Hanging on the telephone[1]

Antivirus cold-calling support scams

David Harley
CITP FBCS CISSP
ESET North America Senior Research Fellow

Urban Schrott
IT Security and Cybercrime Analyst
ESET Ireland

Jan Zeleznak
IT Services Manager
ESET Ireland

Table of Contents

Introduction	3
Thank you for your support	4
A view to a scam	5
True or false?	6
Log me in, clean me out	7
Oh! Calcutta!	8
Not everything is Microsoft's fault...	8
Conclusion	9
References	11
Other resources	13

We gratefully acknowledge the help of the following in researching, addressing and publicizing this issue:

- Steve Burn, hpHosts Online
- Andrew Brandt, Webroot
- Sara Claridge, Marylebone Media Relations
- Alan Thake, Paul Brook, Quinton Watts, Charles Jeter, Darin Anderson and Peter Kovac, ESET

Introduction

In June 2010, ESET's David Harley was contacted[2] by Andrew, a researcher working for another security company. Andrew was concerned that a colleague in the UK had come across a highly suspicious and, at best, unethical attempt to sell what was claimed to be ESET antivirus software.

The prospective victim had received an unsolicited phone call, allegedly from Microsoft, informing him that notification had been received concerning a virus infection on his PC, and offering to help him to install antivirus software. When asked what antivirus software was being offered, the caller claimed that it was ESET's.

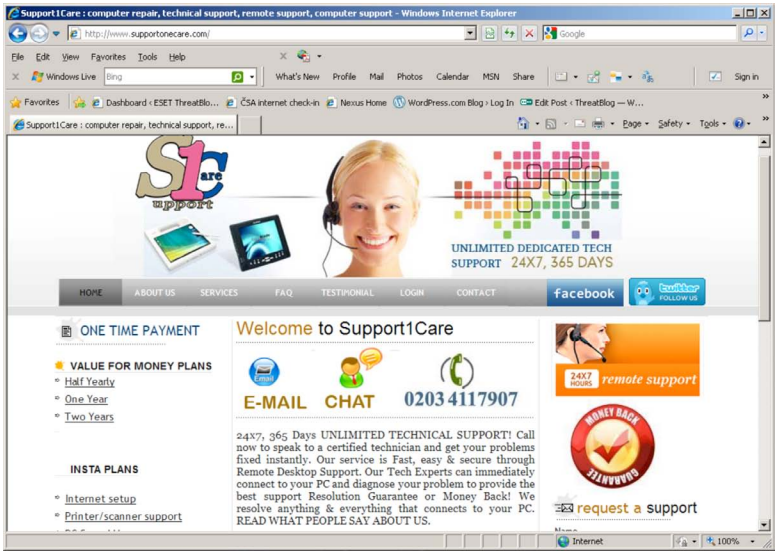
This may sound like an ethically challenged distributor using fraudulent techniques closely resembling those used by distributors of fake AV, but it's not the way that reputable, law-abiding companies like ESET UK and its partners operate. A little research quickly turned up a similar (though not identical) story from PC Pro[3].

ESET UK, however, had come across an almost identical scam, and was able to provide more information. In this instance, the caller claimed to belong to a Microsoft-affiliated organization called "Support One Care" (note the resemblance in the name to a Microsoft product) and had contacted a prospective victim to tell her that:

- her PC was infected,
- her AV was out-of-date, and
- for a one-time fee of £79 (US $127), he would install a better product (yes, it was claimed to be ESET's) and give her a year's support.

He gave her a number to call back, which appears to be in the UK, but reroutes to India. The number is indeed listed on the site belonging to a company based in India, which claims to be a Microsoft-registered partner, that offers various support plans.

When ESET UK contacted the company, they were told that "many people are calling customers pretending to be us and giving our phone number." Who is impersonating Support One Care, and why they would give out the real company's phone number? We don't know the answer to those questions, but we do know that a great many companies in India seem to be working the same scheme, registering very similar company and website names.



