”You have a potential hacker’s infection”: A study on technical support scams

Sampsa Rauti
University of Turku
Turku, Finland
Email: sjprau@utu.fi

Ville Leppänen
University of Turku
Turku, Finland
Email: ville.leppanen@utu.fi

***Abstract*—Technical support scams have become more prevalent and turned into a profitable business. We engage 10 technical support scammers from different fake support sites via a live chat and study what kinds of actions they take once we let them control our machine over a remote connection. We then provide a qualitative analysis on the main characteristics of technical support scams that have received little scientific attention until recently.**

***Index Terms*—Scamming, Technical support scams, Remote support**

I. Introduction

Technical support scams, which have been around since 2008, are a lucrative business [3]. Innocent victims are swindled of hundreds of dollars spent on computer problems that do not actually exist. Despite several actions taken by agencies and companies like Federal Trade Commission [7] and Microsoft [1], [2], [17], the scams do not show any signs of slowing down. Ordinary Internet users lose tens of millions dollars every year because of these scams [18].

An original tactic of technical support scammers in recent years has been calling the potential victims and explaining their machine is infected. As many people have become aware of such deceit, the scammers have devised other methods to get people to contact the company supposedly providing technical support. Consequently, several ”Microsoft support” fake pages and sites telling the visitor that their system is infected have popped up. The victim is then asked to call a specific phone number or open a live chat in order to get support.

The schemes vary, but the core idea is the same in all of them: pretend to be a reliable actor associated with Microsoft or some other well-known and reliable brand, gain remote control of the victim’s machine, convince the user his or her system is in the need of cleanup or optimization and collect a payment for this ”service”.

In this study, we engage ten potential scammers and analyze their behavior while they proceed to remotely fix an alleged computer problem. This allows us to analyze how the scheme works in the cases where the user actively seeks assistance for computer problems and falls victim to a technical support scam.

There has recently been some academic interest in technical support scams [18], [8]. Still, the academic research is very new in this field. The details on scams are usually recorded by victims who recount their experiences [9], [10], [19], [21] or by antivirus companies in their blog posts [5], [16].

Miramirkhani et al. [18] present a large-scale study on technical support scams. They collect a big corpus of scams and use this statistical data to offer insights on the prevalence of the scams, the infrastructure behind them, and the evasion attempts by scammers. They also experiment interacting with scammers and report their social engineering strategies. Harley et al. [8] provide an interesting overview on the development of fake support scams and also discuss the infrastructure behind them. They also present some observations on the scam sessions, although not in a systematic way.

This paper differs from these studies by only focusing on the remote support sessions and presenting a qualitative case study with more detailed observations on smaller set of scam instances. Moreover, our study follows a scenario where a user is actively looking for support online and a live chat is used instead of telephone calls.

The rest of the paper is organized as follows. The next section gives background information on technical support scams and describes how the scam proceeds. We then cover the setting of our study. This is followed by a section discussing the observations we made during the support sessions and reporting the results. Finally, we present some concluding remarks.

II. Technical support scams

Phase 1: Attracting users

Our scenario begins with the user looking for technical support online (see Figure 1). For this purpose, the scammers have set up dozens of convincing support websites implying they have some kind of association with Microsoft or some other well-known computer brand. The user therefore lands on a fake support web page that usually prompts him or her to call a toll-free number or alternatively open a live chat with a scammer, or a ”certified technician” as they like to call themselves.

On the phone or in the live chat, the user is usually asked to describe the nature of the problem and provide a name, an email address and a phone number. He or she is then instructed to start a remote session using a remote control application such as LogMeIn Rescue and give an ID that

