MY PC HAS 32,539 ERRORS: HOW TELEPHONE SUPPORT SCAMS REALLY WORK

David Harley
ESET, North America
Email david.harley@eset.com

Martijn Grooten
Virus Bulletin, UK
Email martijn.grooten@virusbtn.com

Steven Burn
MalwareBytes, UK
Email sburn@malwarebytes.org

Craig Johnston
Independent Researcher, Australia
Email cajohnston@optusnet.com.au

ABSTRACT

Fake security products, pushed by variations on black hat SEO and social media spam, constitute a highly adaptive, longstanding and well-documented area of cybercriminal activity. By comparison, lo-tech *Windows* support scams receive far less attention from the security industry, probably because they're seen as primarily social engineering and not really susceptible to a technical 'anti-scammer' solution. Yet they've been a consistent source of fraudulent income for some time, and have quietly increased in sophistication. In this paper, we consider:

1. The evolution of the FUD and Blunder approach to cold-calling support scams, from '*Microsoft* told us you have a virus' to more technically sophisticated hooks such as deliberate misinterpretation of output from system utilities such as Event Viewer and ASSOC.
2. The developing PR-oriented infrastructure behind the phone calls: the deceptive company websites, the flaky *Facebook* pages, the scraped informational content and fake testimonials.
3. Meetings with remarkable scammers: scammer and scam victim demographics, and scammer techniques, tools and psychology, as gleaned from conversational exchanges and a step-through remote cleaning and optimization session.
4. The points of contact between the support scam industry, other telephone scams, and mainstream malware and security fakery.
5. A peek into the crystal ball: where the scammers might go next, some legal implications, and some thoughts on making their lives more difficult.

INTRODUCTION

Between 2008 and 2010 some of us started to become aware of a 'service' whereby people are cold-called to let them know that they 'have a problem' with malware infection, and are offered a 'better' replacement for their current 'inadequate' anti-virus [1]. The caller claimed to be from *Microsoft* or *Dell*, or 'Windows Support', 'Support One Care', or some other reassuring company name like 'Warm and Fuzzy PC Support Care and Customer Therapy', and offered (for a fee) the services of a *Microsoft* or *Cisco*-certified specialist to help to install anti-virus software.

This may sound like an ethically challenged distributor using fraudulent techniques closely resembling those used by distributors of fake AV (and that does happen), but it's not the way that reputable, law-abiding AV companies operate (although there have been instances where reputable and ethical companies have been forced to take action when they discovered that companies with which they were associated seemed to be abusing that relationship by using support scam techniques [2–5]).

THEORY OF EVOLUTION

The basic scam is very simple. The victim is cold-called and persuaded that that he needs to pay the company the caller represents to fix a problem with his computer remotely.

The scammer claims to call on behalf of an authoritative entity, usually some kind of service provider and more often than not *Microsoft*. According to *Microsoft* itself [6], scammers often claim to represent or be allied with units with names like these:

- Windows Helpdesk
- Windows Service Center
- Microsoft Tech Support
- Microsoft Support
- Windows Technical Department Support Group
- Microsoft Research and Development Team (Microsoft R&D Team)

While other reports confirm the use of these names, some will also – especially if pressed – reveal another company name, suggesting that they are supplying an outsourced service to *Microsoft* or another entity. However, the nature of the affiliation is usually vague, and even self-contradictory at various stages in the conversation. In later incarnations, scammers have cast their net wider and claimed to be (or be associated with) an ISP or some other kind of provider of goods or services – a computer manufacturer (*Dell* is frequently mentioned), *Cisco*, *BT* [7] or another ISP, even anti-virus companies.

Is it possible that *Microsoft* might actually ring out of the blue to advise someone that they have a security problem? Yes, but it's not a common scenario [8]. The company itself tells us [4]:

> 'There are some cases where *Microsoft* will work with your Internet service provider and call you to fix a malware-infected computer – such as during the recent cleanup effort begun in our botnet takedown actions [9]. These calls will be made by someone with whom you can verify you already are a customer. You will never receive a legitimate call from *Microsoft* or our partners to charge you for computer fixes.'

However, as more ISPs are considering the walled garden approach long favoured in Australia [10–12], where the customer can't access the Internet unless their machine is uninfected, customers will be conditioned into finding phone calls from remote call centres credible, and the legal ramifications are getting more complicated. We have other reports of ISPs contacting customers to advise them that they have or may have a bot-related problem, and it has been suggested that even financial institutions might include such a service when advocating the use of approved proprietary security technology.

