Malwarebytes

Crushes malware. Restores confidence.

Tech Support Scams 2.0:

An inside look into the evolution of the classic Microsoft tech support scam

Virus Bulletin 2014, Seattle

About @jeromesegura

- Senior security researcher at Malwarebytes
- Primarily work on honeypots, exploits
- But also investigate scams, especially Tech Support Scams
- Attended VB2008 and VB2009
- Born in France, live in Canada

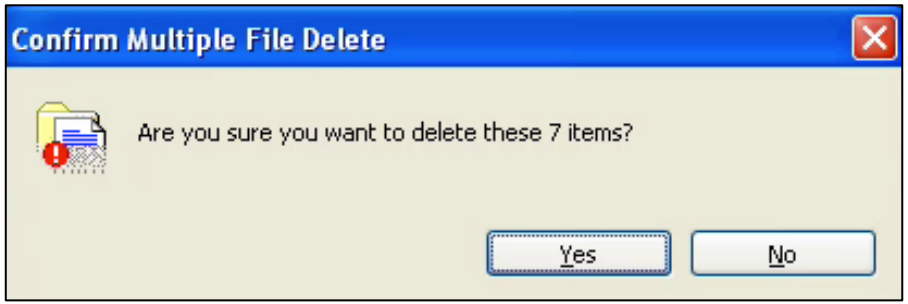
Agenda

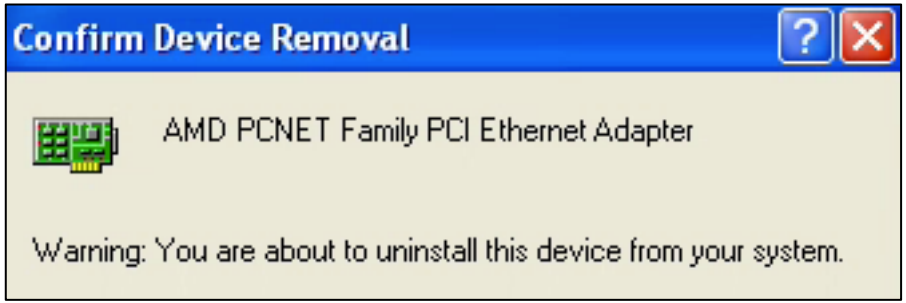
- How I got interested in Tech Support scams
- A brief history: From cold calls to Toll-free numbers
- Not just Windows and India: Mac, Android and the US
- Themed scams: Targeted and aggressive
- Intelligence gathering: Tracking and reporting
- Resources: The fight continues!

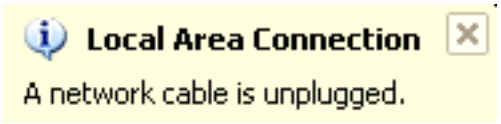
Scammers call the wrong guy

- I received my first tech support scam call April ’13
- The so-called ‘Microsoft’ technician logged in remotely
- Showed me ‘viruses’ on a clean system (VM)
- Demanded money to fix the problem
- I played along but refused to pay
- Things got nasty…

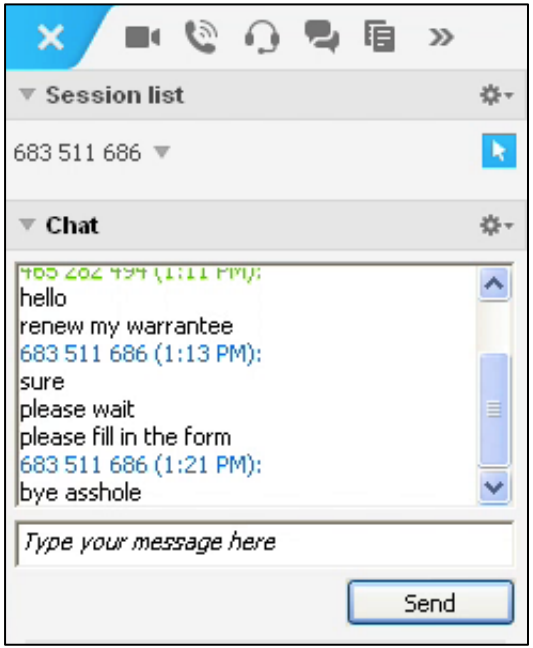
Technician trashed my Virtual Machine

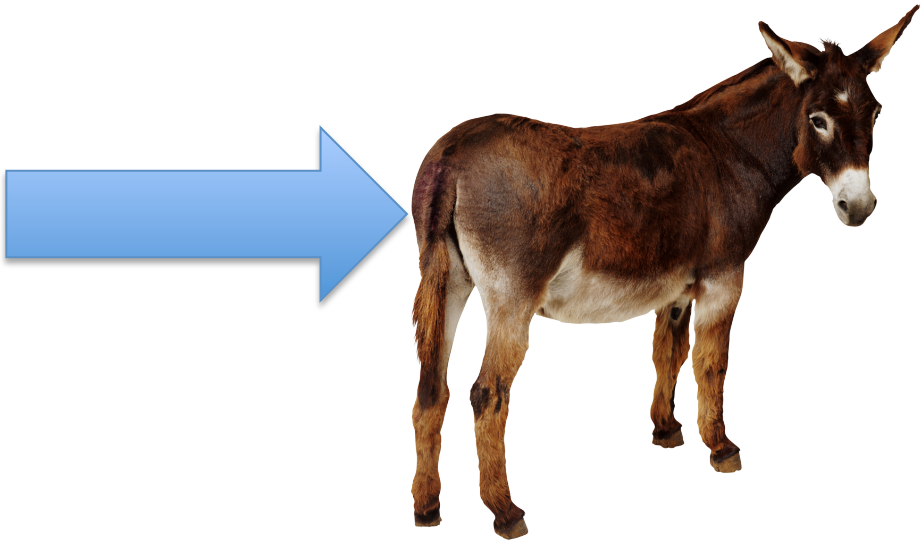






‘Technician’ called me an ***hole





Thousands of victims every day!