Thank you for your support

Here's a slightly edited account of a support scam sent to ESET UK by someone wanting to know if he really had a problem, and if so, how to resolve it.

"... I was contacted via telephone by a company purporting to be a Microsoft solutions finder, who told me that my computer had a problem that was increasing every day. I do not know how they got my phone number or how they knew I had a problem when I didn't. I attempted to verify their authenticity, but could only do so by following the steps they gave me, which seemed to check out.

"At their request, I switched on my computer and, following the steps they told me to take, gained entry to what seemed to be the systems part of the computer. I was told to scroll down looking for a red symbol saying 'error' and a yellow triangle saying 'warning.' There appeared to be more errors than warnings. I got up to 63 errors and 20 warnings, going back to January this year, when the guy took me on to the next step.

"This involved going onto a rescue site that asked for a 6-digit code, which I didn't have. It was allegedly my warranty code — but as my computer is over a year old and therefore out of warranty they could, under strictest secrecy, upload the warranty back on to my computer. At this point, I smelled a rat and asked them how much it was going to cost me. The cost was 65 pounds. I, of course, said 'No way.' I was not going to pay someone I didn't know, using my credit card for something I didn't know I needed ..."

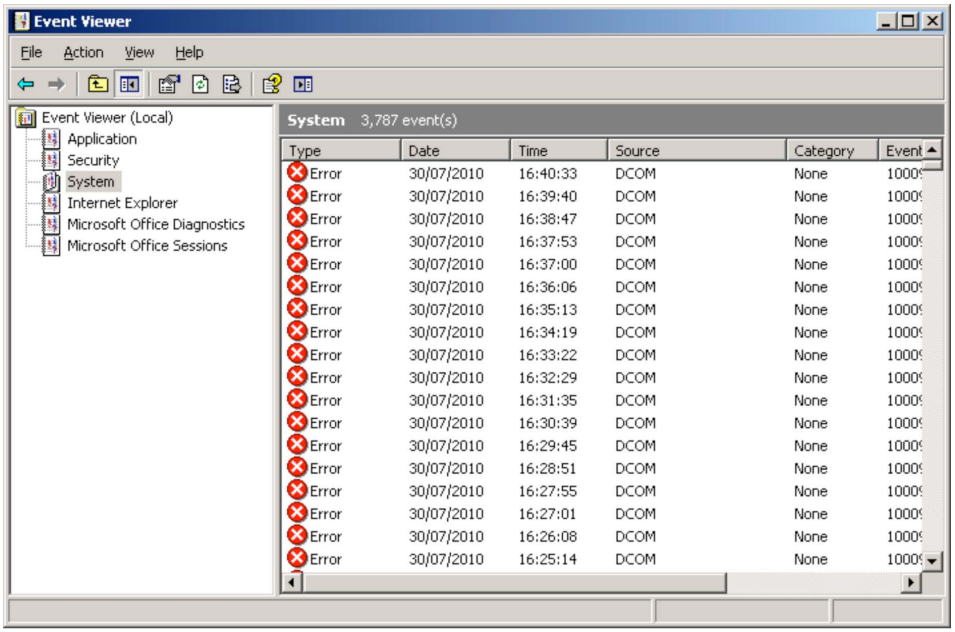
In this case, the individual targeted avoided the con, but others didn't. While for a time it was unclear what actually was downloaded if the victim did fall for the pitch, subsequent reports to ESET UK made it clear that cracked or pirated software was being installed. Indeed, much of our information comes from people who thought they'd already become legitimate ESET customers, asking for support because it wasn't working as expected. (Some have indeed become legitimate customers.)

ESET has heard of people paying anywhere from between £45 (US $73) to £79 (US $127) to clean their computers and install a "better" antivirus product[4].

A view to a scam

Steve Burn of hpHosts Online[5], a community-managed HOSTS file for ad and malware site blocking, has been exchanging malware-related intelligence with David Harley for some time. After Harley's first blog on this issue, Burn got in touch to tell us that he has been following similar scams since 2009.