When (or even before) the victim is persuaded that the call is genuine, the scam caller either claims that they have been notified of problems with the victim's system, or offers to check that system for problems. More often than not, the pitch involves the misuse of system utilities (as described below) to 'prove' the existence of problems. It also usually involves persuading the victim to allow the scammer remote access to the system in order to check its condition and, in many cases, to install software that will 'fix' the problem. While the problems are usually non-existent, the software used by scammers for remote access, to fix problems, and to protect the machine from future issues, may be quite genuine – though it will usually be a version that the victim could have obtained free of charge from other sources, without paying the service charges required by the scammer. On the other hand, an installed package could be practically anything. There have been instances where the software installed was a cracked version of a for-fee utility, and while we haven't seen reports of fake AV (or worse) installed by support scammers, it's obviously a common fear [13] and a distinct possibility. We have already seen many instances where free products and services were supplied by a semi-fraudulent for-fee service: particularly relevant in the context of this paper is a service that offered (for a fee and at different times) both the free version of a legitimate AV product and an unequivocal example of scareware. A clear case of profit overriding the welfare of the customer...

Finally, while the pitch may begin with the offer of a free service, it always includes at some point persuading the customer to furnish credit card details in payment for fixing problems and/or providing a protection plan for a fixed period.

EVENT VIEWER

In early versions of the scam, the victim is typically asked to open up an Event Viewer window to see the 'evidence' of infection [8] (in fact this ploy is still in common use: scammers are as reluctant as malware authors to abandon social engineering tricks and vulnerabilities that have already been proven effective). In the real world, this utility simply reports information, warnings and errors regarding programs and *Windows* services, but it's easy to persuade the IT-challenged that small transient errors (often found in absurdly high volumes) indicate the presence of malware or serious system problems.

Microsoft tells you to open Event Viewer, click Start, click Control Panel, click Performance and Maintenance, click Administrative Tools, and then double-click Event Viewer. However, a scammer is more likely to tell you to go to the Run menu and type in eventvwr. (Perhaps because it's simpler and works across most versions of *Windows*, though it may also make it less obvious that this is a maintenance utility rather than an anti-malware tool.) That will take you to a screen that shows you various system events, some of which will indeed be problems, though they're usually transient problems that have already come and gone. They are not malware infections (though it's remotely possible that one might be caused by infection). In fact, the utility is only useful to someone with a very good grasp of how *Windows* works trying to trace a known problem (and that certainly isn't your average support scammer). As a malware infection diagnostic, it's useless.

Typically, these scam callers use free versions of remote access software like ammyy.com and logmein.com to gain access to the victim's PC (they may even have ammyy or a similar tool hosted on their own sites) in order to install Something. On occasion, Something is a cracked version of genuine AV, but it could be anything: there have been reports of scammer *Facebook* pages that point to fake AV. However, we're still not seeing this used to install unequivocally malicious software. Mostly, products are installed that convince the victim that there is a serious problem with their PC and demonstrate that the technician is dealing with it. This is still the 'social engineering phase'.

CLSID

Here's a later ploy to convince victims that the scammer really knows something about their systems. The continuing success

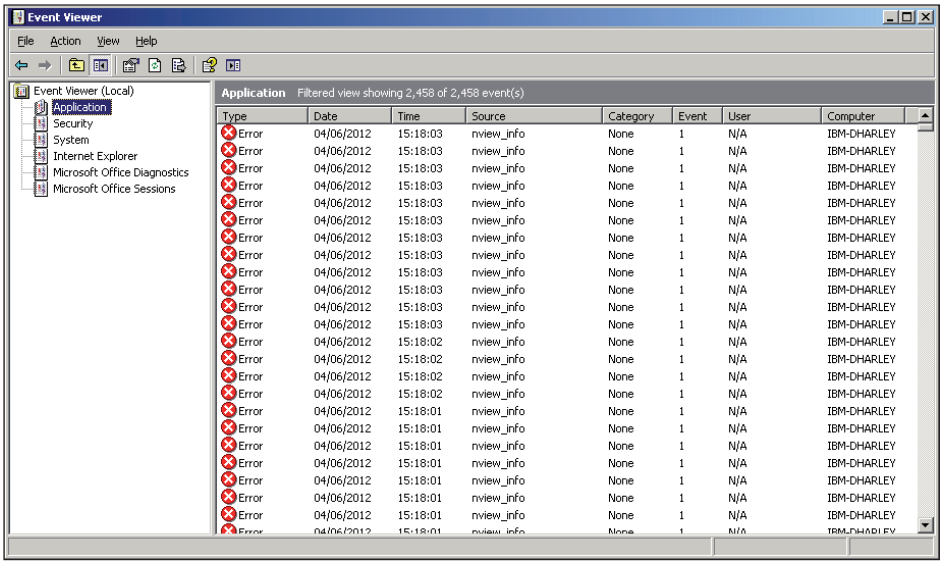

Figure 1: Event Viewer.

