



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

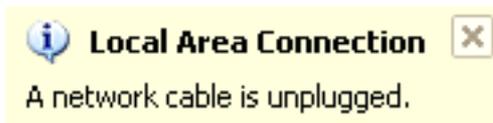
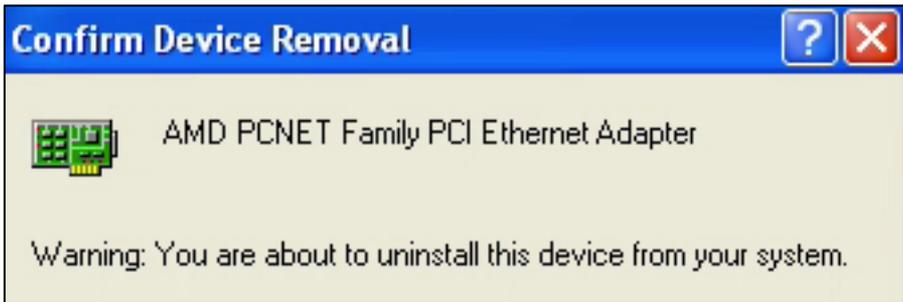
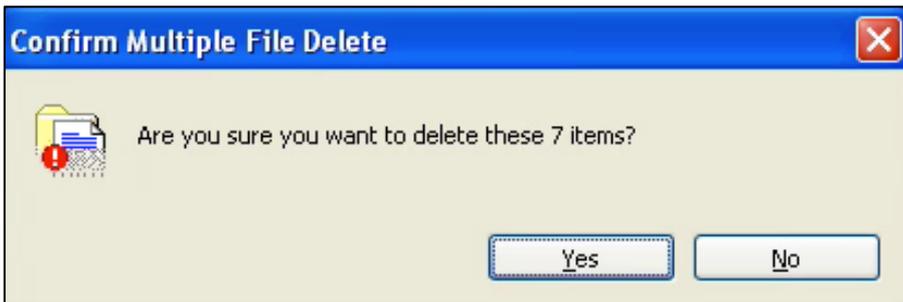
- How I got interested in Tech Support scams
- A brief history: From cold calls to Toll-free numbers
- Not just Windows and India: Mac, Android and the US
- Themed scams: Targeted and aggressive
- Intelligence gathering: Tracking and reporting
- Resources: The fight continues!



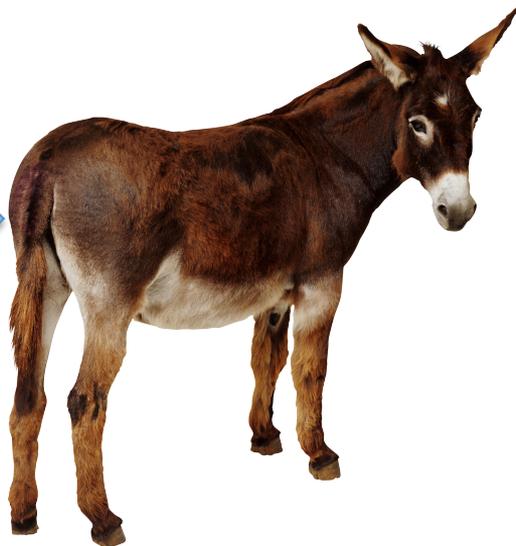
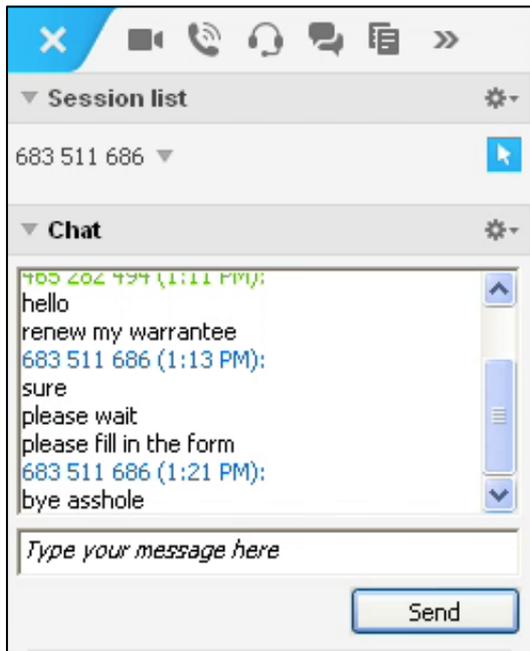
Scammers call the wrong guy

- 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!

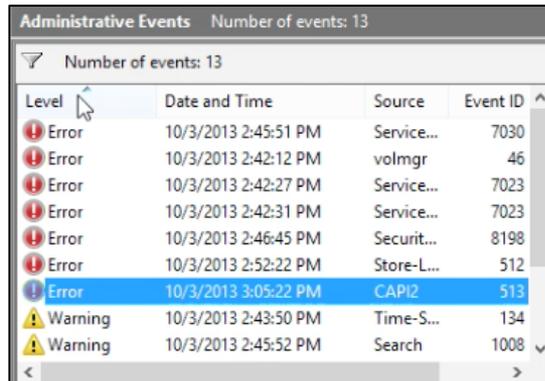
“Ended up being charged \$600.00 dollars and now they are taking an extra \$19.97 out of my account a month. Want to get my money back.”