The details vary, but typically, the caller is asked to open up an Event Viewer to see the "evidence" of infection, before being asked to download remote desktop software in order for the technician to rectify the problem. Being guided in this way to the Event Viewer is how most people are persuaded that something is wrong with their machine, but in actual fact, this utility simply reports information, warnings and errors regarding programs and Windows services.



Fake and pirated antivirus software have long been major problems. In the past fake or rogue security applications[6] have characteristically taken hold by way of screen pop-ups, but low Internet telephony rates and the use of telephone fraud may now mean that it's almost as cheap to call a victim as it is to wait for him to drop by your website. Of course, there's a difference between intrinsically useless (or worse) scareware and legitimate software that's been subverted and neutered by cracking, but in either case the objective is fraudulent.

True or false?

Like most scams, this one relies on social engineering techniques[7] to convince the user it's genuine. Unfortunately, attacks like this only make it harder for consumers to tell the difference between security truth and falsehood. This is, of course, part of the scam. At the same time as the scammers are making money, they're also attacking the reputations of legitimate security organizations and vendors.

ESET Ireland have also been observing reports of suspicious phone calls via tech support staff and online forums. These are also calls from people claiming to represent online computer repair services, using various generic names such as PC Support, PC Doctor, Online PC Repairs, and so on. It turns out that related scams have been observed as far back as 2008, but reports have multiplied dramatically in 2010. Worst affected, of course, are English-speaking countries (and public warnings from some sites and crimefighting institutions have already been posted in the UK, the US and Australia), but cases have also been reported in countries where other languages are used.

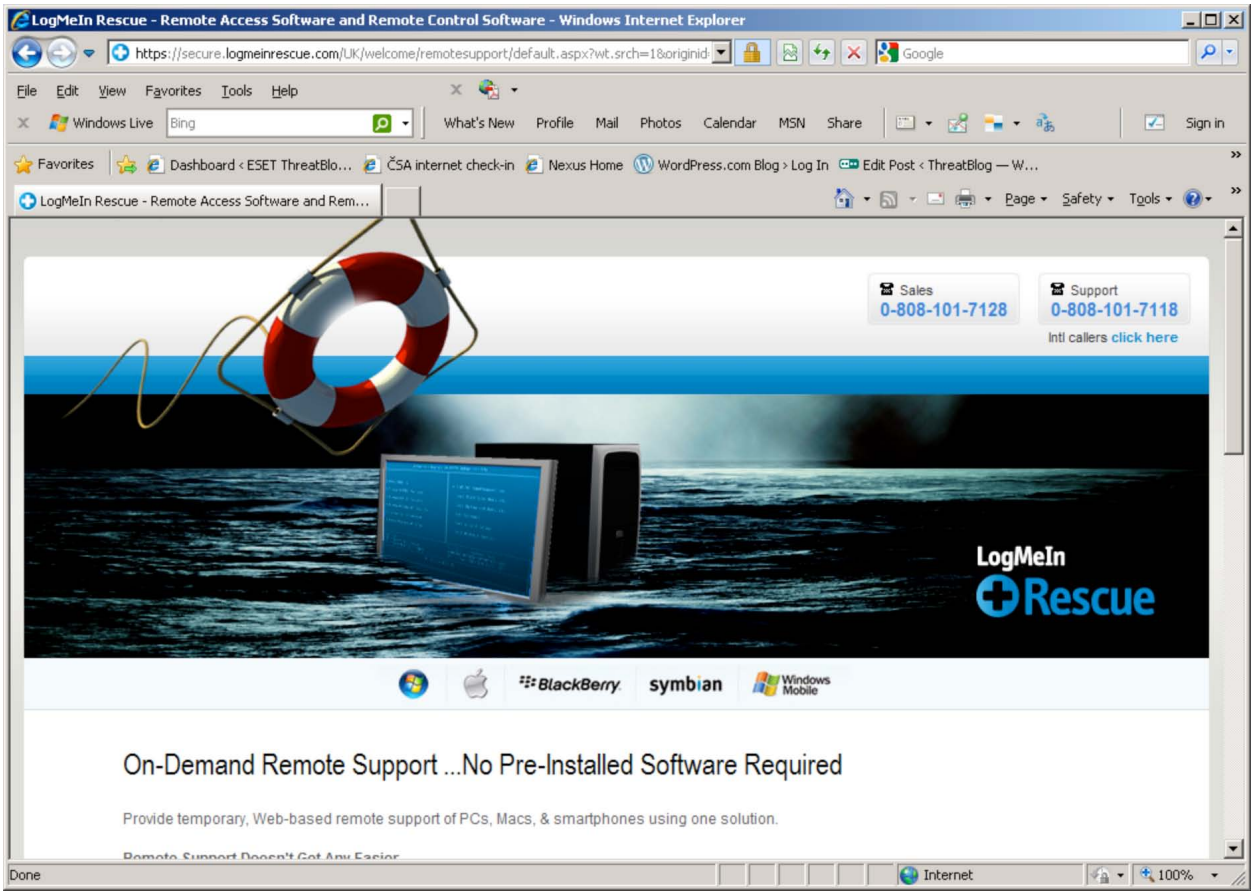
According to reports received in Ireland, the caller is likely to claim to have MCSEs (Microsoft Certified Systems Engineers) and Cisco Certified engineers available, and offers to fix and optimize the computer remotely, as well as to remove any malware. As with other reports, hesitant "customers" are told that their systems are probably riddled with worms and viruses, and the caller gives simple instructions on how to open the Event Viewer and use it to look for errors and warnings. As the Event Viewer is a reporting tool and therefore commonly flags frequent but usually noncritical errors and warnings anyhow, this looks convincing enough for most computer-wary victims, who are all too ready to believe that their antivirus program has let them down.