Figure 2: LogMeIn.

of this approach may be the reason why a blog article explaining how it works has attracted more blog comments than any other *ESET Threatblog* article [14]. As well as giving you your address (which they can get from a telephone directory) and a fake IP number to convince you that they can really see your system, they ask you to check a CLSID.

Microsoft tells us that ASSOC 'Displays or modifies filename extension associations. Used without parameters, ASSOC displays a list of all the current filename extension associations.' However, scammers tend to use one of the items near the bottom of the list it outputs that looks like this:

```
.ZFSendToTarget=CLSID\{888DCA60-FC0A-11CF-8F0F-
00C04FD7D062}
```

That's a Class Identifier stored in the *Windows* registry, but no registry hacking is needed. The scammer directs you to the DOS prompt to type ASSOC. That command actually lists file associations, telling you (for instance) that a file with the suffix .xltx is an *Excel* Template file.

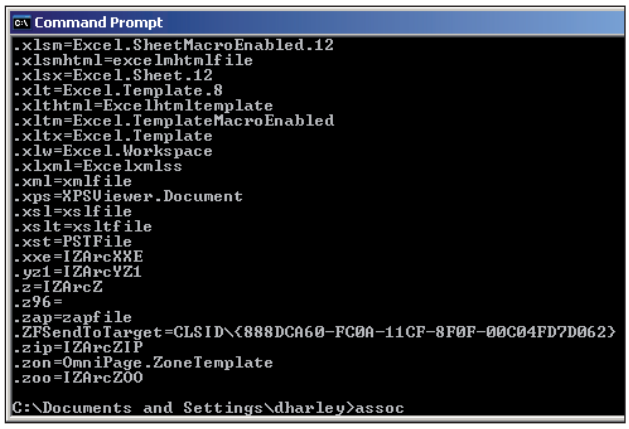

Figure 3: ASSOC.

That identifier isn't unique: it's the same on all the PCs we've checked. In other words, this doesn't prove in the least that the scammer can see CLSIDs or anything else on the victim's PC, including Event Viewer logs. Unless, of course, they fall for the scam and give the scammer remote access. The ASSOC command actually tells us here that files with the extension .zfsendtotarget are used for compressed folders by *Windows*, *WinZip* and *WinRAR*. However, the scammer will usually tell the victim that this is the unique identifier of his PC, as proof that he (the scammer) really can see that there is a problem uniquely associated with the victim's system.

In other variations the caller claims that *Microsoft*'s Computer Licence Security (or Secret) ID has been identified as obsolete and needing renewal, or is illegal. There's no such thing: it's the same class identifier.

INF AND PREFETCH

These are alternatives (or supplements) to the Event Viewer and ASSOC/CLSID ploys used by support scammers from India to 'prove' to a victim that their system is infected with malware or has other security/integrity problems. They are, in fact, legitimate system utilities [15].

The 'PREFETCH' command shows the contents of C:\Windows\Prefetch, containing files used in loading programs.

The 'INF' command actually shows the contents of a folder normally named C:\Windows\Inf: it contains files used in installing the system.

INF and PREFETCH are legitimate system utilities, so how are they misused by scammers? By asking a victim to press Windows-R to get the Run dialog box, then asking them to type in something like 'PREFETCH hidden virus' or 'INF trojan malware'. When a folder listing like those above appears, the victim believes that the system is listing malicious files. In fact, these commands ignore parameters in the Run box. You could type 'INF elvish fantasy' or 'PREFETCH me a gin and tonic and then peel me a grape' and you'd get exactly the same directory listing, showing legitimate files.

Event Viewer, ASSOC, INF and PREFETCH are the primary tools we see used in the social engineering phase where the scammer sets up the victim.

SITES FOR SORE EYES

Looking at some of the companies claiming to offer online technical support [16], we find a whole raft of common, suspicious characteristics:

- Local company addresses that turn out to be fake, unregistered at Companies House, at accommodation addresses that may or may not exist.
- The same sites turning out to be registered by the same registrant for multiple (but obviously closely related) companies, almost invariably in India. This multiplicity of related sites and companies under different names has a clear survivalist functionality: while we've had some success in taking down scam sites, some have shown impressive resilience in terms of reappearing under different names.
- Claims to have been established for several years that haven't been substantiated by registration data.
- Use of the same photographs, text and statistics in different contexts and on different sites, indicating the use of stock photographs and boilerplate content.