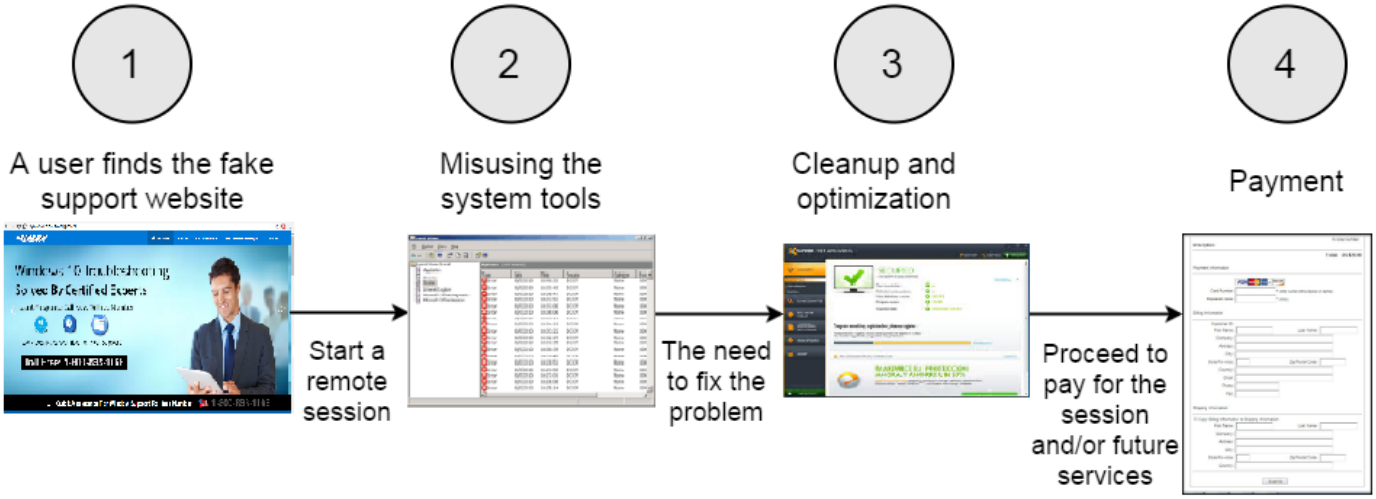


Fig. 1. The phases of a typical technical support scam.

allows the scammer to connect to the user's machine. The "support session" can now begin [16].

Phase 2: Opening a remote connection and misusing the system tools

During a remote support session, the scammer gains full control of the user's system. He or she supposedly takes a look at the problem the user has described. However, this is where the real social engineering and deception begins.

The scammers often want to demonstrate to the user that something is indeed wrong with their system. In many cases, this involves a deliberate misinterpretation of the data displayed by system tools like Event Viewer or Check Disk, for example to convince the user to believe there is a virus in the system [14], [5], [8].

Phase 3: Cleanup and optimization

Oftentimes, the scammers perform some cleanup and optimization of the system as a part of the support session, although sometimes this is offered only after the user has made the payment.

Usually the tools used are legitimate free tools downloaded from Internet. However, this is also the perfect time for a malicious scammer to slip harmful programs in the system if that is his or her objective.

Phase 4: Making the payment

Receiving a payment from the user is usually the sole purpose of the whole scam. More often than not, the user pays a fair amount of money for almost nothing. The scammer usually opens a web page in the user's browser using the remote connection and has the user fill in his or her credit card information.

III. Setting of the Study

For our experiments, we used a second-hand laptop with a clean copy of Windows 7. The system ran smoothly and it was clean of malware. We installed some programs, like Skype and Notepad++ to make the system more convincing. Likewise, we added some fake folders and files to the desktop. After each support session, System Restore utility was used to roll the system back to the previous state.

Technical support scam websites were searched using Google. Search terms such as "Windows support", "Windows 7 support", "Windows technical support", "Microsoft support" and "Microsoft technical support" were used to find fake support pages. Of course, it is impossible to draw a clear line between legitimate technical support services and scam pages. However, the following criteria were used to find web pages:

1) *Pretends to be working with a trusted company.* The page strongly implied some kind of association with Microsoft or other well-known and reliable brand. This often includes misleading domain names with "windows" in them. At the same time, however, the page usually included a small print disclaimer saying that the support service in question is a third-party service.
2) *A toll-free number.* The tech support had a toll-free number. Large companies like Microsoft usually do not provide toll-free technical support numbers.
3) *Fake testimonials.* The page contained "testimonials" from the happy "customers" that were quite apparently fake.
4) *Dubious reputation.* The web pages with bad reputation were preferred. This could not be verified for all the pages because the scammers change the domain names all the time and many pages are therefore too new to be appraised.
5) *Live chat.* We chose web pages with a live chat because this form of communication gives us more time to react and also makes taking notes easier. It is also easier to convincingly deceive the scammers on the live chat, especially as we are not native English speakers (technical support scammers usually primarily target