“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



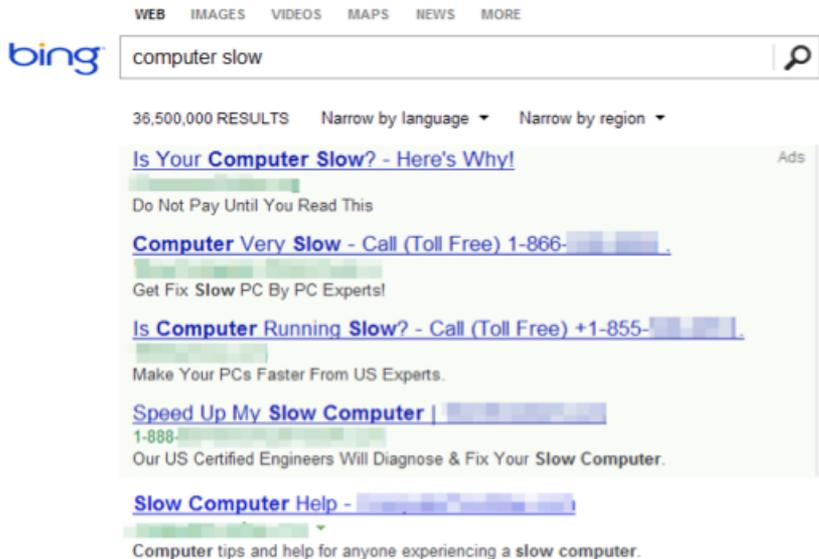
Administrative Events Number of events: 13

Number of events: 13

Level	Date and Time	Source	Event ID
Error	10/3/2013 2:45:51 PM	Service...	7030
Error	10/3/2013 2:42:12 PM	volmgr	46
Error	10/3/2013 2:42:27 PM	Service...	7023
Error	10/3/2013 2:42:31 PM	Service...	7023
Error	10/3/2013 2:46:45 PM	Securit...	8198
Error	10/3/2013 2:52:22 PM	Store-L...	512
Error	10/3/2013 3:05:22 PM	CAPI2	513
Warning	10/3/2013 2:43:50 PM	Time-S...	134
Warning	10/3/2013 2:45:52 PM	Search	1008

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



WEB IMAGES VIDEOS MAPS NEWS MORE

bing computer slow

36,500,000 RESULTS Narrow by language Narrow by region

Is Your Computer Slow? - Here's Why! Ads
Do Not Pay Until You Read This

Computer Very Slow - Call (Toll Free) 1-866-...
Get Fix Slow PC By PC Experts!

Is Computer Running Slow? - Call (Toll Free) +1-855-...
Make Your PCs Faster From US Experts.

Speed Up My Slow Computer | ...
1-888-...
Our US Certified Engineers Will Diagnose & Fix Your Slow Computer.

Slow Computer Help - ...
Computer tips and help for anyone experiencing a slow computer.

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



 **Apple Support**

Affordable & Effective Tech Support

An elite band of tech support experts offering you technical support services for a whole range of desktops, laptops, etc.

