CFET 2012

6th International Conference on

Cybercrime Forensics Education & Training

FUD and Blunder: Tracking PC Support Scams

David Harley, ESET N. America

Martijn Grooten, Virus Bulletin

Craig Johnston, Independent Researcher

Stephen Burn, Malwarebytes

FUD and Blunder: Tracking PC Support Scams

David Harley, ESET N. America
Martijn Grooten, Virus Bulletin
Craig Johnston, Independent Researcher
Stephen Burn, Malwarebytes

Abstract

While the main driver of nearly all malware authoring nowadays is profit, fake security also undermines the credibility and effectiveness of the real security industry on many levels.

- Threatened or actual legal action, spamming and quasi-legitimate blogs and articles asserting the legitimacy of dubious products and services
- Marketing models that parody those used by the security industry
- The ethically challenged, and sometimes essentially fraudulent selling-on of legitimate but free products and services

Fake security products, supported by variations on Black Hat SEO and social media spam constitute a longstanding and well-documented area of cybercriminal activity. By comparison, lo-tech Windows support scams receive less attention, perhaps because they're seen as primarily social engineering 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.

The increased volumes, sophistication and infrastructural complexity of cold-call support scams suggest that social engineering with minimal programmatic content has been as profitable as attacks based on the use of unequivocally malicious binaries: lo-tech attacks with hi-tech profits.

These attacks have gone beyond the FUD and Blunder approach, from "Microsoft told us you have a virus" to technically more sophisticated hooks such as deliberate misrepresentation and misinterpretation of output from system utilities such as Event Viewer, Assoc, Prefetch, Inf and Task Manager.

We also look at the developing PR-orientated infrastructure behind some of the scammer phone calls, including deceptive company web sites and Facebook pages making use of scraped or deceptive informational content and fake testimonials.

We discuss some of the interaction we've had with 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 with a particular scammer. We consider the resemblances between the support scam industry, other telephone scams, and the security fakery associated with mainstream malware. And finally we ask where the scammers might go next, what are the legal implications, and 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, is the only answer education and reverse victimology?

Introduction

Where once malware was mostly about mischief, bragging rights, and occasionally sheer destruction, nearly all malware authoring nowadays is about profit. However, fake security in all its forms is also an attack on the credibility and effectiveness of the real security industry. The attack is by no means restricted to scareware (fake security products such as rogue AV) and other utilities without utility, such as software that makes unrealistic claims of enhanced system performance. [1]

Anti-malware companies are constantly besieged by the gangs behind programs either side of the borderline between more-or-less useless and actively malicious – what else do you call a program that makes your system next to useless by forcing you to view a stream of advertising by diverting your web searches to irrelevant sites? In some cases, the security industry refers to such borderline cases as Possibly Unwanted. Or, in some other cases, as Possibly Unsafe, a category that usually includes programs that are legitimate but prone to malicious misuse.). [2]

There's something not altogether wholesome about this evasion of plain speaking: often, what it means is "we daren't call it malware, but you wouldn't like what it does when it's installed!" However, it does mitigate (but by no means eliminate) the constant (and expensive) stream of threatened or actual legal action – ranging from cease-and-desist letters to court action – clearly intended to hamper the effectiveness and credibility of the security community. [3] Unfortunately, it also means that the responsibility for deciding on whether to detect (or install) such programs is pushed back to the user, even though the problems with litigation make most security companies reluctant to discuss the issue publicly, even in an educational context. This, however, deprives the customer of the opportunity to make an informed decision. Even while many sectors of the security industry have been pressured in this way, the anti-security industry has applied further pressure to the AV industry through PR-oriented activities such as forum, email and blog spamming, and blogs and articles proclaiming the legitimacy of dubious products. At the same time, they've reduced public trust in legitimate security by misusing or counterfeiting our own tools. For example, quasi-legitimate marketing, online support structures, and pricing models that mimic the models used by the real security industry, while borrowing and extended marketing approaches from some legitimate companies that were already pushing the ethical envelope. [4].

Fake security products, supported by variations on Black Hat SEO and social media spam, constitute a longstanding and well-documented area of cybercriminal activity. "Blackhat SEO" (Search Engine Optimization) (also known as index poisoning or search poisoning) is used to compromise web searches using the likes of Google and Bing by ensuring that malicious sites are highly ranked. One of its uses is for driving potential victims to a site where programs flag "viruses" and demand money. (They may also self-install in the time-honoured manner of 'drive-by' attacks so that leaving the site, shutting down the browser or even restarting the computer isn't enough to fix the problem.) They can also incorporate "online support" to escalate the victim's engagement from free product, to free (but very short term) trial product, to removal of the "infections", to a customer satisfaction survey. Support staff at Innovative Marketing, a notorious marketer of fake AV, seem mostly to have dealt with enquiries such as: "I'm trying to install your product, but my antivirus keeps blocking it: how can I get it installed?"