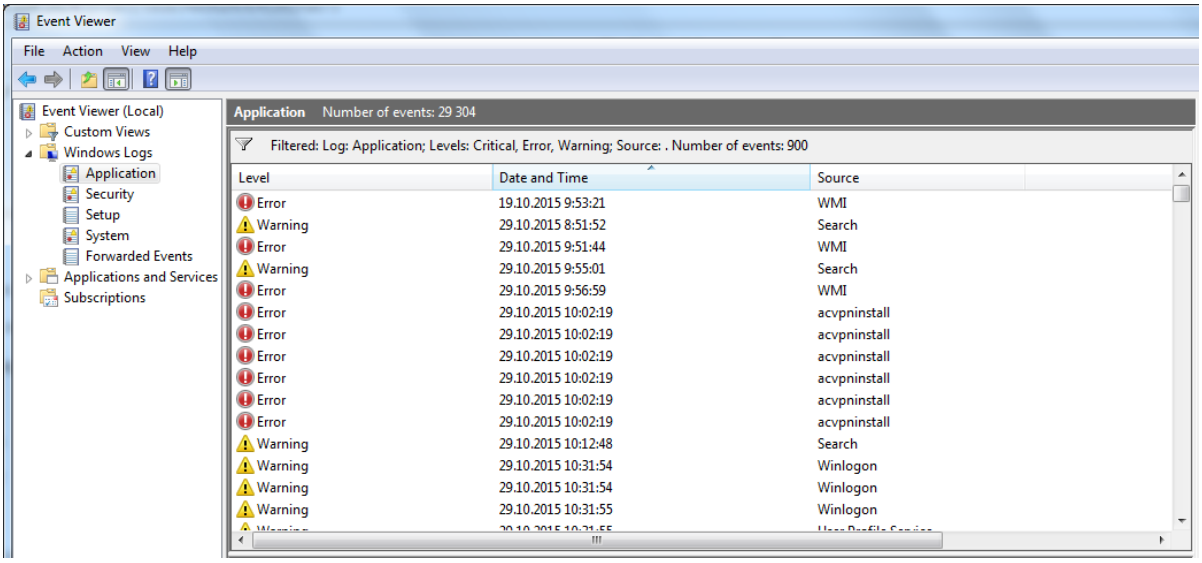


Fig. 2. The Event Viewer displaying lots of warnings and errors.

English speaking countries).

We have chosen not to list the actual malicious scam domains in this study (the information is available on request). The domain names and phone numbers the scammers use keep changing in order to avoid blacklisting. Two weeks after our experiments (on 13th April 2017), 5 of 10 sites we studied had already been shut down.

During the live chat session, when asked to state what the issue with our computer was, we told the scammers that the computer has been running slow recently (naturally, these performance problems did not really exist in the recently installed clean operating system). If asked to elaborate, we told them that applications start slowly and web pages often take a long time to load.

We pretended to be a user with only minimal knowledge about how a computer works. If the scammer gave any instructions during the remote session, we followed them. We also usually asked the scammer some questions, like whether or not our computer had a virus. This was to see if they would blatantly lie to us. Each scammer was observed and interacted with until they asked us to make a payment (or until the scammer closed the connection, as happened in one case), at which point we cut off the remote connection.

IV. Results

Phase 1: Attracting users

We first opened a live chat on the chosen scam pages. It usually took only a few minutes for scammers to respond. These ”certified technicians” always used typical English names like John, Tony, Susan or Rose as their nicknames. They always asked us to provide contact information such as a name, an email address and a phone number. The scammers then proceeded to ask ordinary questions like ”What is the issue with your machine?”, ”How old is your computer?”, ”What version of windows are you using?” and ”How long has the problem persisted?”. Finally, we were told that a technician has to take a look at our machine to fix the issue.

The script the scammers followed was very similar every time, except in one case where the scammer demanded a payment before taking a look at the computer. This could be a countermeasure against scambaiting, which has picked up some popularity recently [20]. By requesting payment in advance, the scammers do not get tricked by scambaiters (or researchers such as us!). As the support session was not initiated, we did not include this case in the study.

To form a remote connection, several different remote control applications were used. The cases included LogMeIn Rescue (in 5 cases), GoToAssist (3), Bomgar (1) and Geek-Buddy (1). These are remote support tools that are not harmful per se, although many of them have quite a bad reputation because they are so often used by technical support scammers.