TOLL FREE

1-800-806-0768

Apple Consultants are Online



US-Based Technicians

~~OUTSOURCING~~

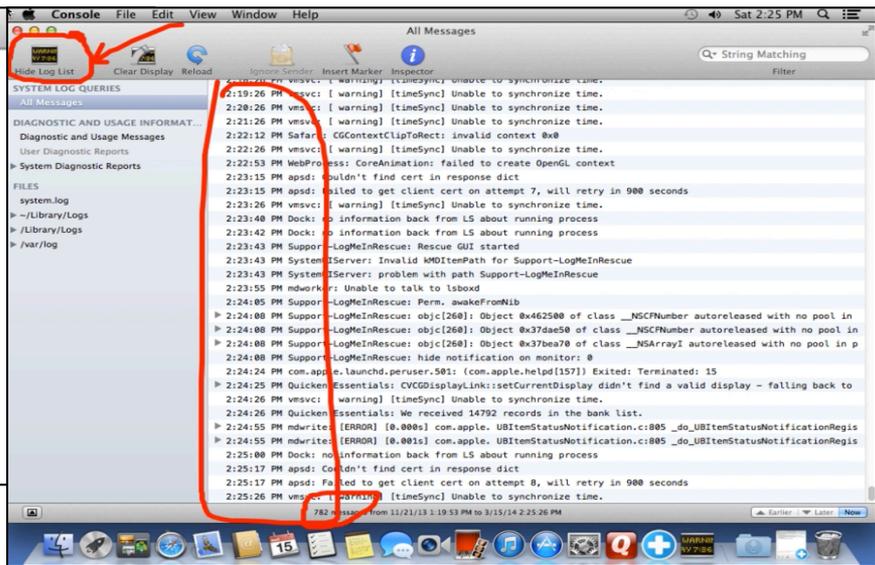
No Outsourcing

Mac users: finding issues is easy

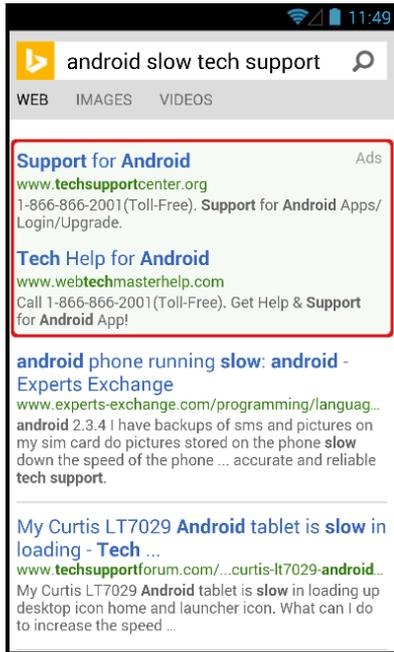
Pinging protection.com to test for AV

```
jeromefusion — ping — 80x24
Last login: Thu Oct 3 09:28:04 on console
Jeromes-Mac:~ jeromefusion$ ping protection.com
PING protection.com (72.26.118.81): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
Request timeout for icmp_seq 6
Request timeout for icmp_seq 7
Request timeout for icmp_seq 8
Request timeout for icmp_seq 9
Request timeout for icmp_seq 10
Request timeout for icmp_seq 11
```

Mac Console == Event Viewer



Android users: empty promises



android slow tech support

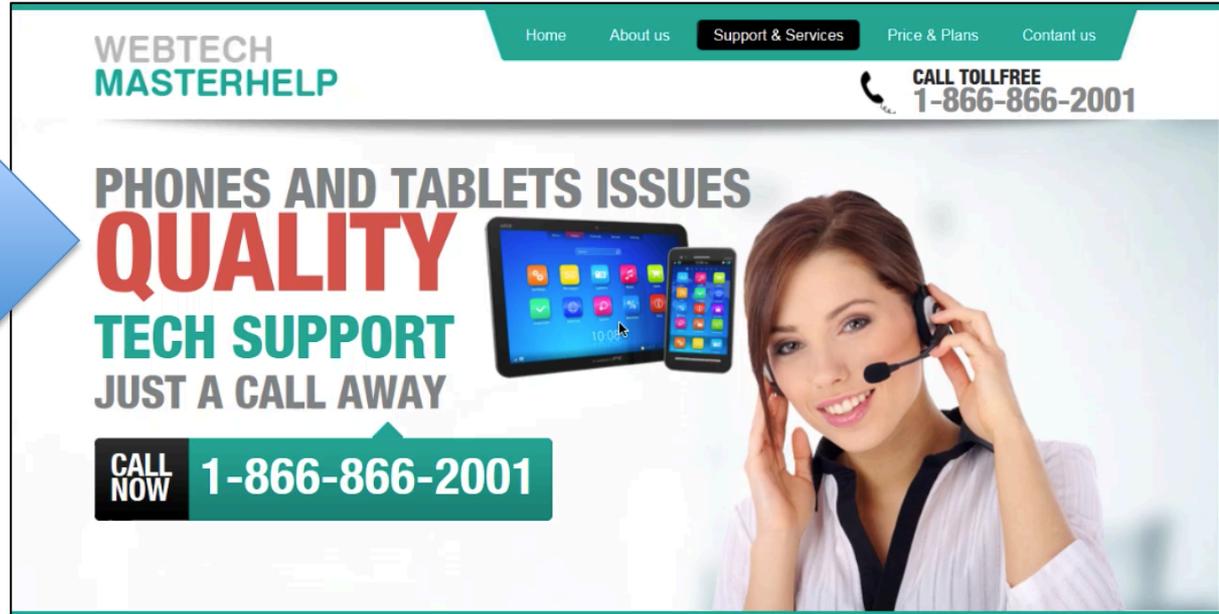
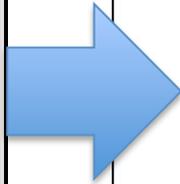
WEB IMAGES VIDEOS

Support for Android Ads
www.techsupportcenter.org
1-866-866-2001 (Toll-Free). Support for Android Apps/ Login/Upgrade.

Tech Help for Android
www.webtechmasterhelp.com
Call 1-866-866-2001 (Toll-Free). Get Help & Support for Android App!

android phone running slow: android - Experts Exchange
www.experts-exchange.com/programming/languag...
android 2.3.4 I have backups of sms and pictures on my sim card do pictures stored on the phone slow down the speed of the phone ... accurate and reliable tech support.

My Curtis LT7029 Android tablet is slow in loading - Tech ...
www.techsupportforum.com/...curtis-lt7029-android...
My Curtis LT7029 Android tablet is slow in loading up desktop icon home and launcher icon. What can I do to increase the speed ...



WEBTECH MASTERHELP

Home About us Support & Services Price & Plans Contact us

CALL TOLLFREE 1-866-866-2001

PHONES AND TABLETS ISSUES

QUALITY

TECH SUPPORT

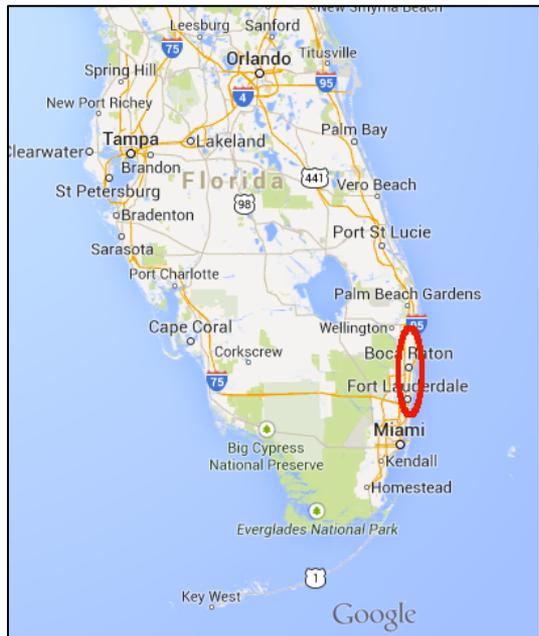
JUST A CALL AWAY

CALL NOW 1-866-866-2001



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 \$\$

Thank You For Installing [REDACTED]