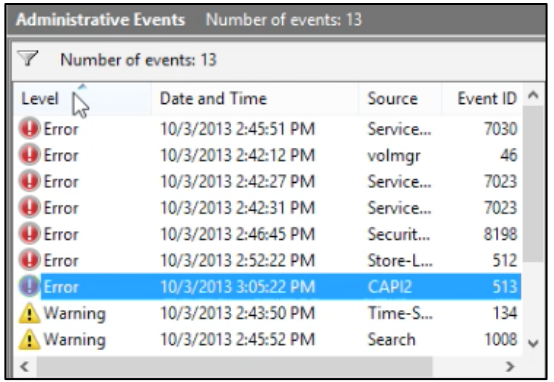
“Ended up being charged $600.00 dollars and now they are taking an extra $19.97 out of my account a month. Want to get my money back.”

“OMG I am idiot! I fell for this only thing was I got a pop up and it told me to call them.”

“I am not sure at this point that if there were even the viruses and if I paid for nothing. My concern now is that he didn't put anything in my PC when he had remote access.”

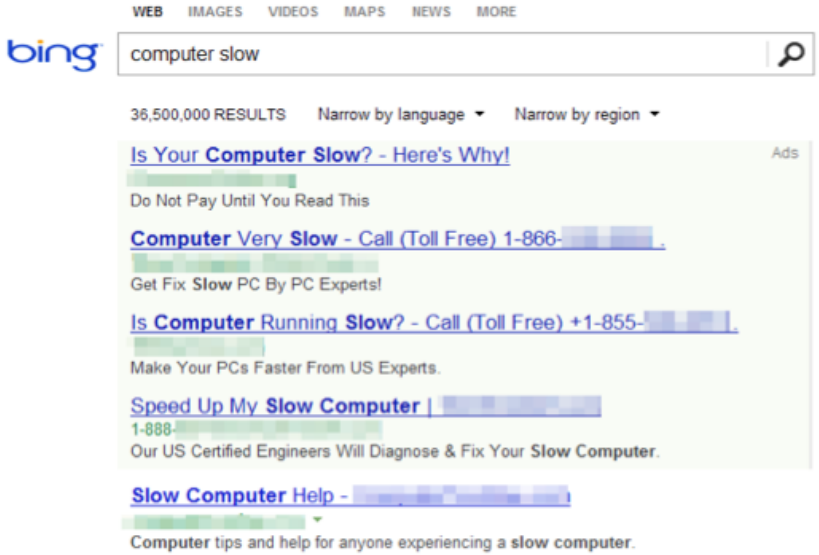
A brief history: cold calls

- Impersonate Microsoft or ‘Windows’
- Mainly originate from India
- Scare tactics to remotely login
- Identify fake errors and viruses
- Payment required to fix the ‘issues’
- Ongoing since at least 2008



A brief history: Toll-free numbers (TFN)

- AKA ‘Premium Tech Support’
- Get in front of the mark
- Sponsored ads, pop-ups
- Upsell from registry cleaners
- Well rehearsed sales pitch
- Highly profitable



Cold calls Vs Toll-free #: Recap

	Cold calls	Toll-free numbers
Advertising costs	-	High
Average Order Value (AOV)	$200	$300
Conversion rate	Low	High
Country of origin	India	India, US

Not just Windows and India

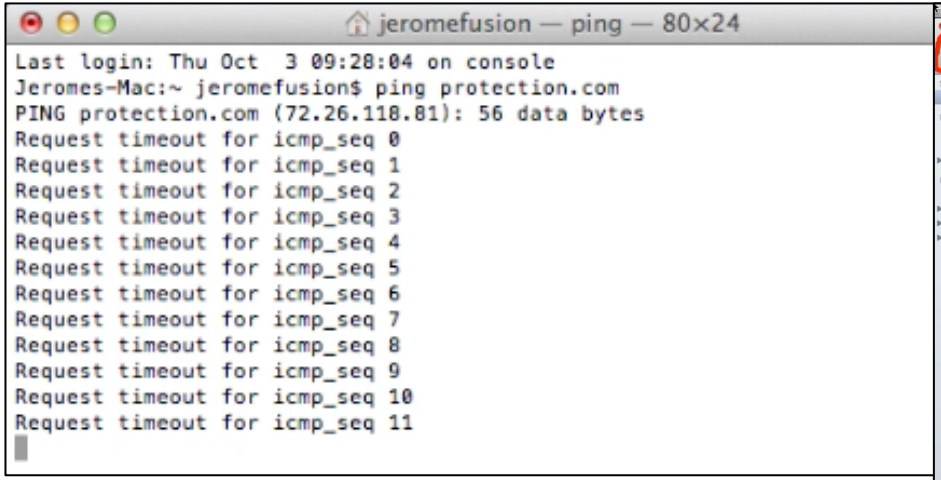
- Mac and Android users targeted
- Rapid growth in the US