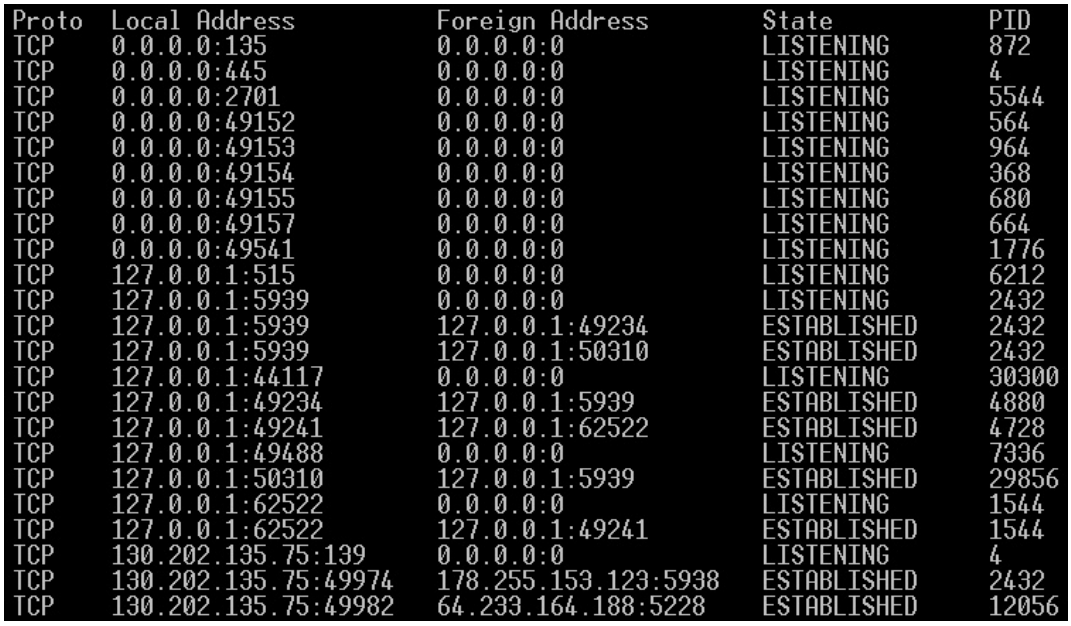
To sum up, during this phase, nothing (except for the web-sites and the scammers’ broken English) was really suspicious yet, and the service provided by ”certified technicians” still seemed quite legitimate.

Phase 2: Opening a remote connection and misusing the system tools

After the remote connection was established, most of the scammers used the system tools and in some cases applications downloaded from the internet to demonstrate to us that there are performance problems or even malicious programs on our computer.

The misinterpretations we observed included the following:

- Showing the Event Viewer’s application log to us and explaining that the large amount of errors there indicates a virus infection (see Figure 2). In reality, these are ordinary event logs that have hundreds or thousands of errors in any normal Windows machine. This particular misinterpretation seems to be a quite popular tactic in



Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	872
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:2701	0.0.0.0:0	LISTENING	5544
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING	564
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING	964
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING	368
TCP	0.0.0.0:49155	0.0.0.0:0	LISTENING	680
TCP	0.0.0.0:49157	0.0.0.0:0	LISTENING	664
TCP	0.0.0.0:49541	0.0.0.0:0	LISTENING	1776
TCP	127.0.0.1:515	0.0.0.0:0	LISTENING	6212
TCP	127.0.0.1:5939	0.0.0.0:0	LISTENING	2432
TCP	127.0.0.1:5939	127.0.0.1:49234	ESTABLISHED	2432
TCP	127.0.0.1:5939	127.0.0.1:50310	ESTABLISHED	2432
TCP	127.0.0.1:44117	0.0.0.0:0	LISTENING	30300
TCP	127.0.0.1:49234	127.0.0.1:5939	ESTABLISHED	4880
TCP	127.0.0.1:49241	127.0.0.1:62522	ESTABLISHED	4728
TCP	127.0.0.1:49488	0.0.0.0:0	LISTENING	7336
TCP	127.0.0.1:50310	127.0.0.1:5939	ESTABLISHED	29856
TCP	127.0.0.1:62522	0.0.0.0:0	LISTENING	1544
TCP	127.0.0.1:62522	127.0.0.1:49241	ESTABLISHED	1544
TCP	130.202.135.75:139	0.0.0.0:0	LISTENING	4
TCP	130.202.135.75:49974	178.255.153.123:5938	ESTABLISHED	2432
TCP	130.202.135.75:49982	64.233.164.188:5228	ESTABLISHED	12056

Fig. 3. An example output of the `netstat -ano` command displaying ”malicious connections”.

technical support scams [18], [8]. In our experiments, it happened in 2 cases.