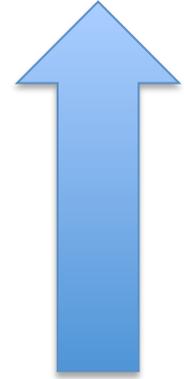
Free 24/7 Toll-Free Support
Call **1-855-**[REDACTED]

- ✓ **Help** diagnosing Your PC?
- ✓ **Questions** about registering [REDACTED]?
- ✓ **General** PC repair questions?

If you require any assistance with [REDACTED], we urge you to call our 24/7 Free Technical Support Team at 1-855-[REDACTED]. Microsoft Certified Technicians are here to help you with any PC problem!



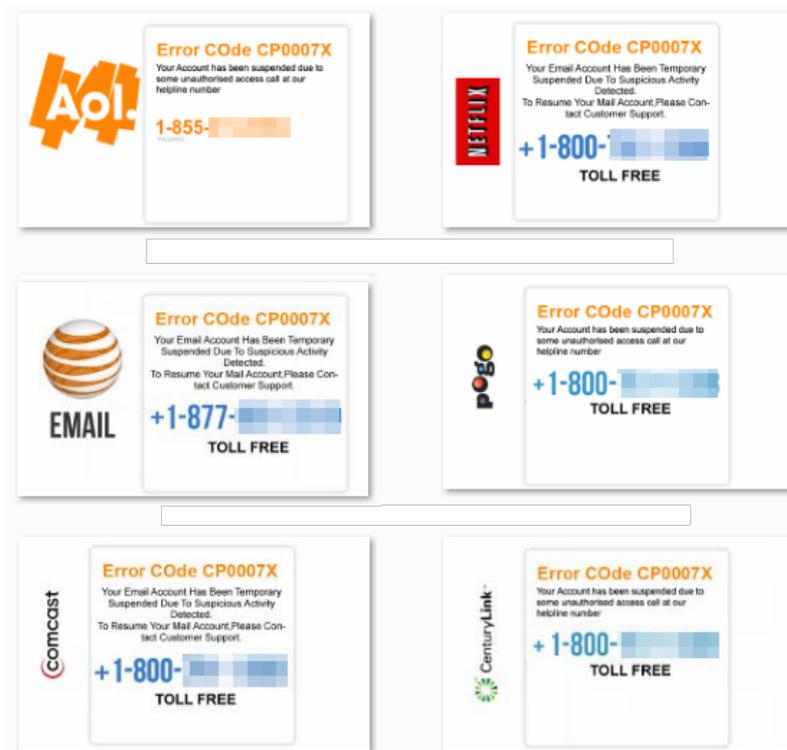
\$399.99



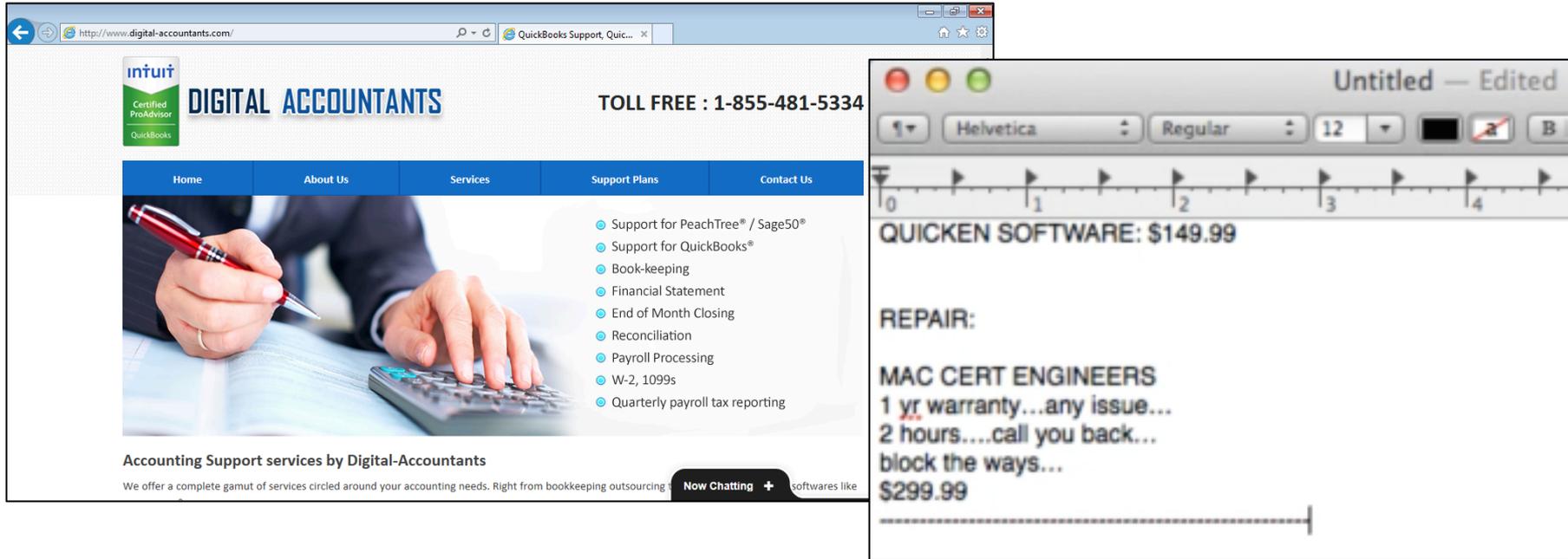
\$29.99

Themed scams

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



Tax season



The image shows a browser window displaying the website for Digital Accountants, an Intuit Certified ProAdvisor. The website features a navigation menu with 'Home', 'About Us', 'Services', 'Support Plans', and 'Contact Us'. A list of services is provided, including support for PeachTree/Sage50, QuickBooks, book-keeping, financial statements, end-of-month closing, reconciliation, payroll processing, W-2/1099s, and quarterly payroll tax reporting. A 'Now Chatting' button is visible at the bottom.