Log me in, clean me out

The next stage is to instruct the victim to access a certain website with Internet Explorer and download components needed to remotely "fix their computer" (and all the risks that can entail). But to add insult to injury, the victim is asked for credit card details to pay for the procedure and then offered an extended "Warranty Service" at serious prices, such as one year for €99 (US $159), two years for €189 (US $304) or three years for €289 (US $464) in some of the reported cases.

We found that these so called "technicians" have been using a legitimate free service from the LogMeIn website and their free service LogMeInRescue, which can be obtained for free during the initial evaluation period. This software allows access to your PC after login to the logmein123.com website. There is nothing illegitimate about this service in principle, but to whom are you giving access? What's to stop them planting scareware (rogue security software) or other forms of malware?

Once they've gained free access to your system, they can install anything for present or future use, in principle.



Oh! Calcutta![8]

Investigation by ESET researchers in the US, Ireland and the UK, in consultation with independent researcher Steve Burn and various law enforcement and other agencies, has thrown up a number of similar cases, nearly all of them traced back to companies based in Kolkata, India. And sure enough, cracked/pirated versions of ESET software have been installed by the scammers—though of course, being illegitimate copies, they have failed to function as expected. This has led to a number of requests for support being placed with real ESET support desks[9]. We can't tell how many similar scams have used or have claimed to use products from other legitimate companies, but as we are aware of many sites offering cracked versions of software from other companies as well as our own, it may be that reports to ESET are just the tip of a mighty iceberg.

Many customers have granted this access for this "Free" service from a well-known company and allowed the self-proclaimed technician to access their PC and perform checks and scans. These technicians present themselves as contractors working for Microsoft or for companies claiming Microsoft affiliation, using names like Virtual PC Doctor, SupportOnClick[10], [11], Click4Rescue[12], and so on.

Not everything is Microsoft's fault...

...However often the advocates of non-Microsoft operating systems tell us that it is.