US-Based Technicians

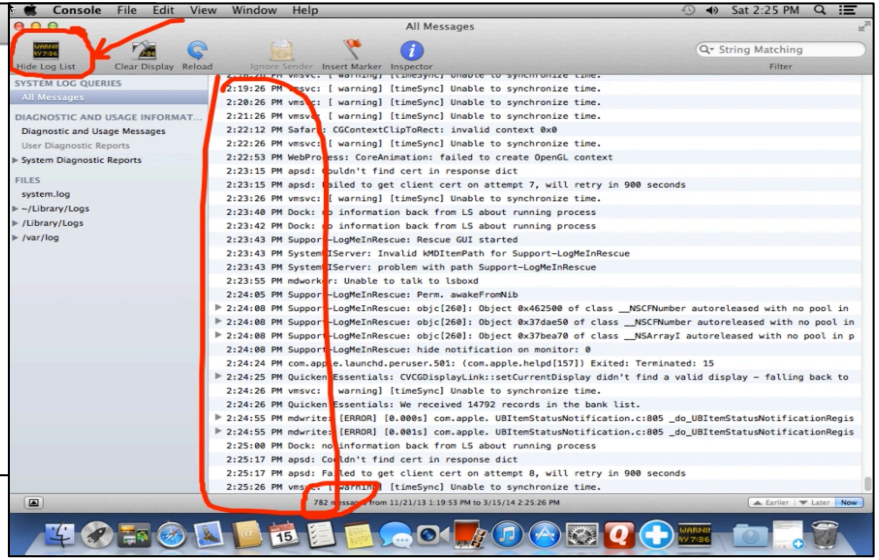
No Outsourcing

Mac users: finding issues is easy

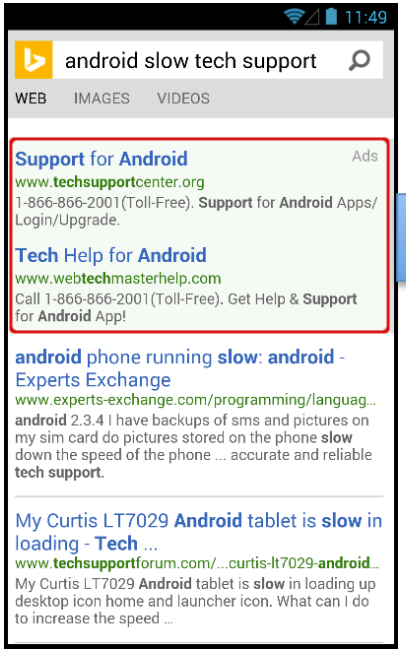
Pinging protection.com to test for AV



Mac Console == Event Viewer

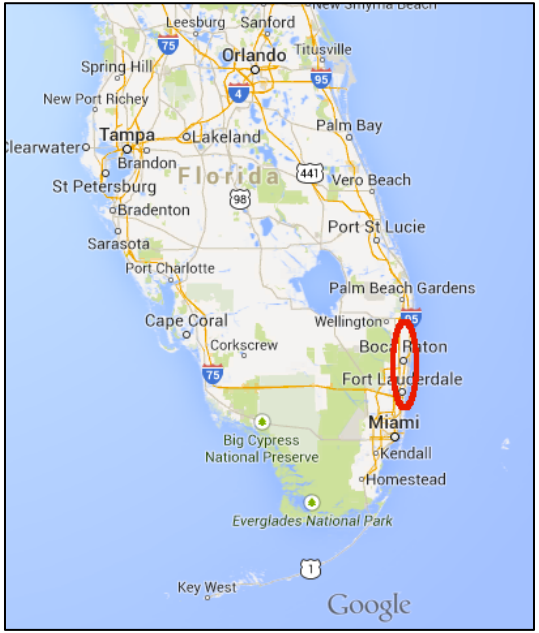


Android users: empty promises

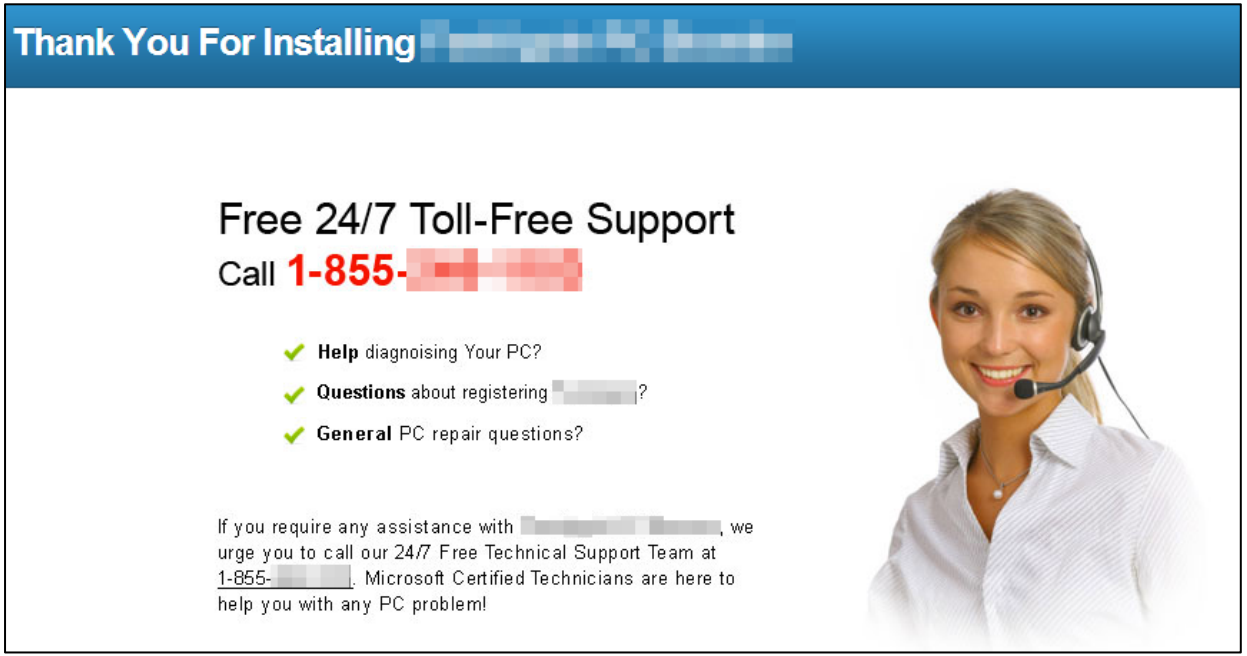


US-Based Scams

- Toll Free Numbers driven
- Same tactics as Indian counterparts
- More expensive packages
- Better after-sale support
- Multi-million dollar industry
- Many located in South East Florida