Overlaid on the right side of the browser window is a text document titled 'Untitled - Edited'. The document contains the following text:

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



WARNING!

Your Computer May be Infected:

1(855)-685-4504

For emergency Tech Support call immediately

The system may have found (2) viruses that pose a serious threat
Browser.Hijacker.Spy / Trojan.FakeAV-Download

Your personal and financial information
may not be secured.

Call now for support

1(855)-685-4504



WARNING!

YOUR COMPUTER IS INFECTED?

System Detected (2) Potentially Malicious Viruses: **Rootkit.Sirefef.Spy** and **Trojan.FakeAV-Download**. Your Personal & Financial Information **IS NOT SECURED**.

To Remove Viruses, Call Tech Support Online Now:

1 (855) 889-7378

(High Priority Virus Removal Call Line)

Phishing

Member Sign In

Email

PASSWORD

Remember me on this computer.

Continue



Account Suspended

netflix.afta3.com/error.html

NETFLIX

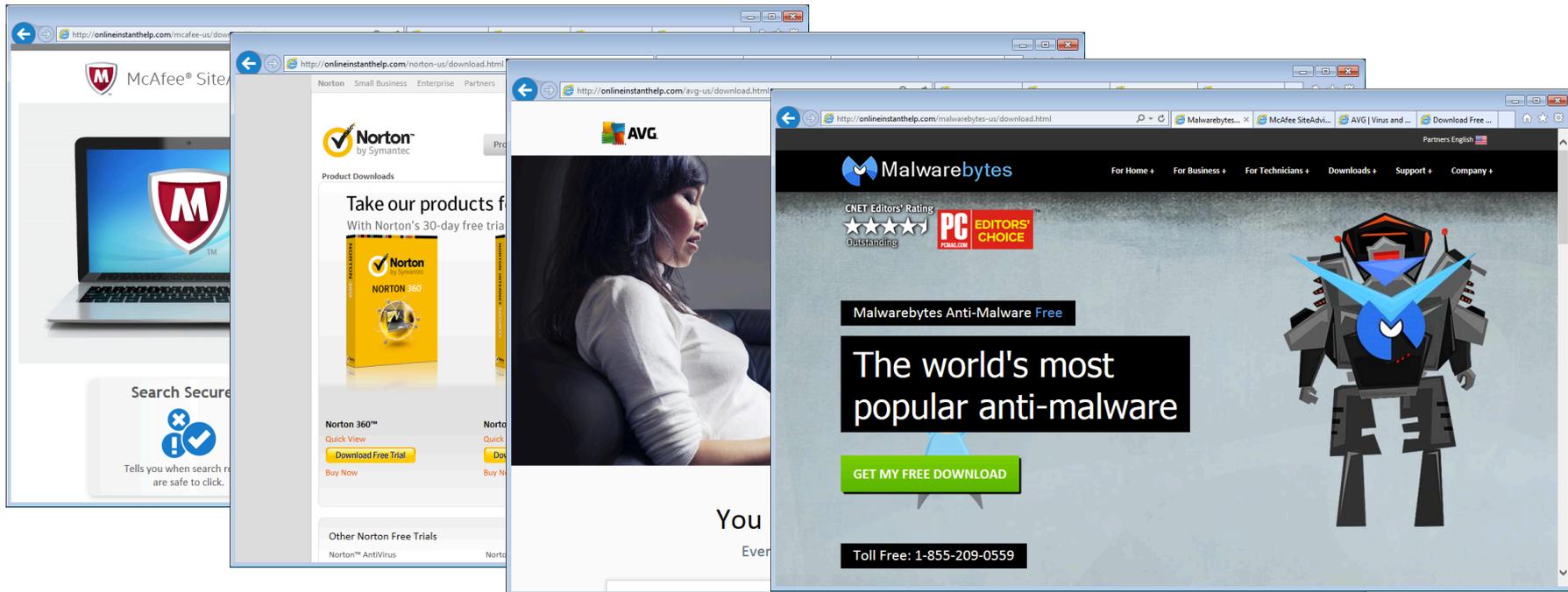
Important Notice

We have detected unusual activity on this account. To Protect your account from unauthorized use, we have temporarily **suspended** this username.