This particular scam has nothing to do with Microsoft or its reputable affiliates. Nor, of course, do ESET or other reputable antivirus companies take this approach. There is very specific legal protection in various parts of the world against cold-calling to offer goods and services where the call recipient is not expecting such a call or has not specifically invited it. However, a contract may exist between a consumer and a provider – such as an Internet Service Provider (ISP) – which gives the provider the right to contact the customer directly or through a third party if it becomes aware of a security problem that affects that customer. However, this would not constitute cold-calling if the right to make such contact is enshrined in the contract, even if the customer is unaware of specific provisions within that contract. While such contractual arrangements are by no means a bad idea, they do have the potential to "groom" the customer into accepting the likelihood of "authorized" calls. How does the customer tell the difference?

The European Union's Data Privacy Directive 2002/58/EC requires members states to enact legislation to control cold-calling, using either an opt-in or an opt-out model. There are a number of opt-out registers:

- UK Telephone Preference Service[13]
- Republic of Ireland National Directory Database[14]
- U.S. "Do Not Call" Lists[15]

Clearly, services like these will not stop scammers and suppliers of fake products and services from breaking the law, but they do provide indirect protection, in that they may make it easier for wary victims to distinguish between legitimate and fake callers. A legitimate caller should not contact anyone on a "do not call" list, and should offer – or at least provide information on request about – opting out of its databases.

But beware: The type of call center scam we're considering here does not start off sounding like an obvious sales pitch. It usually begins with "advice" that the call recipient has a security problem[16]. Note that it's not always along the lines of "you have a virus/malware"; it may use other scare tactics such as advising you of a network problem or a system issue with your PC. Characteristically, it's only after using a number of approaches (such as the much-reported misuse of Event Viewer), in the hope of convincing the victim that he or she really has a problem that needs to be addressed, that they

will offer a for-fee solution. This is analogous to the call that starts with a survey on some issue likely to interest any householder and ends with questions like "Would you agree that XYZ is a problem?" and "Would you be interested in a solution for XYZ?"

Often, in such cases, the unlikelihood of some remote call center analyst knowing in advance what's "wrong" with your system, and having access to your contact details, is a red flag in itself. However, as the "walled garden" approach to service provision, by which an ISP can make continued provision conditional upon the clean state of the client system, becomes more common, it's likely that more customers will come to accept the possibility of telephoned warnings of a problem with their system[17, 18]. In jurisdictions where such legislation exists, a company that uses an alert as an opportunity to offer enhanced support services would be treading on extremely thin legal ice (and a fake alert would be right over the line). But we already know that some legitimate companies are not above taking a leaf out of the scareware provider's book[19]. In this "enhanced service" scenario, the dividing line between the legitimate and the fraudulently motivated caller becomes very hard to distinguish (practically speaking, and perhaps legally). Unfortunately, it's the ability to blur that distinction that the suppliers of fake services and software consistently seek to exploit[20, 21, 22].

Of course, if Microsoft did start a service that cold-called malware victims offering unsolicited support, assuming there was some legal way for it to do so, it's unlikely that it would offer software from its competitors in the security market.

This is a scam targeting anybody who is unaware of the risks entailed by allowing potential criminals remote access to his or her PC. Fortunately, most victims have been wary enough to call ESET support for verification, and the intrusion was immediately stopped with the help of real ESET support technicians, so we don't have consistent information about what happens to people who go right through the "service" process. Mostly, we have reports of nonfunctioning "cracked" installations rather than actively malicious software—"malicious" in the sense of keyloggers, Trojan downloaders and so on—but there's no reason why out-and-out malware couldn't be installed by these means.

Conclusion

"Apparently[22], it is proving financially viable for cybercriminals to set up their own call centers[23], then cold-call at random[24] (according to a Get Safe Online survey in October 2010[23], one in four UK web users were targeted via cold calls, with the perpetrators making some easy bait-and-switch[25] income in the process). The problem with preventing such scams is that social engineering[7] is almost by definition very low-tech in nature, requiring little in the way of technical resources and investment"[26].