Upsell path: sneaky ways to make $$

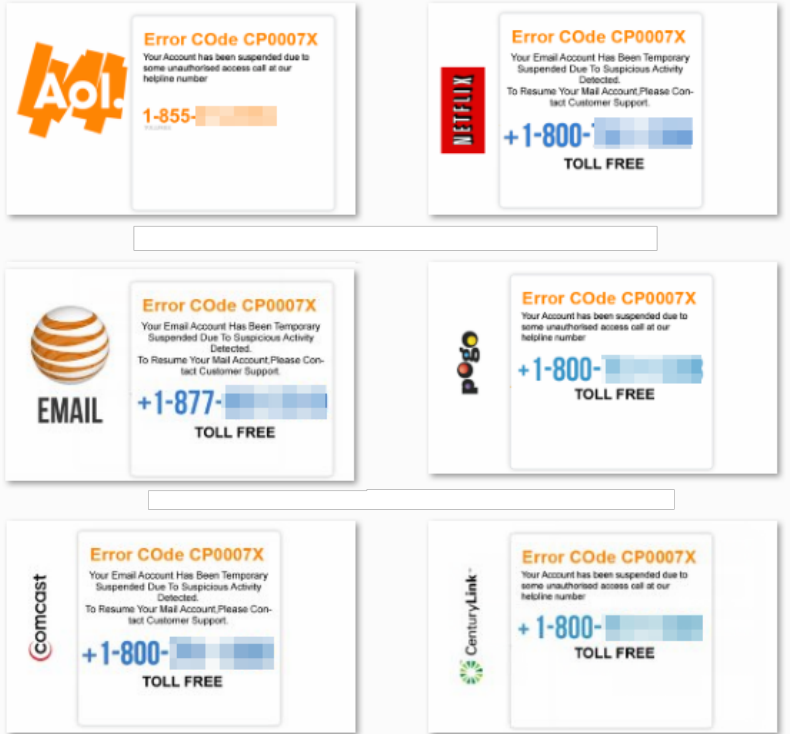


$399.99

$29.99

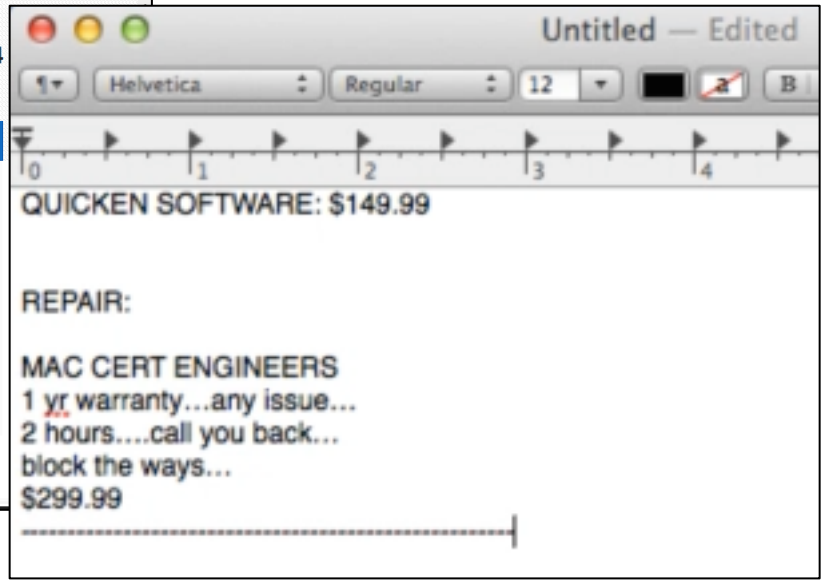
Themed scams

- Leverage popular brands
- Location and time sensitive
- Effective because targeted
- Combined with malware and even phishing
- Full-fledged cyber-criminals



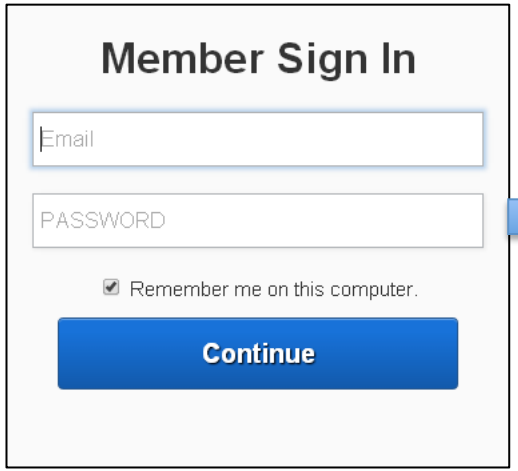
Tax season


http://www.digital-accountants.com/
QuickBooks Support, Quic...
intuit
Certified ProAdvisor
QuickBooks
DIGITAL ACCOUNTANTS
TOLL FREE : 1-855-481-5334
Home
About Us
Services
Support Plans
Contact Us
Support for PeachTree® / Sage50®
Support for QuickBooks®
Book-keeping
Financial Statement
End of Month Closing
Reconciliation
Payroll Processing
W-2, 1099s
Quarterly payroll tax reporting
Accounting Support services by Digital-Accountants
We offer a complete gamut of services circled around your accounting needs. Right from bookkeeping outsourcing
Now Chatting
softwares like