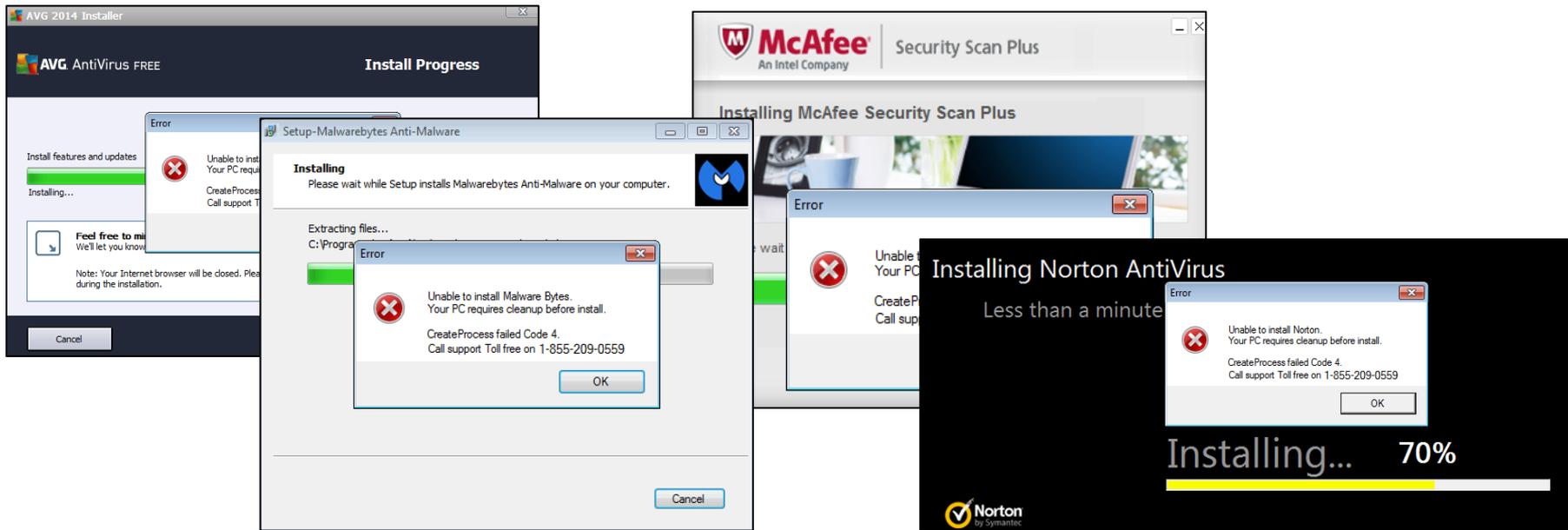
To regain access to your account please contact Member Services at **1-800-947-6570**

Error Code : ERR19902881811

Fake sites



Fake installers



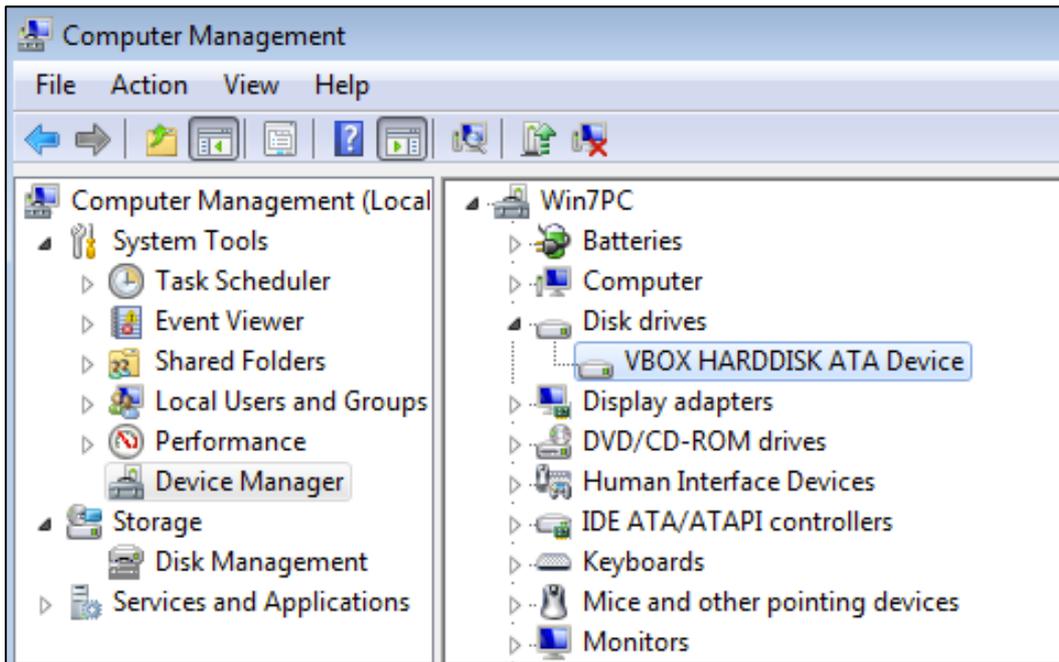
Intelligence gathering: first things first

- 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 1/2 hour
- Leave the call on good terms (find an excuse)