Fake Security and Fake Support

Lo-tech Windows support scams receive less attention, perhaps because they're seen as primarily social engineering and therefore 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 a "rogue service" where 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. The caller claims to represent Microsoft or Dell, or "Windows" or "Warm and Fuzzy PC Support Care and Customer Therapy" offering – for a fee – the services of a Microsoft or Cisco-certified specialist to install antivirus software.

People have been all too ready to assume that this is the work of ethically-challenged AV companies and their distributors using fraudulent techniques closely resembling those used by distributors of fake AV. In fact, the scams in question *do* sometimes install a trial or cracked version of genuine AV as part of their service, along with other utilities that are more often than not genuine. However, these are almost invariably limited versions that don't cost the scammer money, but could be obtained for free by the victim from other sources, if he really needed them. However, the distancing of the antivirus industry from these unpleasant practices has been compromised recently by allegations that a company to which a legitimate AV vendor had outsourced its telephone support had abused that relationship by using the same sort of scaremongering and misrepresentation, employing techniques that are closer to out-and-out fraud than aggressive marketing. [5; 6; 7]

Panic Marketing

The basic cold-call telephone support scam is based on simple social engineering, what we might call the FUD and Blunder approach [8]. The scammer phones out of the blue (actually, almost invariably out of India, though the call sometimes looks as if it's local) and persuades the victim that there is a problem with his computer, which the caller can fix remotely – for a fee, of course. The caller claims to call on behalf of or to be working with *an* authoritative entity, sometimes an ISP [9] or system provider [10], but very often Microsoft [11]. Not so much panic buying [12] as panic marketing.

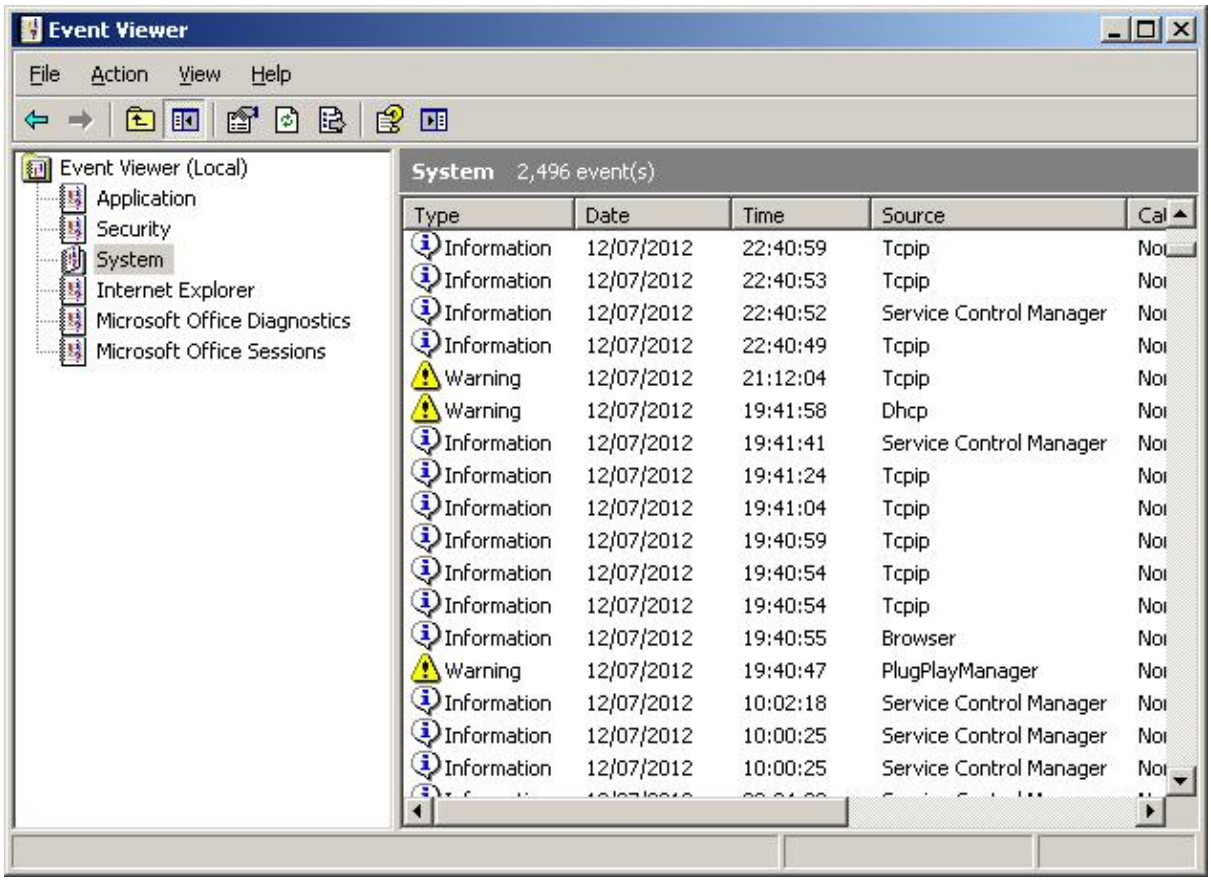
Usually, the persuasion technique consists of demonstrating that problems exist by the misuse and misrepresentation of system utilities that have little relevance to security and malware. These utilities fall into three main groups (and possibly one more that's just attracted our attention [13]) as described in the next sections. This generally involves asking the victim to allow the scammer remote access to his system in order to check its health and, often, to install software that the scammer claims will fix the problem. While most reports (and personal experience) indicates that the software installed is more often than not legitimate (even if it's unethically (misre)presented and irrelevant to the present needs of the victim), there is a common fear that scammers [14; 15; 16] will install something worse than a freeware utility.