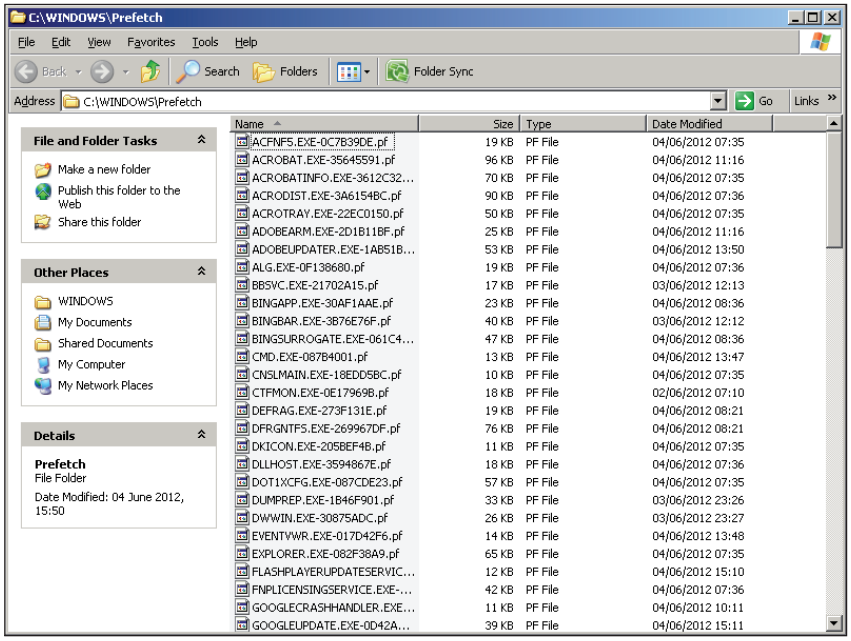

Figure 4: PREFETCH.

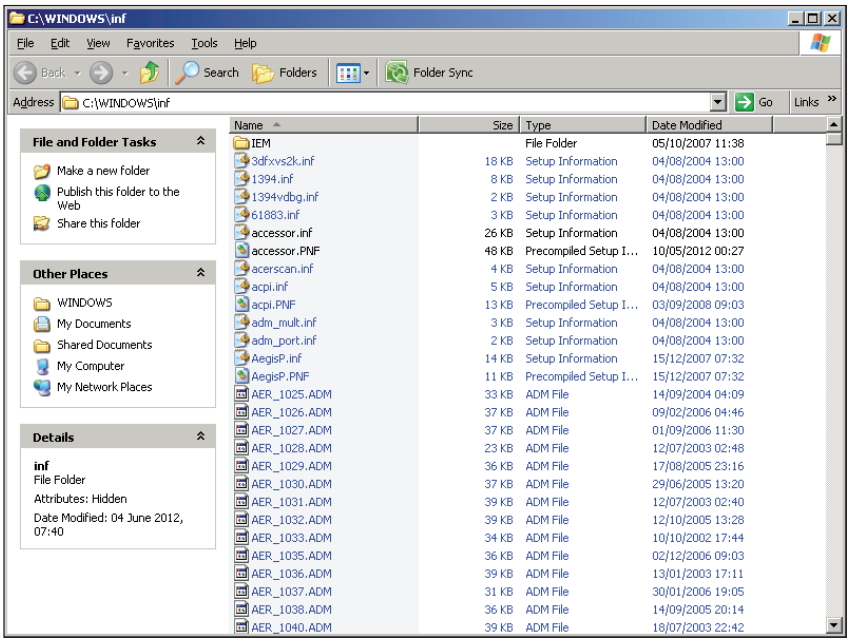

Figure 5: INF.

- Recommendations and testimonials that show suspicious similarities even without the use of textual analysis tools.
- Links to moderately helpful articles scraping content from unrelated sites, such as *CNET*, not necessarily with acknowledgement of the source.
- Content that appears to be original, but more malicious than helpful. Rather than providing a proven step-through process for fixing a problem, they demonstrate unresolved difficulties so that the victim will follow the links to

'computer technical support providers' or '*Dell* technical support' or '*Linksys* support', all of which lead to the same support site. Following the trail further back to licensing sites, for example, may lead to even more unpleasantness such as fake AV.

We don't know of a foolproof, consumer-friendly way of telling which *Facebook* accounts and pages are 'dummies' set up purely to promote a product or service (fraudulent or legitimate). Even a genuine account holder can be the victim of a rogue service, or tricked into 'Liking' an inappropriate page as part of the scam, and anyone could fake a testimonial using stock photos and made-up names. We expect to see more *Facebook* pages and blog pages with scraped or stolen content or even frankly deceptive content, used to add credibility to inauthentic websites. But it's hard to verify the accounts behind social media sites and even registered domains have their challenges. However, even if the data provided by the websites is genuine, that doesn't discount the possibility of a scam. *WHOIS* data, for instance, tends to give at least some information about the real location. It is not necessary for the scam to work to use fake/misleading information on the website/*Facebook* page.