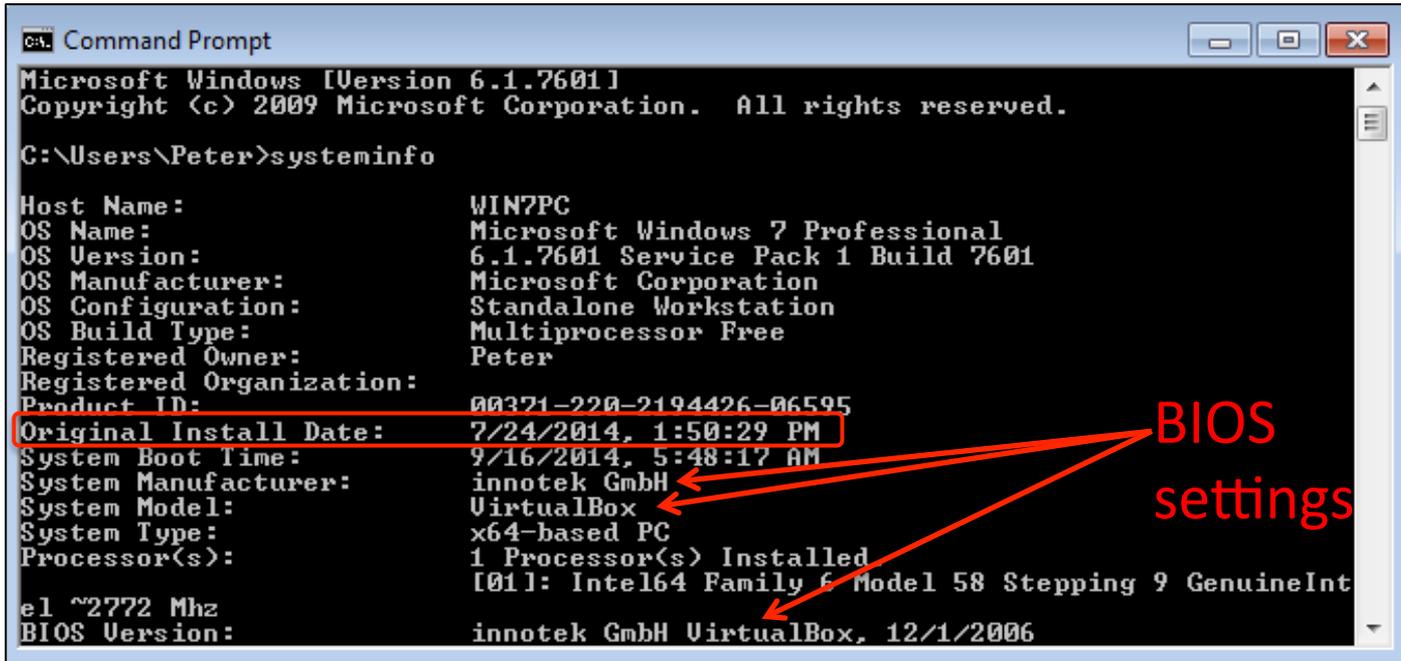
Build a legitimate looking environment

- 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



```
Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

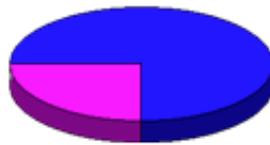
C:\Users\Peter>systeminfo

Host Name:                WIN7PC
OS Name:                  Microsoft Windows 7 Professional
OS Version:               6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:        Microsoft Corporation
OS Configuration:       Standalone Workstation
OS Build Type:            Multiprocessor Free
Registered Owner:        Peter
Registered Organization:
Product ID:                00371-220-2194426-06595
Original Install Date:    7/24/2014, 1:50:29 PM
System Boot Time:         9/16/2014, 5:48:17 AM
System Manufacturer:     innotek GmbH
System Model:              VirtualBox
System Type:              x64-based PC
Processor(s):             1 Processor(s) Installed
                          [01]: Intel64 Family 6 Model 58 Stepping 9 GenuineInt
e1 ~2772 Mhz
BIOS Version:             innotek GmbH VirtualBox, 12/1/2006
```