Even though there is no evidence of a direct link between support scams and fake AV, we have seen many instances where end users were charged significant sums by a semi-fraudulent for-fee service for products and services they could easily have obtained and installed for free. One of the authors has previously commented on other services that offered (at different times but in both cases for a fee) both the free version of a legitimate AV product and an unequivocal example of scareware. [17] If you're happy to make money by pretending to provide security software, or charge semi-

fraudulently for free security software, you're not going to be concerned about whether it's real or fake software.

Event Viewer

An early (and still much-used) version of the scam involves talking the victim through opening up an Event Viewer window. Event Viewer is, unsurprisingly, a utility that shows system events, some of which will indeed show problems: however, they're usually problems that have already been and gone. While it's possible in some cases that such errors might be infection-related, that's not a common scenario, and it would be even less common, even for a helpdesk technician, to be able to identify malware infection from an event log that shows many events but in no detail. Someone who is that familiar with malicious processes is most likely to be working in an AV lab, not in a call centre, and would be using somewhat sharper tools.

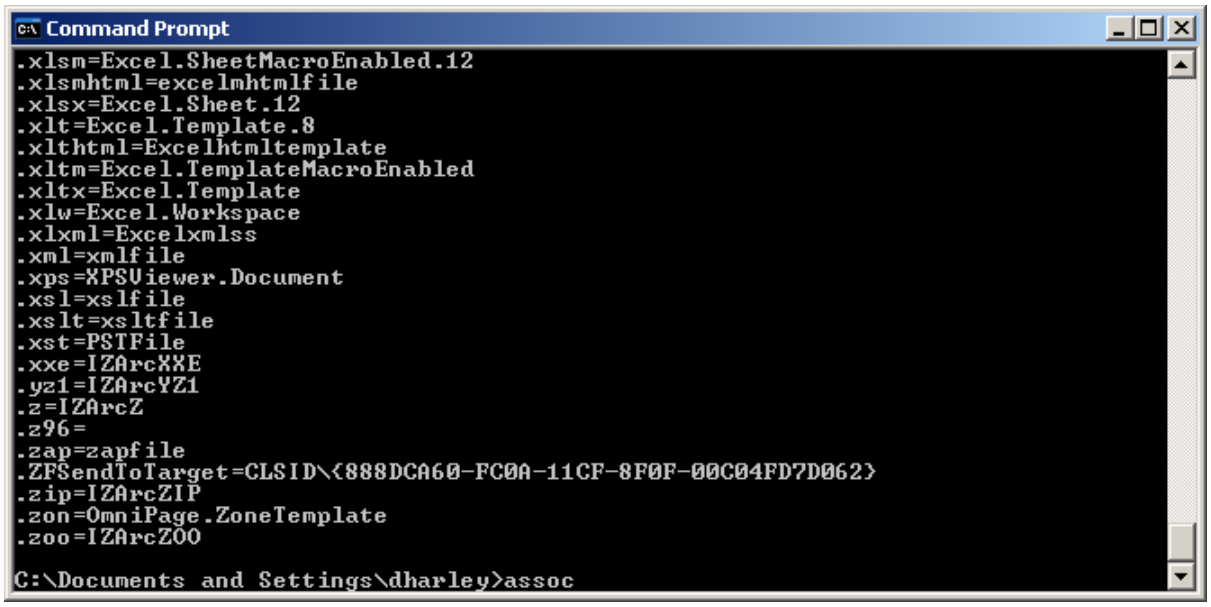


CLSID: Guilt by ASSOCiation

More recently we've seen scammers try to convince victims that they really know something about the condition of their systems by misrepresentation of the CLSID (file class identifier) shown by the ASSOC utility. They try to kid you that the entry in the output of the ASSOC utility shown below is a unique licence number.

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

In fact, it's an identifier for a type of file, and can be found on many millions of Windows PCs. [18]



That file association simply indicates that a file with the filetype .zfsendtotarget is used for compressed folders by Windows, WinZip and WinRAR. It isn't in the least unique: it's the same on *all* the PCs we've checked. However, the scammer will usually tell the victim that this uniquely identifies his PC, often by claiming that CLSID stands for Computer Licence Security/Secret ID. Sometimes he will claim that it is illegal or obsolete and that the victim must pay for registration.