Untitled — Edited
Helvetica
Regular
12
B
QUICKEN SOFTWARE: $149.99
REPAIR:
MAC CERT ENGINEERS
1 yr warranty...any issue...
2 hours....call you back...
block the ways...
$299.99

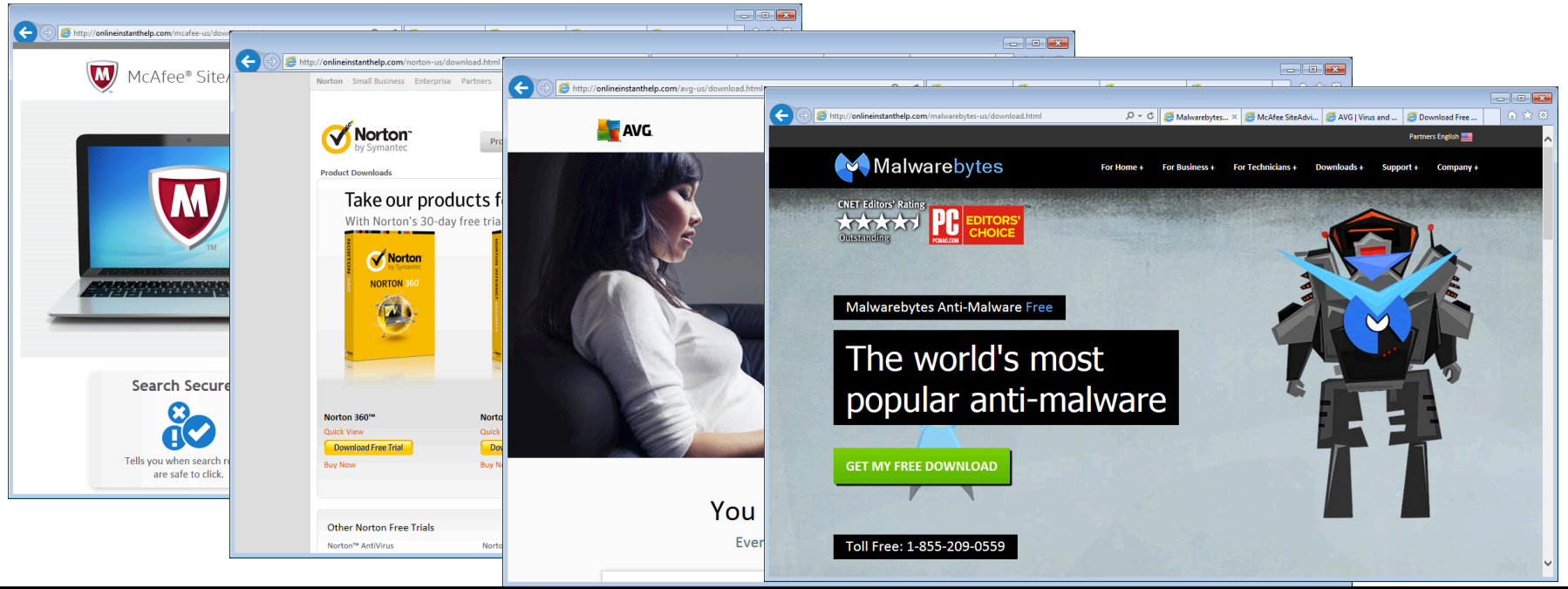
Fake infection pop ups

Phishing

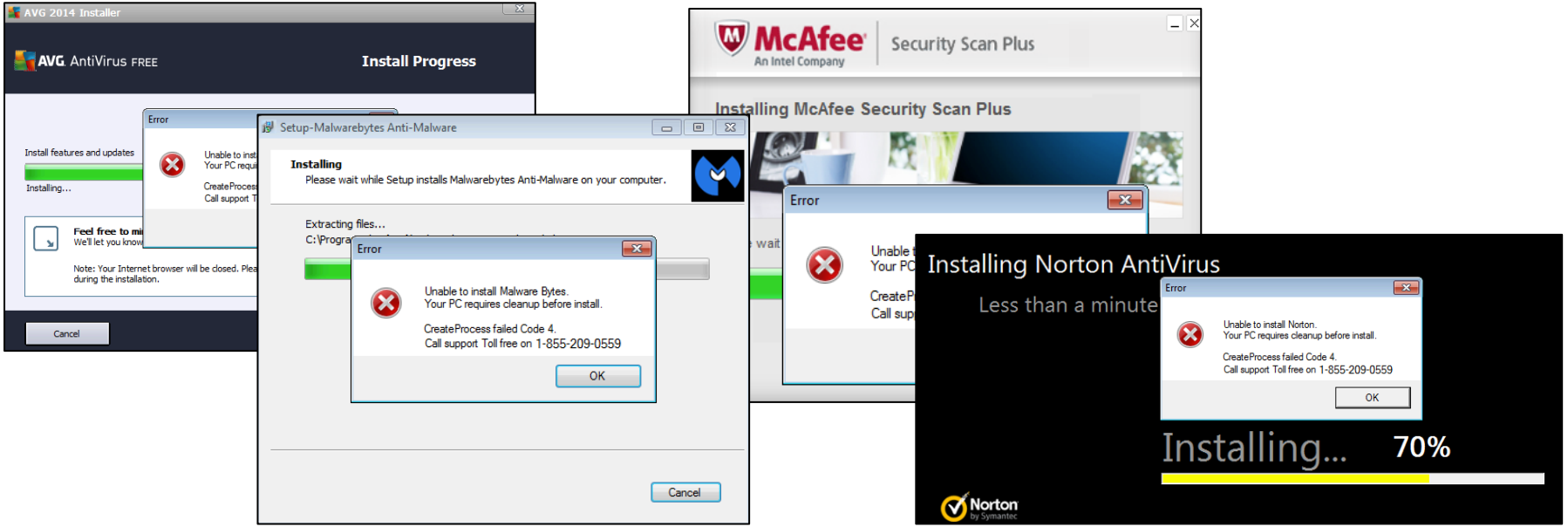

Member Sign In
Email
PASSWORD
Remember me on this computer.
Continue


Account Suspended
netflix.afta3.com/error.html
NETFLIX
Important Notice
We have detected unusual activity on this account. To Protect your account from unauthorized use, we have temporarily suspended this username.
To regain access to your account please contact Member Services at 1-800-947-6570
Error Code : ERR19902881811