MEETINGS WITH REMARKABLE SCAMMERS

There is a wealth of material available in various corners of the Internet where people have recounted their experiences of conversations with support scammers: some of these are victims who have subsequently realized they were being scammed, while many more are accounts of scambaiting, an exercise which probably affords more amusement to the scambaiters (and their readers) than harm to the scam industry. The authors have also 'enjoyed', and in some cases written about many such encounters [11, 17, 18], and comments added to our own blogs [14] have also furnished us with a great deal of anecdotal information.

Support scams are particularly common in the UK, Ireland, Australia and New Zealand, and in the US and Canada, but we're seeing increasing numbers of reports from other European countries (especially those where a high proportion of the population speaks English) and even South Africa and Singapore. We suspect that the call centres in question have cast their nets wider as the more established phisheries have become depleted due to increasing awareness of the scam and the sheer volume of scam calls placed again and again to the same telephone numbers.

The callers often introduce themselves using very English-sounding names – which is apparently common practice in Indian call centres – but nearly all reports mention their heavy accents, also usually assumed to be Indian. (We have just one report of a very 'English' accent.) Since most of the calls seem to originate in or around New Delhi or Kolkata, they generally don't care much about national Do Not Call lists. In fact, one caller refused to believe that there was any such thing as the UK's Telephone Preference List [19] (the equivalent to the US National Do Not Call Registry [20]).

Sometimes, the caller gives a number to call back on which appears to be local, but which reroutes to India. (More recently, we've seen many reports where the caller seems to have a local number or gives a local number to call back on.) Later, we started to find these numbers listed on sites belonging to a company based in India, claiming to be a *Microsoft*-registered partner, and offering various support plans.

Over time, the scammers have diversified into other techniques and topics: not just 'malware' alerts but warnings of 'system errors' and system utilities like registry cleaners, offers to 'fix' files that are only broken because the scammer encrypted them, even fake surveys so that they can ring back later and use a sales pitch tailored to your system. There are later reports of other survey-based scam financial services, and demands for loan repayment. However, there are practical difficulties in following up on all these variations, let alone (in)validating their claims. Apart from the resources such an investigation would consume, there are issues where a legitimate provider or vendor uses offshore call centres – obviously for financial reasons, but possibly also to get around local 'Do Not Call' legislation.

The reports we have are somewhat self-selecting: it's likely that actual victims of scamming are under-represented, since even if they've become aware that they've been scammed, they don't necessarily go and brag about it. Scambaiters, on the other hand, are less diffident about their efforts to waste the time and diminish the profits of the unfortunate scammers who cross their paths. While both groups have furnished us with significant information, we could wish that there was a higher-profile, more direct channel where victims could share their experiences. But what do we know about the cold-callers themselves?

Psychologically, it seems that they're a pretty mixed bag. While some of the ploys used in scammer scripts (Event Viewer, ASSOC, and the INF and PREFETCH folders) [21] suggest fairly extensive knowledge of the *Windows* interface (though not necessarily of the internals), it's rare to find significant expertise demonstrated by the crews that make the actual phone calls. We suspect that some lack the meagre technical knowledge they would need to recognize that what they're doing is fraudulent. Where call centres are contracted to supply services to (or are otherwise affiliated to) legitimate services, it's like that – on the ground floor where the phone calls are made, at least: some staff are unable to discriminate between legitimate, ethical support practice and downright fraud.

Others are clearly more aware. Some of them are surprisingly ready to talk about what they're doing [11]:

> 'The caller was more than happy to answer my questions about the group's *modus operandi* and admitted that his job was to cause confusion and fear in the victim, while posing as a trusted advisor, so that he could sell the victim a product.'

Others have been more inclined to bluster and threaten, even when (or possibly particularly when) their lack of understanding has been highlighted during interrogation by a less patient recipient of their attentions [17]. As our writing deadline looms, we note a number of recent reports where the scammer threatens to deprive the victim of the *Windows Update* service or even their network connectivity: hopefully, a sign of frustration that the con is getting harder to work.

WHAT DO WE TELL THE USERS?

How can the industry best help the user distinguish between 'good' and 'bad' products and services? In the absence of a technical attack susceptible to a technical defence, are education and reverse victimology the only answer?