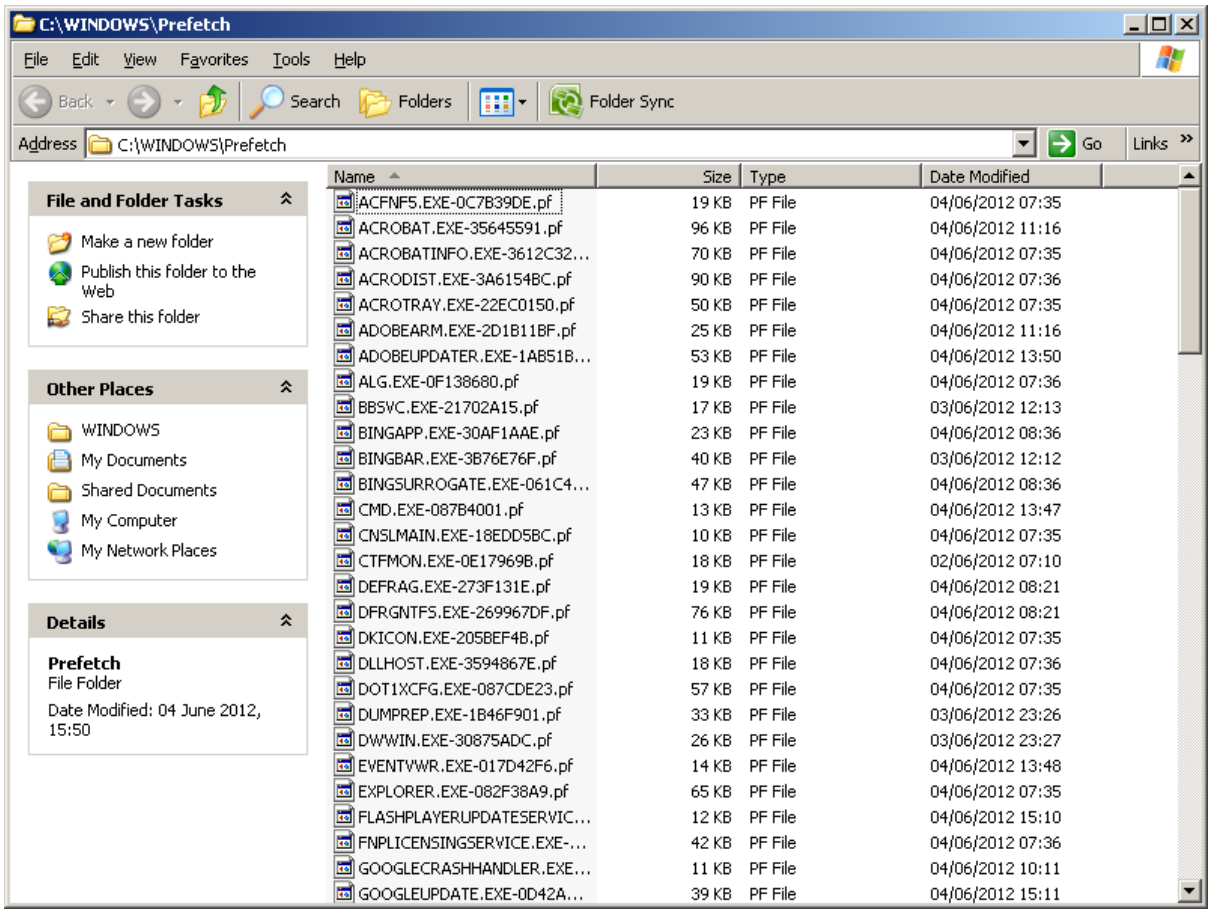
INF and Prefetch

ASSOC is not usually used with parameters, and in fact if called with an illegal parameter will put up an error message. A scammer could, in fact, get a cleaner display using the .zfsendtotarget filetype as a parameter.

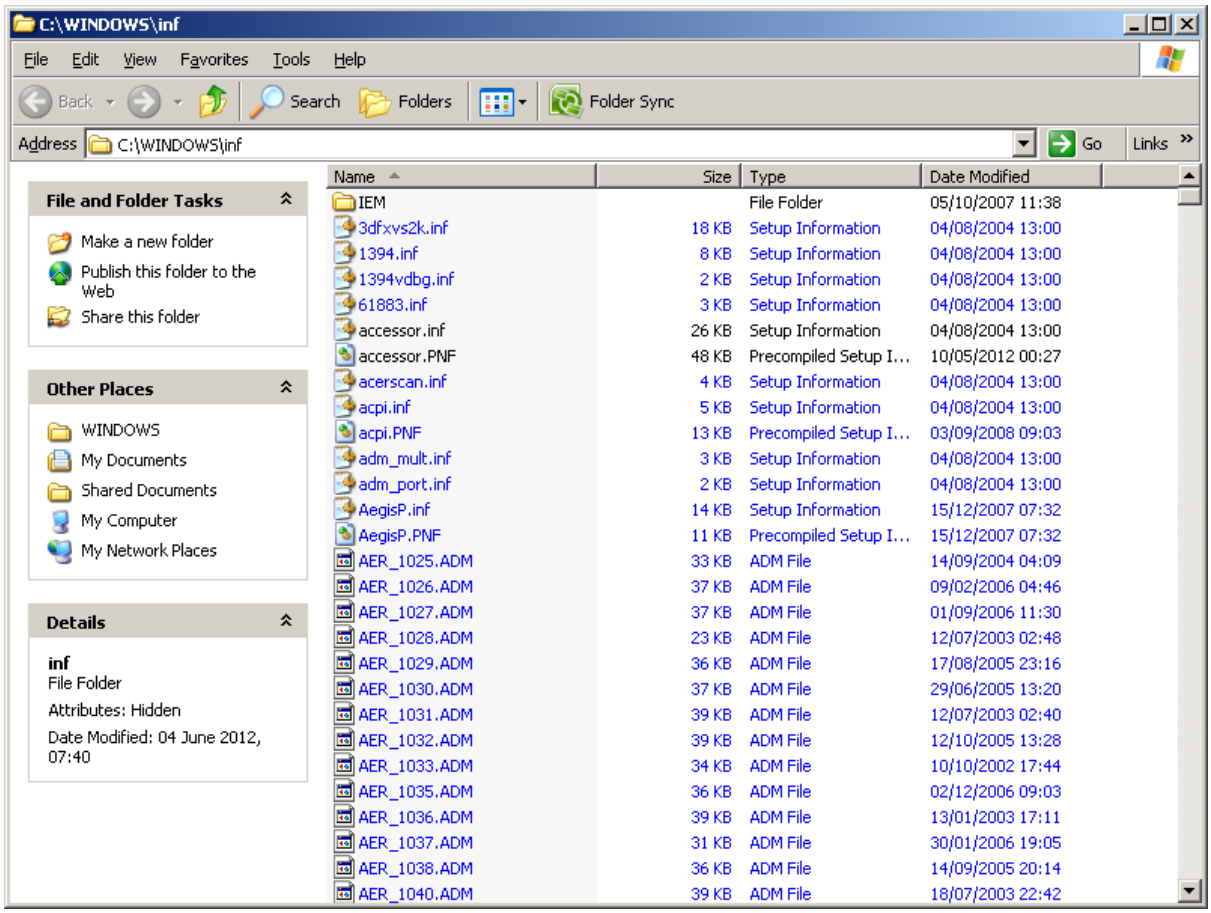
```
C:\ >assoc .zfsendtotarget
.zfsendtotarget=CLSID\{888DCA60-FC0A-11CF-8F0F-00C04FD7D062}

C:\>
```

They probably don't because that's a slightly challenging parameter to type in and doesn't look particularly security-related. And an illegal parameter like ASSOC GETLICENSE would generate an error message. However, scammers have seized with joy on a couple of system utilities that simply ignore illegal parameters. [19]

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 which contains files used in installing the system.