It's difficult to differentiate between various types and levels of this kind of fakery: Today's criminals operate in environments where it's standard procedure to obfuscate connections and make it difficult to "follow the money." It may be that this kind of fake support scam is not carried out by operators directly related to other criminals working in other areas, such as purveyors of fake security programs, credit card fraud, generation of Black Hat Search Engine Optimization (index poisoning), used to herd victims into installing other kinds of malware, or the kind of borderline malware commonly described as "Possibly Unwanted." (A classification that may do scant justice to the damage it can cause to a victim's experience online.) It's quite possible that the kind of heavily resourced call center associated with IMU's fake AV operations[27] has no direct connection with the operations reported out of India. It's also possible (even likely) that there are overlapping connections, but it's unusual for all these criminal activities to be traced to a single group.

Service support scammers are relying on the naiveté of their victims in order to persuade them to grant access to their computers and credit card details. There's very little a security company can do directly to prevent this activity, apart from keeping its own software up to date so as to block as many scammer websites as possible, and to detect the malware scammers may try to install and use once granted access. However, victims of the scams described here are either not

using up-to-date, legitimate security software, or are voluntarily replacing it with scareware[28] or with compromised versions of other products, so this may have little impact on the problem.

Most often, it is difficult enough for the security community even to learn of the various scam calls taking place. There is no single, centrally organized reporting system for victims who become suspicious. Some call the police, some call an AV vendor's tech support line, and some just hang up and forget about it. Those victims who actually fall for the scam may similarly react in ways that don't attract immediate or direct attention in the security community. Indeed, quickly terminating such a phone call rather than trying to find out more about it is often a highly rational approach to lessening the risk, as is using opt-out registers. In fact, any cold call should be regarded as suspicious, and more so if it offers security advice. At the very least, it makes sense to verify the source and authenticity of any offer of service, and not to be panicked by warnings of immediate threat into making unwise decisions about whom to trust with your credit card details.

While ESET has been doing its best to warn potential victims of the scam (and it's good to see other vendors now taking this issue seriously), this fraud is already all too similar to the fake antivirus reports we've grown accustomed to in recent years[29]. It would be all too easy to extend the scam to use completely fake software — not just antivirus software. Threats like this don't only harm users, but are an assault on the credibility of real security software, system maintenance tools and so on.

References

1. Wikipedia, Hanging on the Telephone, 2010. http://en.wikipedia.org/wiki/Hanging_on_the_Telephone
2. David Harley, Marketing Misusing ESET's Name, 2010.
   http://blog.eset.com/2010/06/23/marketing-misusing-esets-name
3. Stuart Turton, Pensioner Targeted by Fake Virus Phone Scam, 2010.
   http://www.pcpro.co.uk/news/security/356833/pensioner-targeted-by-fake-virus-phone-scam
4. ESET Global Threat Trends for July 2010.
   http://www.eset.com/resources/threat-trends/Global_Threat_Trends_July_2010.pdf
5. hp-Hosts, 2005. http://hosts-file.net/
6. Cristian Borghello, Free But Fake: Rogue Anti-Malware, 2009.
   http://www.eset.com/resources/white-papers/Free_but_Fake.pdf
7. Cristian Borghello, translated by Chris Mandarano, A Tried and True Weapon: Social Engineering, 2009.
   http://www.securingourecity.org/resources/whitepapers/Social_Engineering_Borghello.pdf
8. Wikipedia, Oh! Calcutta!, 2010. http://en.wikipedia.org/wiki/Oh!_Calcutta!
9. David Harley, Fake AV, Fake Support, 2010. http://securityweek.com/fake-av-fake-support
10. hp-Hosts, ALERT: metsupport.com – Yet Another Telephone-Based Fraud (aka SupportOnClick Revisited — Again),
    2010. http://hphosts.blogspot.com/2010/06/alert-metsupportcom-yet-another.html
11. hp-Hosts, supportonclick.com Scamming You by Telephone!, 2009.
    http://hphosts.blogspot.com/2009/03/supportonclickcom-scamming-you-by.html
12. hp-Hosts, techonsupport.com, click4rescue.com, pcrescueworld.com: SupportOnClick Revisited, 2009.
    http://hphosts.blogspot.com/2009/12/techonsupportcom-click4rescuecom.html
13. UK Telephone Preference Service. http://www.mpsonline.org.uk/tps/
14. Republic of Ireland National Directory Database. http://www.dataprotection.ie/viewdoc.asp?DocID=908
15. National Do Not Call Registry. https://www.donotcall.gov/default.aspx
16. Orla Cox, Technical Support Phone Scams, 2010.
    http://www.symantec.com/connect/blogs/technical-support-phone-scams
17. Paul Ducklin, Sick of call centres? Don't worry, it gets worse... 2010.
    http://nakedsecurity.sophos.com/2010/11/04/sick-of-call-centres/
18. David Harley, Fake Security and Marketing with a Dull FUD, IS Now, submitted.
19. John Leyden, Check Point defends ZoneAlarm scareware-style warning, The Register 2010.
    http://www.theregister.co.uk/2010/09/21/zonealarm_defends_controversial_malware_warning/
20. David Harley, Fake Anti-Malware: Blurring the Boundaries, 2009.
    http://blog.eset.com/2009/10/24/fake-anti-malware-blurring-the-boundaries
21. David Harley, Scareware and Legitimate Marketing, 2010:
    http://blog.eset.com/2010/09/19/scareware-and-legitimate-marketing
22. BBC, Warning over anti-virus cold-calls to UK internet users, 2010. http://www.bbc.co.uk/news/uk-11754487