To date, while our attempts to raise awareness of the issue in other segments of the security industry, law enforcement agencies and others [22, 23] have been well received, they haven't translated into conspicuously effective impact on the problem as a whole. You might think that the anti-malware industry would have a particular interest in mitigating an attack that damages its own credibility, and honourable mentions are due to *Microsoft* [24, 25], *Symantec* [26] and *Sophos* [12] for their attempts to publicize the problem, while one of the authors has bored *ESET*'s blog followers [27] and his other readers [28–30] to death on the issue. However, these piecemeal efforts have not attracted much (consistent) attention from the world – or the media – at large.

Two questions have come up time and time again in the course of our research into support scams, and answering them seems to offer a baseline for an educational initiative.

The first is, 'Can't the authorities do something about these guys?'.

This is a crime across international borders. If you're subscribed to a 'do not call' registry, that gives you a little less hassle from cold-callers within national borders, but a police force in the US or the UK can't just take and verify a complaint, trace a phone number, and have scammers arrested in Gurgaon or Kolkata, any more than they can in the Ukraine or Moscow. There has been some successful cooperation in shutting down some scammer websites, just as there has with taking down botnets and fake AV sites. However, a more permanent fix hasn't so far proved possible without a level of international cooperation that doesn't seem to exist yet. Partly that's about patchy cross-border relationships between governments and law enforcement agencies. But it's also about the fact that, in general, this type of fraud is what has been described by one of the authors as a 'mosaic crime': large profits built up from small sums stolen from individual victims. If you're one of those victims, the sums might not always seem so small, but law enforcement generally has to prioritize individual incidents involving large sums stolen from individual entities. It might be different if more incidents were traceable back to a single gang or organization, but that doesn't seem to be the case so far.

The European Union's Data Privacy Directive 2002/58/EC requires member states to enact legislation to control

cold-calling, using either an opt-in or an opt-out model. For example:

- UK Telephone Preference Service: http://www.mpsonline.org.uk/tps/
- Republic of Ireland National Directory Database: http://www.dataprotection.ie/viewdoc.asp?DocID=908
- In Spain, there is a do-not-call list called Robinson's List: https://www.listarobinson.es/default.asp.

In the US, there is the National Do Not Call Registry at https://www.donotcall.gov/default.aspx, and an equivalent site for Australians is https://www.donotcall.gov.au/.

Spanish telecom providers are somewhat relaxed about the extent to which businesses cold-call, at any rate on weekdays and Saturday mornings, but there is at least an agreement between most of the major providers that callers are not allowed to withhold the number from which they call. However, the telephone (like the Internet) is not good at recognizing national boundaries and the legal frameworks that go with them. Scammers will not respect local do-not-call lists (to which they may not even have access). Where phone calls are made on the basis of a quasi-war-dialling trawl through numbers served by a particular area code, or by progression through a public directory, there's no effective external filter. Even an ex-directory number might not be a defence against an automated dialler.

One commenter on an *ESET* blog article asked if there's more to be done to 'trap' scammers somehow so that they can be put out of business. A number of people (including the authors) have summarized, recorded or transcribed conversations with individual callers [31], and some have also recorded in some form what has taken place on their desktop when they've allowed an 'engineer' remote access so as to 'fix' problems. When bona fide researchers have done this, they've used either a virtual machine or a 'disposable' system containing no sensitive data that can easily be re-imaged. It may be that if more people reported such incidents to the police, the scams would get more attention. Sharing information on sites like callcenter.com does help end-users to identify scam calls, but it isn't information that's likely to filter through to active investigations.

And the other question? 'What can people do to protect themselves against this attack?' There is a blog article by one of the authors that attempts [32] to answer that question, but it's a topic that we'll certainly return to in greater detail, sooner rather than later and in greater depth.

SMARTER THAN THE AVERAGE SCAMMER, BOO-BOO?

What happens when a legitimate company finds itself allied with a company that uses ethically suspect selling techniques? This has happened on a number of occasions. Of course, sometimes a company is assumed to be involved in bad marketing because what appears to be one of its products is the subject of the hard-sell technique. For example:

- David Harley [8] first became aware of the scam because he was notified by another company that an *ESET* product was being sold this way. In fact, it turned out that the product being sold was a cracked copy. Other companies are believed to have had similar experiences.
- Craig Johnston [11] was told by one of the scammers he talked to that his company was installing legitimate copies of Registry Mechanic, by *PC Tools*/*Symantec*, though this cannot be verified.

Microsoft, however, eventually had to terminate its relationship with *Comantra*, a Gold partner, because of the volume of complaints about *Comantra*'s business practices [3, 33–35].