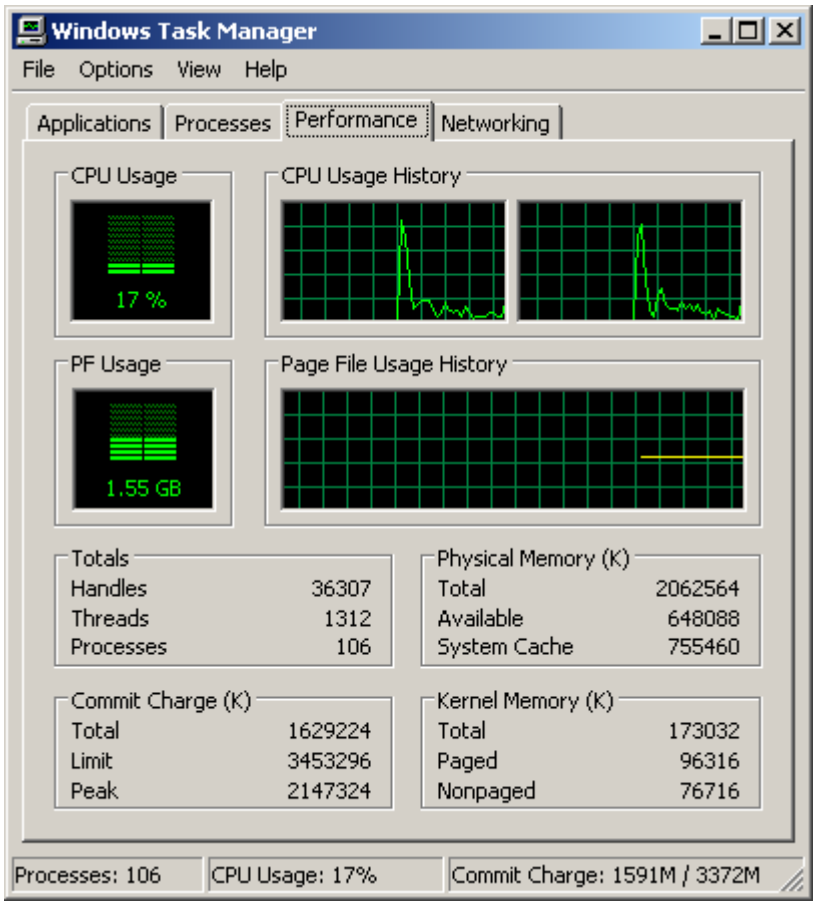


However, scammers have taken to asking the victim to type something in at the command line like "prefetch hidden virus" or "inf trojan malware". When a folder listing like those above appears, the victim believes that the system is listing malicious files. In fact, you could type "inf dustpan and brush" or "prefetch me a cup of tea" and you'd get exactly the same directory listing, showing the same harmless 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 to believe that there is a system problem.

Task Manager

However, one of the latest reports to cross our horizon tells us of a scammer who directed his intended victim to Windows Task Manager, trying to convince her that it was a problem that CPU usage was running at 3%, and it should be running at 80%. [20]



This is not only nonsense, but intentionally (and possibly dangerously) misleading: low CPU usage just means that the processor doesn't have much to do right now. A continuously high CPU usage percentage might actually indicate a problem of some sort, though probably not one that a cold-calling 'tech support' person is likely to be able to diagnose or fix.

Smelling a RAT [21]

Martijn Grooten has presented a comprehensive account of how he allowed a scammer to access a virtual system, complete with screen captures. [22]

Typically, scam callers keep their own software costs down by using free versions of remote access software (most often ammyy.com or logmein.com) to gain access to the victim's PC. However, they may have one of these tools or something similar hosted on their own sites. Primarily, this is to allow them to inspect (or pretend to inspect) the system and install security-related tools and system utilities, though some commentators have expressed concern that they might misuse that access to install malware such as keyloggers, or even to steal data directly.