Fake sites


McAfee® Site
Search Secure
Tells you when search r
are safe to click.
Norton
by Symantec
Product Downloads
Take our products f
With Norton's 30-day free tria
Norton 360™
Quick View
Download Free Trial
Buy Now
Other Norton Free Trials
Norton™ AntiVirus
AVG
You
Malwarebytes
For Home +
For Business +
For Technicians +
Downloads +
Support +
Company +
CNET Editors' Rating
Outstanding
PC EDITORS' CHOICE
Malwarebytes Anti-Malware Free
The world's most popular anti-malware
GET MY FREE DOWNLOAD
Toll Free: 1-855-209-0559

Fake installers



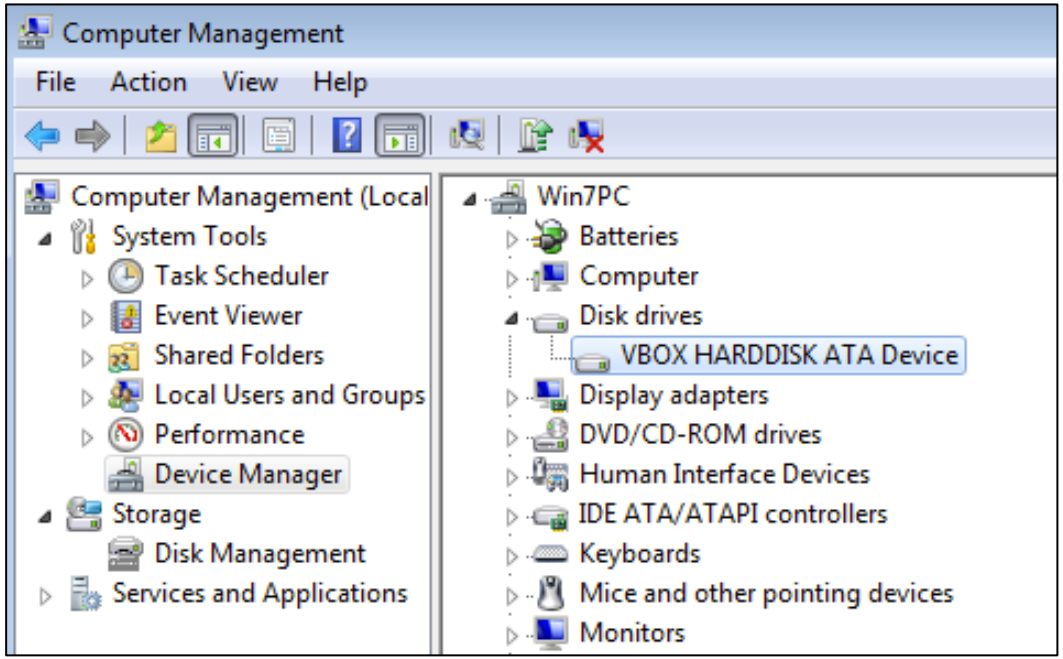
Intelligence gathering: first things first

- Prepare your environment (software, hardware + physical)
- Create a persona (name, email, location, etc)
- Use disposable phone numbers
- Use audio/video recording software to capture evidence
- Give yourself at least ½ hour
- Leave the call on good terms (find an excuse)