Perhaps the closest case to home for those of us in the security industry was that of *iYogi*, which was contracted to supply support services to *Avast!*, a highly reputable anti-virus vendor, but was exposed in March by journalist Brian Krebs as using unsavoury selling practices [36]. *Avast!* promptly suspended its relationship with *iYogi* pending further investigation [4, 5]. While there are many unverifiable reports about this affair, many of the comments on the Krebs articles suggest that telephone support staff may have been encouraged when selling support contracts to go far beyond the terms of the company's agreement with *Avast!* Some of the comments claim to be from *iYogi* employees, some defending it and some agreeing that it engaged in unethical and possibly fraudulent practices. An earlier anonymous blog article [37] also seems to give an interesting picture of life inside a call centre where scamming was to be found and even encouraged. There have been subsequent reports of other security companies using *iYogi* or a similar service: however, those who made those reports may have been misled by the fact that such companies are offering for-fee support of specific products, even where the actual vendors already offer free support. However, offering an extra layer of for-fee service is not necessarily illegal or even unethical: in fact, it's not far removed from the model used to generate income from some open-source software. Another instance of how a slight modification to a marketing model can make the difference between legality and illegality, if not between ethical and unethical.

CONCLUSION

Fake security products are not just an attack on the victim's credit card: while the main driver of nearly all malware authoring nowadays is profit, they're also an attack on the credibility and effectiveness of the security industry. The attack is not restricted to scareware and other utilities without utility and constantly morphing malicious binaries, either: it's carried out on many levels, though not necessarily by the same gangs:

- Threatened or actual legal action from cease-and-desist letters to court action in order to hamper the effectiveness and credibility of the security community
- PR-oriented activities such as forum, email and blog spamming, blogs and articles proclaiming the legitimacy of a dubious product
- Quasi-legitimate marketing, online support structures, and pricing models that mimic – or parody – the models used by the security industry

- The semi-fraudulent selling-on of legitimate but free products and services
- The increasingly sophisticated use and misuse of social media bolstering traditional black hat search engine optimization.

But in recent years the battlefield has been broadening far beyond the highly adaptive technical attacks that characterize malware-based attacks: we're seeing increased volumes, sophistication and infrastructural complexity of cold-call support scams, proving that social engineering with a minimum of programmatic content can be as profitable as unequivocally malware-based attacks. This is the sort of lo-tech social engineering attack that is hard to address technologically. It gets little official attention because it's a mosaic threat like SMS fraud and fake AV: individually, a small profit from a single scam, but a big enough hit rate to add up to a large profit in a country where the average wage is very, very low. It's aimed at individuals rather than businesses, so there are no corporate legal departments pressing for redress, and the cross-border implications make legal remediation tricky, even where the fraud seems unequivocal.

For the moment, it seems that the best remediation available is still education and raising awareness, while security companies outsourcing support services to India probably need to be particularly careful to monitor how appropriately these services are implemented. Well, we didn't say it was the perfect solution…

REFERENCES

[1] Harley, D. Marketing Misusing ESET's Name. http://blog.eset.com/2010/06/23/marketing-misusing-esets-name.

[2] Harley, D. Product Support and Now Fake Product Support. http://blog.eset.com/2012/03/15/fake-support-and-now-fake-product-support.

[3] Arthur, C. Microsoft drops partner accused of cold-call scam. http://www.guardian.co.uk/technology/2011/sep/22/microsoft-drops-partner-accused-scam.

[4] Steckler, V. iYogi Support Service Removed. https://blog.avast.com/2012/03/15/iyogi-support-service-removed/.

[5] Krebs, B. Avast Antivirus Drops iYogi Support. http://krebsonsecurity.com/2012/03/avast-antivirus-drops-iyogi-support/.

[6] Microsoft. Avoid tech support phone scams. http://www.microsoft.com/en-gb/security/online-privacy/avoid-phone-scams.aspx.

[7] Hodgson, M. Beware Scam Callers Pretending To Be From BT Offering Free Computer Security Checks. http://cumbrianwa.wordpress.com/2012/04/05/beware-scam-callers-pretending-to-be-from-bt-offering-free-computer-security-checks/.

[8] Harley, D.; Schrott, U.; Zeleznak, J. Hanging on the telephone: Antivirus cold-calling support scams. http://go.eset.com/us/resources/white-papers/Hanging-On-The-Telephone.pdf.

[9] Microsoft. Deactivating botnets to create a safer, more trusted Internet. http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/botnet.aspx.

[10] Internet Industry Association. icode commenced 1 December 2010. http://www.iia.net.au/index.php/all-members/869-get-ready-for-icode-in-force-1-december-2010.html.

[11] Johnston, C. Hello, I'm from Windows and I'm here to help you. Virus Bulletin, http://www.virusbtn.com/virusbulletin/archive/2011/01/vb201101-hello.

[12] Ducklin, P. Sick of call centres? Don't worry, it gets worse... http://nakedsecurity.sophos.com/2010/11/04/sick-of-call-centres.