Hard drive: size matters



Capacity: 26,736,586,752 bytes

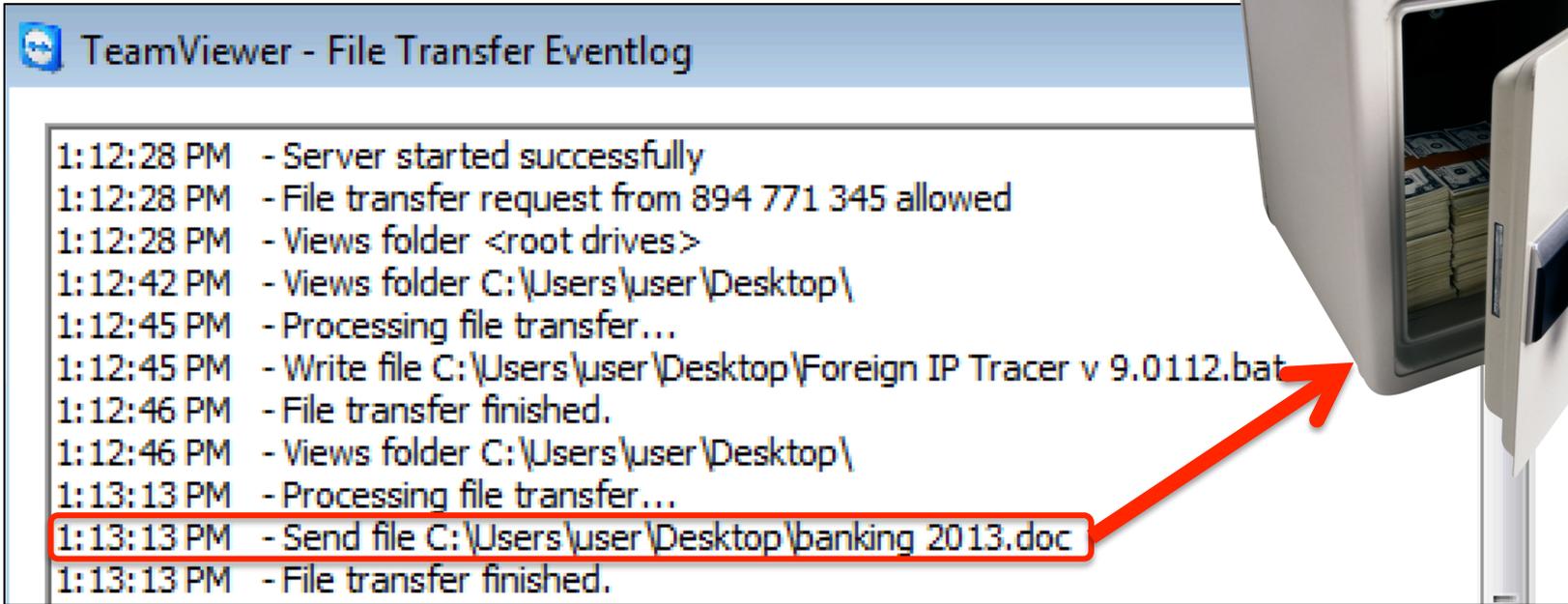


Drive C:



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]
[REDACTED]	xls	Delhi	07	IN	[REDACTED]	[REDACTED]
[REDACTED]	doc	Delhi	07	IN	[REDACTED]	[REDACTED]
[REDACTED]	xls	Delhi	07	IN	[REDACTED]	[REDACTED]
[REDACTED]	xls	Delhi	07	IN	[REDACTED]	[REDACTED]
[REDACTED]	xls	Delhi	07	IN	[REDACTED]	[REDACTED]
[REDACTED]	xls	Delhi	07	IN	[REDACTED]	[REDACTED]
[REDACTED]	xls	Delhi	07	IN	[REDACTED]	[REDACTED]

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



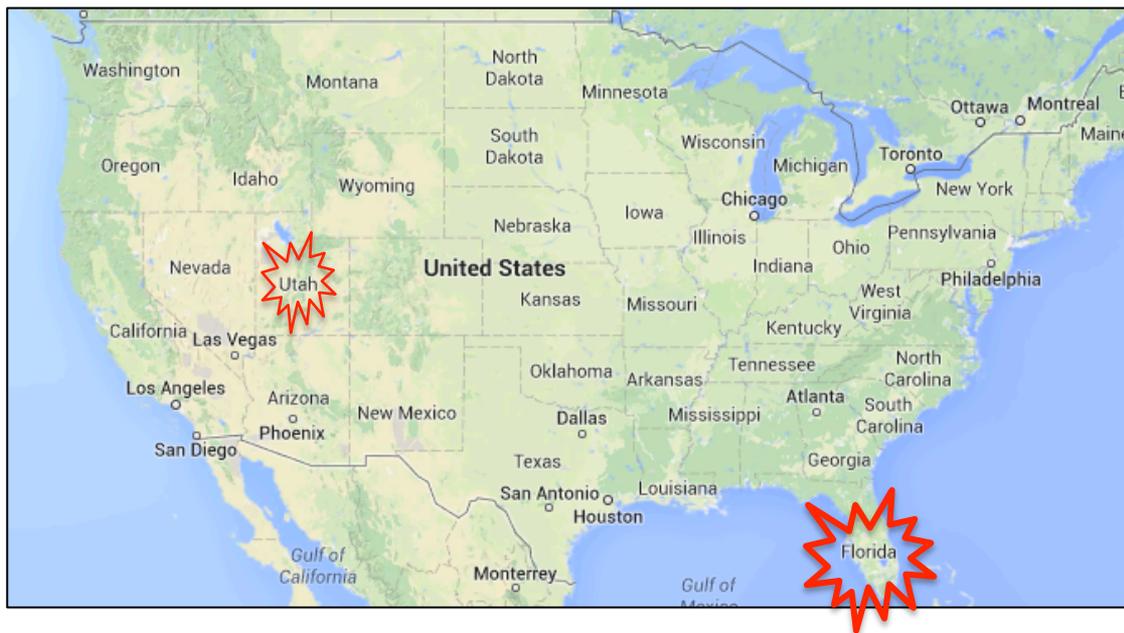
TeamViewer:

```
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

- [How it all begins](#)
- [Remote access](#)
- [Tricks of the trade](#)
- [Getting help \(damage control\)](#)
- [Fighting back](#)
- [Tech Support Blacklist](#)
- [Related articles](#)

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: LogMeln: 432039

Payment processor: N/A

Reason for blacklisting: #2, #4

Incident date: 05/28/2014

Incident ID: 0000028

Other resources



Thank You!

Questions?



[#TechSupportScams](https://twitter.com/hashtag/TechSupportScams)