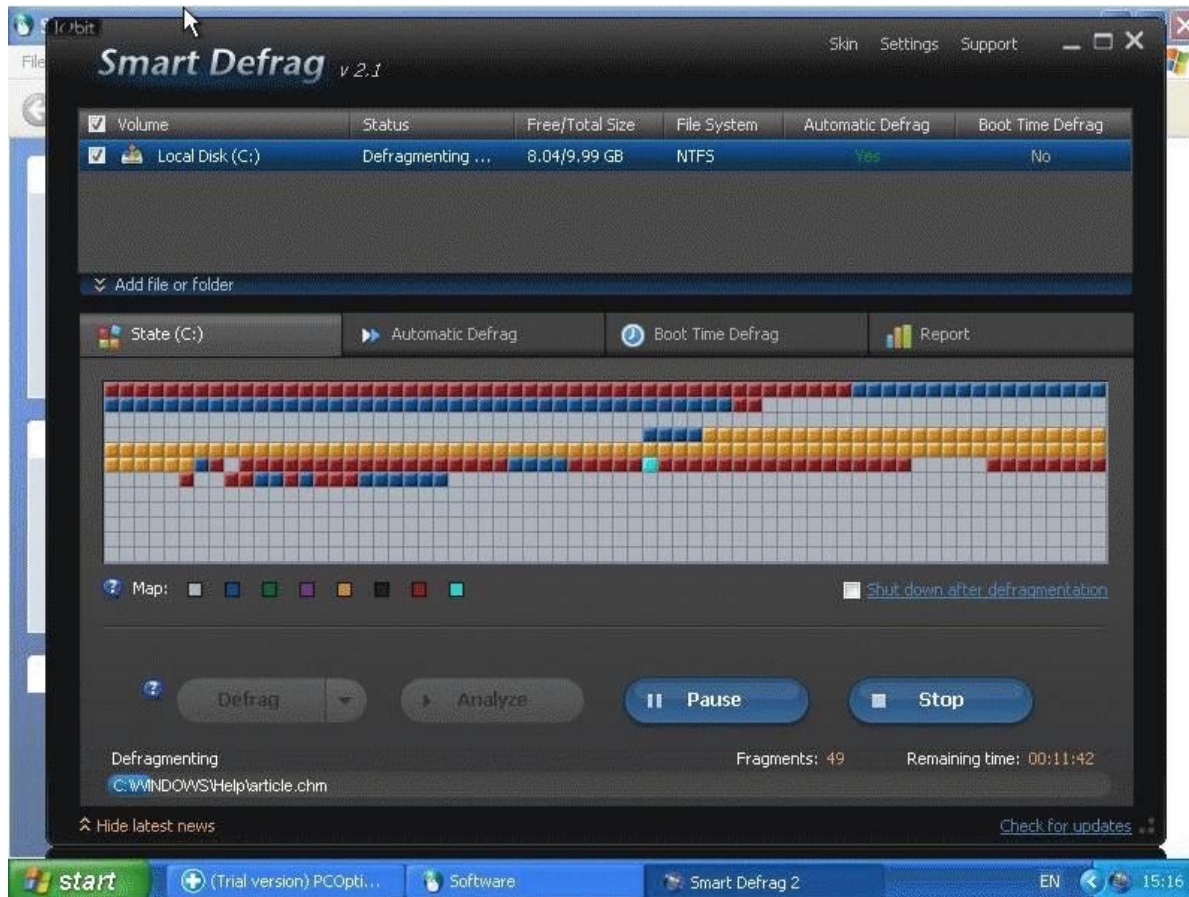
The call ends

...but PC Optimizers' cleaning service doesn't!

Fixing some issues



Tidying up the hard drive



A \$109 gift?



So we're clean, right?



Wrap-up (sorry!)



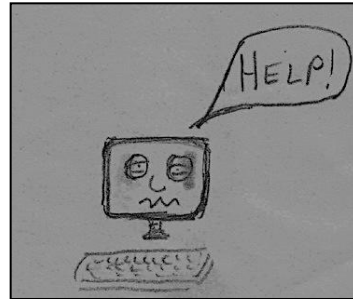
Advice to the public



Not a technical attack.

- Very effective social engineering.**
- Is education & reverse victimology the answer?**
- Limited success with raising general awareness.**
- Many victims don't realise they have been scammed.**

Can't The Authorities Do Something?



Cross border crime.

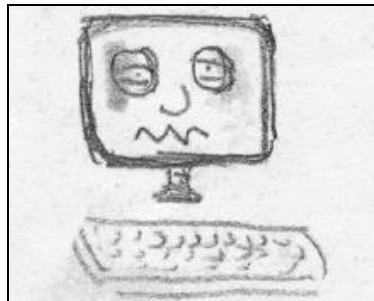
Do not call registers are relatively ineffective.

Cross border law enforcement collaboration is difficult.

Large numbers of victims with small losses.

Difficult to gain focus from law enforcement.

How Can We Trap These Scammers?



Act dumb & play along.

Recorded, transcribed & summarised conversations.

Allow remote access on disposable systems.

Any information gleaned may be passed on.

More reporting of incidents may help gain more attention.

What Can People Do To Protect Themselves?

Caller ID

- International Calls
- Number Withheld

Do not call lists:

- Varies from nation to nation.
- Not perfect, but may help.



What Can People Do To Protect Themselves?

Be aware of the scam.

- The **elderly** are targeted.
- Do NOT give remote control to a stranger - ever!
- If in doubt, see a trusted local.



Be aware of legitimate calls:

- Australia's iCode.
- Will not offer to fix the system for the user.

What If My System May Be Compromised?

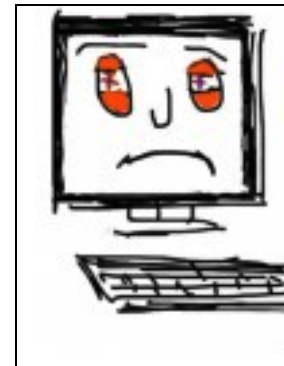
If you realise mid-scam, say so!

If you have already given payment details, demand a refund.

If remote access software is installed, get it removed.

Scan your system for malware.

Get help if needed.



The Bottom Line



Difficult to stop.

No technical solution.

Education & awareness are the best defenses.

Moving target.

Flaky versus Criminal



eFix is one of the leading remote computer support service providers who take care of even the most critical computing problems. We make you aware of **the antivirus present** in your PC **and then deleting them** from it. **We use the best virus softwares** for cleaning up your PC.



Next Steps



Q&A/Exeunt Omnes

- Further contact and resources:
 - david.harley@eset.com
 - sburn@malwarebytes.org
 - martijn.grooten@virusbtn.com
 - http://avien.net/blog/?page_id=790
 - <http://go.eset.com/us/resources/white-papers/Hanging-On-The-Telephone.pdf>,
 - <http://www.virusbtn.com/virusbulletin/archive/2011/01/vb201101-hello>
 - <http://blog.eset.com/2012/04/18/how-to-recognize-a-pc-support-scam>