[13] scottls1. MS Windows Service Center Scam!- Will Infect your computer...! http://support.emsisoft.com/topic/8092-ms-windows-service-center-scam-will-infect-your-computer/.

[14] Harley, D. Support Desk Scams: CLSID Not Unique. http://blog.eset.com/2011/07/19/support-desk-scams-clsid-not-unique.

[15] Harley, D. Support Scammers (mis)using INF and PREFETCH. http://blog.eset.com/2012/03/15/support-scammers-using-inf-and-prefetch.

[16] Harley, D.; Grooten, M.; Burn, S. Facebook Likes and cold-call scams. http://blog.eset.com/2011/11/09/facebook-likes-and-cold-call-scams.

[17] Harley, D. Here's my support desk! http://blog.eset.com/2011/03/04/heres-my-support-desk.

[18] Harley, D. Support Scams: Even More Personal. http://blog.eset.com/2010/12/16/support-scams-even-more-personal.

[19] Telephone Preference Service. http://www.mpsonline.org.uk/tps/.

[20] National Do Not Call Registry. https://www.donotcall.gov/default.aspx.

[21] Harley, D. Support-Scammer Tricks. http://blog.eset.com/2011/11/30/support-scammer-tricks.

[22] eCrime Researchers Sync-Up. http://www.ecrimeresearch.org/2012syncup/agenda.html.

[23] Harley, D. Cybercrime and Punishment. http://blog.eset.com/2012/02/13/cybercrime-and-punishment.

[24] Beauchere, J. Phone Scammers: Here to Help… Themselves. http://blogs.technet.com/b/trustworthycomputing/archive/2011/11/28/phone-scammers-here-to-help-themselves.aspx.

[25] Microsoft. http://answers.microsoft.com/en-us/windows/forum/windows_vista-security/i-received-a-phone-call-from-someone-claiming-i/4489f388-d6de-416d-9158-0079764bb001.

[26] Cox, O. Technical Support Phone Scams. http://www.symantec.com/connect/blogs/technical-support-phone-scams.

[27] Harley, D. http://blog.eset.com/?s=Harley+%2B+support+scams.

[28] Harley, D. Supporters Club. http://www.scmagazine.com/supporters-club/article/199459/.

[29] Harley, D. Help Desk Scams and Microsoft. http://blogs.securiteam.com/index.php/archives/1553.

[30] Harley, D. Fake AV, Fake Support. http://www.securityweek.com/fake-av-fake-support.

[31] Herold, R. Cyber Criminals Just Came A Callin' At My House. https://www.infosecisland.com/blogview/15066-Cyber-Criminals-Just-Came-A-Callin-At-My-House.html.

[32] Harley, D. How to recognize a PC support scam. http://blog.eset.com/2012/04/18/how-to-recognize-a-pc-support-scam.

[33] Hunt, T. Interview with the man behind Comantra, the 'cold call virus scammers'. http://www.troyhunt.com/2012/05/interview-with-man-behind-comantra-cold.html.

[34] hpHosts. Microsoft dumps partner over telephone scam claims. http://hphosts.blogspot.com/2011/09/microsoft-dumps-partner-over-telephone.htm.

[35] Security Garden. Microsoft Removes Gold Certified Partner Over Telephone Scam Claims. http://securitygarden.blogspot.com/2011/09/microsoft-removes-gold-certified.html.

[36] Krebs, B. Aghast at Avast's iYogi Support. http://krebsonsecurity.com/2012/03/aghast-at-avasts-iyogi-support/.

[37] Exposing Indian Call Centre Scam. http://indiancallcenterscam.blogspot.co.uk/2011/11/hi-everyone-recently-i-was-working-in.html.

FURTHER RESOURCES

- Harley, D. Giving Cold Callers the Cold Shoulder. http://blog.eset.com/2011/06/24/giving-cold-callers-the-cold-shoulder.
- Harley, D. Support Scam Info: Some More Links. http://blog.eset.com/2010/06/23/support-scam-info-some-more-links.
- Burn, S. Telephony scams: Your machine told them it was infected? Really? http://mysteryfcm.co.uk/?mode=Articles&date=18-01-2012.
- Harley, D. Security Software & Rogue Economics: New Technology or New Marketing? http://smallbluegreenblog.wordpress.com/2011/05/15/eicar-2011-paper/.
- Harley, D. PC Support Scam Resources. http://avien.net/blog/?page_id=790.
- Microsoft. Microsoft Survey Reveals Extent of Emerging Internet Phone Scam. http://www.microsoft.com/en-us/news/press/2011/jun11/06-16MSPhoneScamPR.aspx.