One possible variation reported on the latter theme involves inviting the victim to back up his data to the scammer's site: so far we only have one report of that, but it does suggest a particularly potent misuse of common security advice. We do, after all, sometimes advocate backing up data before a potentially hazardous process such as malware disinfection, and we do, in other contexts, advocate the use of off-site backups. We *don't*, of course, advocate backing up to an untrusted site and service on the unverified say-so of someone who calls out of the blue claiming to be Microsoft.

In fact, there are scenarios where Microsoft *might* ring out of the blue (for instance) as part of a botnet takedown [23] or on behalf of a third party, but it's fairly unusual. [24] And that invites concerns as to whether the 'walled garden' approach will work in favour of the scammer. The principle of the 'walled garden' is that customer access to the Internet [25; 26; 27] (or even to specific services and resources such as online banking) is conditional upon the customer's system being uninfected. The concern, therefore, is that everyday users will be conditioned into finding phone calls from remote call centres credible. This is not strictly hypothetical: recently, we've been seeing instances where a potential victim is told that unless they comply with the scammer's instructions, he or she will not be allowed access to the Microsoft update server, or that all their access to the Internet will be blogged.

David Harley has also blogged at some length on his own conversations with scammers [as well as summarizing reports from scam victims and others who've interacted with fake support techs [28]. These reports include references to increasingly aggressive and sometimes downright threatening behaviour. These range from threats to hack the victim's system and predictions of imminent system crashes, to threats of legal action on account of 'illegal downloads', blacklisting from the Windows update service, and even threats of assault and worse. In recent cases, the scammer, enraged at the reluctance of the victim to surrender the details of his credit card, has tried to delete system files or crash the system while the remote access tool was connected. Hopefully, some of this aggression comes from frustration born of trying to scam an increasingly sceptical population.

This has a bearing on the increase of calls reported to countries where English is not the first language for most residents, but where a high proportion of the population is likely to speak it with some degree of fluency. For example, Microsoft NL has apparently seen enough activity in the Netherlands to put up a warning in Dutch [29], but in similar terms to the frequent warnings posted to its English language sites. It's likely that this increased targeting of regions like the Netherlands and Scandinavia reflects a need to widen the pool of potential victims in order to extend the scam's effective lifetime, as more people within the regions originally targeted learn to recognize the scam.

Craig Johnston [26] records a particularly enlightening (but rather less tense) interaction with a scammer who acknowledged that his advice was inaccurate but still believed himself to be providing a useful service. [10]

Conclusion

Unfortunately, it can be (and often is) argued that the security industry has brought some of this about by its own hype and FUD marketing practices. And indeed, it's worth asking why the general public finds it so hard to distinguish between the (usually) legitimate marketing model used by the industry, and the rogue marketing approach used by fake AV and fake support. [5] While there is no proven interaction between rogue AV gangs in Eastern Europe (and elsewhere) and support scammers in Kolkata, both have learned from ethically grey marketing practices sometimes associated (not always unfairly) with the security industry. Clearly, we need to do a better job of keeping our own business models distinct from the all-too-similar parodies we associate with rogue software and rogue support. We certainly need to avoid mimicking rogue marketing as well as educating both our customers and the people who market and sell products. It's a truism that a business is far more than a product: it's a whole infrastructure that ranges from R&D, to marketing,

to support, and to second-tier infrastructural support such as accounting and human resources. In a threatscape based on profit, though, fake security is equally complex and wide ranging, including:

- product development
- search engine optimization and other marketing tools
- social engineering (or 'marketing' as we call it in more legitimate contexts) as a means of entrapping victims
- identity and brand theft
- the whole gamut of fraud support techniques such as carding and moneylaundering
- the misuse of social media as a means of 'legitimizing' and 'authenticating' the spurious claims and practices that are the bread and butter of rogue software and support:
    - Deceptive company web sites and Facebook pages [30] and the misuse of scraped content, fake testimonials, and misrepresentation of real issues in order to sell fake services and products. [31]
- And – most relevant to this paper – call centres that are hard to tell apart from legitimate support schemes.

Cheng Chen, of the University of Victoria, Canada, recently posted a paper [32]arising from his work undercover as a paid poster for the "Internet water army". This is a team of individuals posting favourable comments on products and services they're paid to push, and unfavourable comments on competitors' products. You might think this practice sounds a little like some Tripadvisor reviews, or the effusive review that always gets posted first when a new book appears on Amazon, which just goes to show how paper-thin the distinction between legitimate marketing and marketing by misrepresentation can sometimes be.