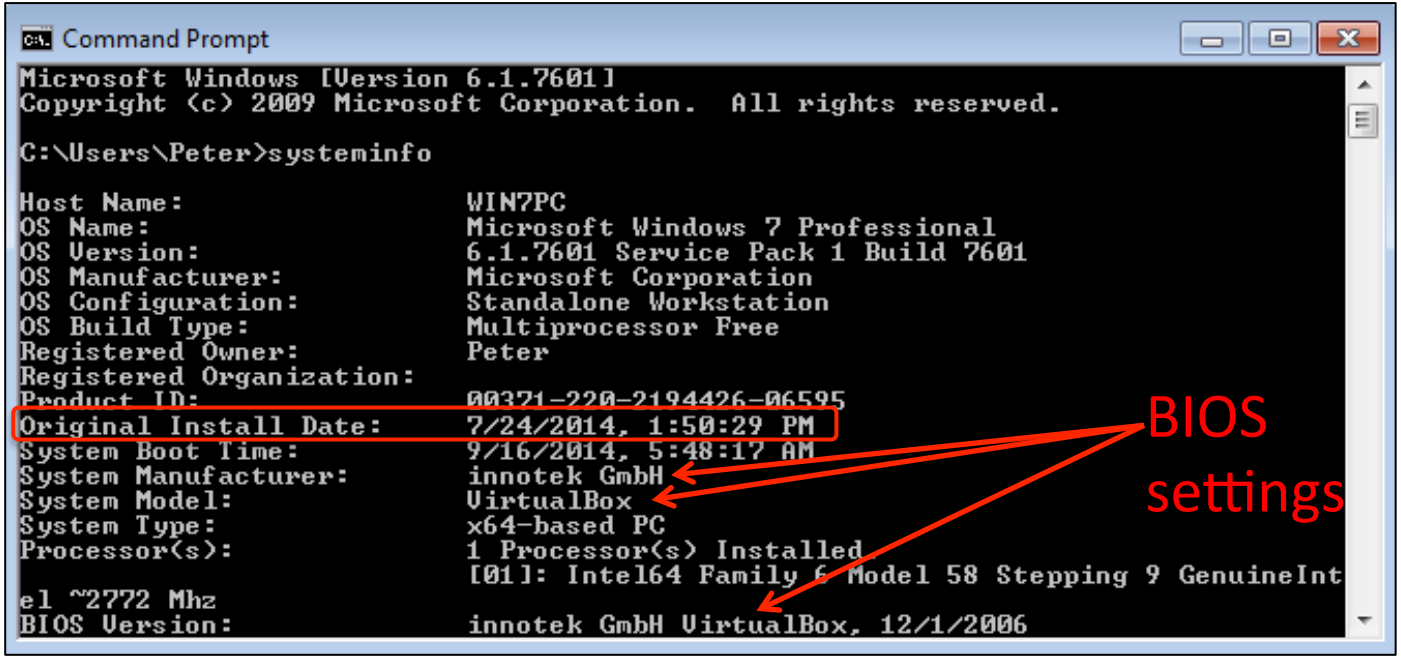
Build a legitimate looking environment

- Windows 7 or 8
- Install updates, activate Firewall
- Make sure the PC looks used (browser history, etc)
- The PC must be free of viruses, malware, adware…
- Assume the machine will be compromised
- Use a VPN on your host to disguise your real location

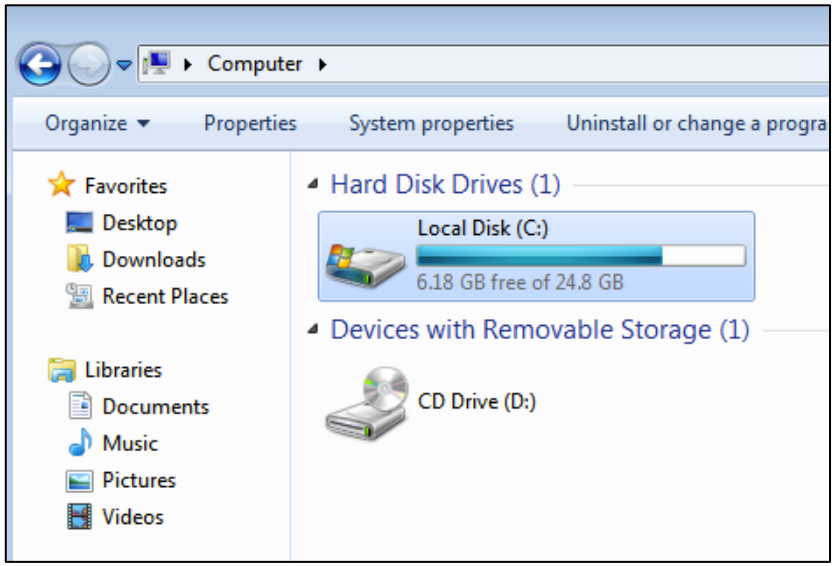
VM detection: remove VBOX, Vmware tools

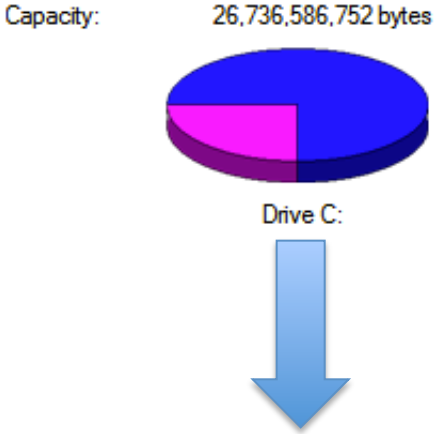


OS install date: the older the better



Hard drive: size matters





Too small for a ‘typical’ machine

Bait documents

TeamViewer - File Transfer Eventlog

```
1:12:28 PM  - Server started successfully
1:12:28 PM  - File transfer request from 894 771 345 allowed
1:12:28 PM  - Views folder <root drives>
1:12:42 PM  - Views folder C:\Users\user\Desktop\
1:12:45 PM  - Processing file transfer...
1:12:45 PM  - Write file C:\Users\user\Desktop\Foreign IP Tracer v 9.0112.bat
1:12:46 PM  - File transfer finished.
1:12:46 PM  - Views folder C:\Users\user\Desktop\
1:13:13 PM  - Processing file transfer...
1:13:13 PM  - Send file C:\Users\user\Desktop\banking 2013.doc
1:13:13 PM  - File transfer finished.
```

Harvest the data

- Save the video recording for evidence
- Save the TeamViewer or LogMeIn ID
- Save the scammer's IP address
- Identify the payment processor
- Report to appropriate people/orgs

Bait calls home

Buzz: tech_support_scams

IP Address	Document	City	Region	Country	Latitude	Longitude
[redacted]	xls	Delhi	07	IN	[redacted]	[redacted]
	xls	Delhi	07	IN		
	doc	Delhi	07	IN		
	xls	Delhi	07	IN		
	xls	Delhi	07	IN		
	xls	Delhi	07	IN		
	xls	Delhi	07	IN		
	xls	Delhi	07	IN		

Honeydocs: https://www.honeydocs.com/

Gmail activity (reverse social-eng.)