23. Get Safe Online, Watch out for malicious 'anti-virus' software scams, 2010. http://www.getsafeonline.org/nqcontent.cfm?a_id=1788
24. David Harley, Support Scams: This Time It's Personal, 2010. http://blog.eset.com/2010/11/12/support-scams-this-time-its-personal
25. Wikipedia, Bait-and-Switch, 2010. http://en.wikipedia.org/wiki/Bait-and-switch
26. David Harley, Fake AV Support Scams, 2010. http://blog.eset.com/2010/07/20/fake-av-support-scams
27. Jim Finkle, Inside a global cybercrime ring, Reuters 2010. http://www.reuters.com/article/idUSTRE62N29T20100324?pageNumber=3
28. Wikipedia, Scareware, 2010. http://en.wikipedia.org/wiki/Scareware
29. ESET blog, 2010. http://blog.eset.com/?s=fake+AV

Other resources

- hp-Hosts, SupportOnClick: Phoned by Malwarebytes? BigPond? Anyone Else?, 2009.
  http://hphosts.blogspot.com/2009/07/supportonclick-phoned-by-malwarebytes.html
- hp-Hosts, SupportOnClick Update, 2009.
  http://hphosts.blogspot.com/2009/04/supportonclick-update.html
- Jonathan H., Fake Tech Support Call Scam – Prefetch Virus logmein123.com, 2009.
  http://www.digitaltoast.co.uk/fake-tech-support-call-scam-prefetch-virus-logmein123com
- Malwarebyte, New Scam – They Call You by Phone!, 2009.
  http://www.malwarebytes.org/forums/index.php?showtopic=11156
- Staffordshire Council, Telephone Computer Support Warning, 2009.
  http://www.staffordshire.gov.uk/NR/rdonlyres/6997DBB0-E31E-4AFB-A886-C9DDEE114204/90090/TelephoneComputerSupportWarning.pdf
- The H, Cold-Call Scam Warns of Virus Infection, 2009.
  http://www.h-online.com/security/Cold-call-scam-warns-of-virus-infection–/news/112893
- The Register, Scareware Scammers Adopt Cold-Call Tactics, 2009.
  http://www.theregister.co.uk/2009/04/10/supportonclick_scareware_scam
- Charles Arthur, Virus Phone Scam Being Run from Call Centres in India, 2010.
  http://www.guardian.co.uk/world/2010/jul/18/phone-scam-india-call-centres
- Charles Arthur, Police Crack Down on Computer Support Phone Scam, 2010.
  http://www.guardian.co.uk/technology/2010/jul/19/police-crackdown-phone-scam-computer

www.eset.com

ESETHOTTWP20110218