There are quite a few unrelated scams (not necessarily primarily cyber) that will, if you use a common search engine, show massive seeding on comparison sites and forums of "good reviews" and other material explaining that "xxx is not a scam". Obviously, there's an element of index poisoning (SEO poisoning) here, but as an industry we could learn something about PR campaigns from some of these guys, if we were prepared to lift our foot from the ethical brake pedal.

This is the sort of lo-tech social engineering attack that is hard to address technologically. We suspect it's going to be best addressed by education and raising awareness, at least in the near future. (Nevertheless the scammers aren't doing themselves favours by calling the same victims time and time again, thus helping to reduce the scammable population.) While there *is* co-operation between law enforcement and the security industry, even across national boundaries, the scam still gets little official attention because it's a 'mosaic' threat like SMS fraud and fake AV: individually, the profit from a single scam is normally small, but a big enough hit rate adds 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.

References

[1] 'Fake But Free And Worth Every Cent', Robert Lipovský, Daniel Novomeský, Juraj Malcho; Virus Bulletin 2011 Conference Proceedings: http://go.eset.com/us/resources/white-papers/fake_but_free.pdf

[2] 'Problematic, Unloved and Argumentative: What is a potentially unwanted application (PUA)?', Aryeh Goretsky, 2011: http://go.eset.com/us/resources/white-papers/Problematic-Unloved-Argumentative.pdf

[3] 'Is there a lawyer in the lab?', Juraj Malcho, Virus Bulletin 2009 Conference Proceedings: http://go.eset.com/us/resources/white-papers/Lawyer_in_the_lab.pdf

[4] 'Security Software & Rogue Economics: New Technology or New Marketing?', David Harley, EICAR 2011 Conference Proceedings: http://smallbluegreenblog.wordpress.com/2011/05/15/eicar-2011-paper/

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

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

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

[8] 'Fear, uncertainty, doubt', Wikipedia: http://en.wikipedia.org/wiki/Fear,_uncertainty_and_doubt

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

[10] 'My PC has 32,539 errors: how telephone support scams really work'; David Harley, Martijn Grooten, Steven Burn, Craig Johnston, Virus Bulletin 2012 Conference Proceedings.

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

[12] 'Panic Buying', Wikipedia: http://en.wikipedia.org/wiki/Panic_buying

[13] 'How to recognize a support scam', David Harley: http://blog.eset.com/2012/04/18/how-to-recognize-a-pc-support-scam

[14] 'MS Windows Service Center Scam!- Will Infect your computer...!', 2012: http://support.emsisoft.com/topic/8092-ms-windows-service-center-scam-will-infect-your-computer/

[15] Channel 4, 2012: http://www.news4jax.com/news/Microsoft-scammers-call-computer-expert/-/475880/15395406/-/rl5m4w/-/index.html

[16] Channel 4, 2012: http://www.news4jax.com/news/-Microsoft-scam-targets-Jacksonville-customers/-/475880/14812252/-/148hwn9/-/index.html

[17] 'Fake AV Spam', David Harley, 2009: http://blog.eset.com/2009/03/18/fake-av-spam

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

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

[20]'Support Scammer Update: Misrepresenting Task Manager', David Harley, 2012: http://blog.eset.com/2012/07/02/support-scams-update

[21] 'Remote Administration Software, Wikipedia: http://en.wikipedia.org/wiki/Remote_administration_software

[22] http://www.ecrimeresearch.org/2012syncup/agenda.html

[23] 'Deactivating botnets to create a safer, more trusted Internet', Microsoft, 2012: http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/botnet.aspx

[24] 'Hanging on the telephone: Antivirus cold-calling support scams'; David Harley, Urban Schrott, Jan Zeleznak, 2011: http://go.eset.com/us/resources/white-papers/Hanging-On-The-Telephone.pdf

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

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

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

[28] http://blog.eset.com/?s=harley+%2B+support+scam

[29] Voorkom telefoonfraude op het gebied van technische ondersteuning, Microsoft: http://www.microsoft.com/nl-nl/security/online-privacy/avoid-phone-scams.aspx

[30] 'Facebook Likes and cold-call scams': David Harley, Martijn Grooten, Steven Burn, 2011: http://blog.eset.com/2011/11/09/facebook-likes-and-cold-call-scams,

[31] 'Scareware on the Piggy-Back of ACAD/Medre.A', Righard Zwienberg, 2012. (In preparation): http://blog.eset.com/?p=14193

[32] 'Battling the Internet Water Army: Detection of Hidden Paid Posters': Cheng Chen, Kui Wu, Venkatesh Srinivasan, Xudong Zhang, 2011: http://arxiv.org/abs/1111.4297