Recent activity:

Access Type [?] (Browser, mobile, POP3, etc.)	**Location (IP address) [?]**	**Date/Time** (Displayed in your time zone)
Browser (Chrome) Show details	* [redacted]	11:41 am (1 minute ago)
Browser (Chrome) Show details	[redacted]	11:35 am (7 minutes ago)
Browser (Chrome) Hide details *"Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36,gzip(gfe),gzip(gfe)"*	India ([redacted])	11:34 am (8 minutes ago)
Browser (Chrome) Show details	India ([redacted])	[redacted] (18 hours ago)
Browser (Chrome) Show details	India ([redacted])	[redacted] (18 hours ago)

Log review 

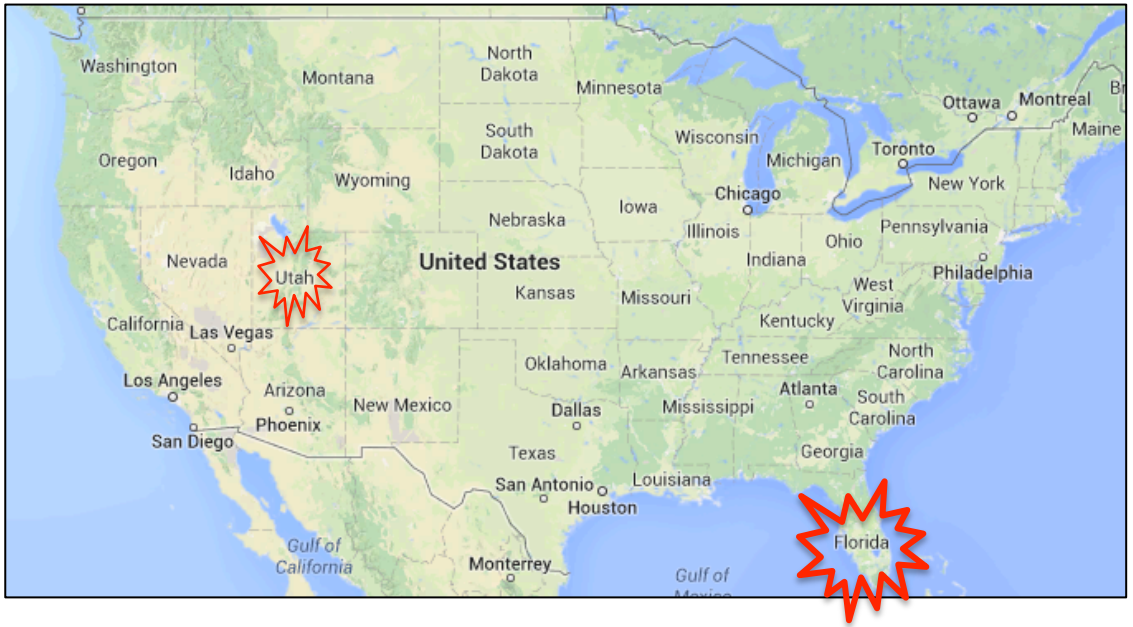
TeamViewer:

```
1128  3920 S0   CT12 GWT.SendUDPPunchRequest 4
1128  3920 S0   CT12 GWT.CmdUDPPing.PunchReceived, a=[redacted], p=16874
```

LogMeIn:

```
- Rescue   - Socket - [redacted]:42307/rawssl - SSL shut down - socket stays connected
- Rescue   - Socket - [redacted]:42307/rawssl - SSL handshake started.
- Rescue   - Socket - [redacted]:42307/rawssl - SSL handshake done.
- Rescue   - Socket - [redacted]:42307/rawssl - SSL cipher AES256-SHA (256 bits) TLSv1/SSLv3 selected.
- Rescue   - Socket - [redacted]:42307/rawssl - SSL session: REUSED, timeout is 600 seconds
- Rescue   - Socket - [redacted]:42307/rawssl - Takeover Connection ID: 74577
```

Geolocation: India / USA



Resources: blog.malwarebytes.org

Malwarebytes UNPACKED

Home Authors Videos Scams

Tech Support Scams – Help & Resource Page

OCTOBER 4, 2013 | BY JÉRÔME SEGURA

> *Hello, we are calling from Windows and your computer looks like it is infected. Our Microsoft Certified Technician can fix it for you.*

Sound familiar? Whether you have just been scammed or simply want to find out more on the topic, you have come to the right place.

Tech support scams are a million-dollar industry and have been around since 2008. Every single day, innocent people are tricked into spending hundreds of dollars on non-existent computer problems.

There is no sign of these scams slowing down despite several actions taken by the Federal Trade Commission.

TABLE OF CONTENTS

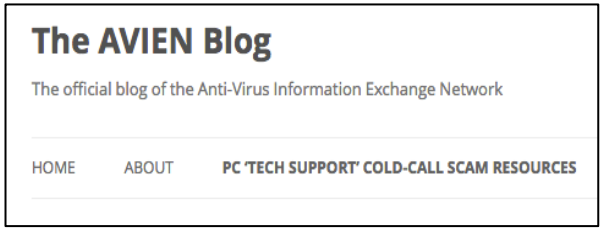
Tech Support Scams Blacklist: Criteria

1. Pretends to be working for Microsoft or ‘Windows’
2. Uses misleading tactics to force a sale
3. Finds viruses, malware or an infection on a perfectly clean system
4. Validates a fraudulent popup or page as legitimate

Tech Support Scams Blacklist: Example

Company name and aliases: **E-Racer Tech (Clean IT PC)**
Website(s): e-racertech.com, cleanitpc.com
Phone number(s): 1-855-486-1800, 1-877-648-7339
Affiliate(s): error711971669.com
Remote control software: LogMeIn: 432039
Payment processor: N/A
Reason for blacklisting: #2, #4
Incident date: 05/28/2014
Incident ID: 0000028

Other resources



Thank You!
Questions?

#TechSupportScams