- Pretending that `sfc /scannow` (repairing Windows system files), `chkdsk` (checking the disk for errors) or `tree` (printing a tree listing of the current directory) commands run some kinds of virus scans and explaining that our system has viruses in it. `sfc` was used in 4 cases, `chkdisk` in 2 cases and `tree` in 1 case.
- Using `netstat -ano` command and claiming every IP address in the output list is a connection let in by a virus (2 cases). In reality, the command simply shows open ports in the system but the produced listing can look confusing to a normal user (see Figure 3).
- Deceptively informing us that tracking cookies that are reported by anti-malware software (such as malwarebytes) are a sign of a serious malware infection (1 case).
- Using the processor and memory usage diagrams produced by the Windows Task Manager to imply that the computer is working slower than it should (3 cases).

It is worth noting, however, that these kinds of misinterpretations did not happen in all cases. Some of the scammers skipped this phase completely (see Table 1) and moved on to perform clean-up and optimization and subsequently request a payment. Because we were the ones who originally contacted the scammers, many of them probably found it was unnecessary to convince us that the system really needed to get fixed. This is why social engineering and misinterpretation of system tools is more often reported when the scammer is the one taking initiative – for instance in the cases in which the victim receives a cold call or a malicious advertisement is used to tell the user his or her computer is infected with malware.

An example case of Phase 2

To further illustrate how the scammers misuse system tools to deceive the user, we will briefly present a part of one support session as an example. After gaining access to our computer, the scammer first proceeded to ”scan” our system by using `netstat -ano` command on the command prompt. He or she then explained (a direct quotation, typos and grammar mistakes not removed):

> *”I deeply scan your computer using our sytem I have found out that its Infected by Posssible malwares , Junk files and Junk registries errors and warnings One of the Possible Malware found is KNCTR,Pluto Tv and weather bug, Bytefence, Malware this is software that is specifically designed to gain access or damage a computer without the knowledge of the owner. you also have a potential hackers infections where in all the informations that you typed in to your keyboard can be recorded and can be used to any fraudulent activity.”*

The scammer names many pieces of malware found in our system to make the threat more concrete and intimidating. It is quite apparent that these explanations are a part of the script that the scammer copypastes to several victims. On some occasions, the scammer even accidentally pasted the same line to us several times. The use of term ”hacker’s infection” – also included in the title of this paper – is interesting as well. The scammer does not say ”keylogger”, perhaps because this would not tell much to an ordinary user. ”Hacker’s infection”, on the other hand, sounds more menacing, even though the term is quite vague and meaningless. We can also see that the

scammer's English is broken. Many of these scammers are poor people in India forced to work in scamming business in order to make a living [4].

The scammer then opened the Event Viewer and showed us all the errors from the event logs. "Let me show you this. Do you see how many ERRORS and WARNINGS you have?" he asked dramatically. When we inquired whether this indicated there is a virus on our machine, the scammer answered "Yes" without any hesitation. He or she also explained:

> *"Those are the possible software accumulated issuses because of the infections This will make your comoputer very slow , issues opening an application , and it will also affect the stability of the computer where in your Pc might Freeze or stop working properly."*

There was no doubt at this point that our computer had a problem. Therefore it was crucial for us to purchase their product that would miraculously fix all the "issues".

It is worth noting that while the scammer in this particular support session was very eager to explain what he or she was doing and wanted to clearly demonstrate that our system had multiple malware infections, several other scammers where much more vague in their explanations and only provided any information after we asked them to.

Phase 3: Cleanup and optimization

The cleanup and optimization phase included running some completely legitimate system tools like Disk Cleanup and Disk Defragmenter and also some free tools downloaded from Internet like CCleaner and Malwarebytes. One scammer even used his or her own tailored windows batch script that cleaned up temp and log files in several locations (we checked afterwards that this script was not malicious, although it could have been).

What is more interesting, however, is that the optimization and cleanup phase is the perfect time to slip some dubious software into the unsuspecting customer's machine. According to our observations and other available reports, this is not that common as the primary purpose of technical support scams is usually attaining direct financial gain.

However, in one case the scammer brought suspicious executables into our system using the file transfer function of remote control software right before our eyes. Unlucky from the scammer's point of view, though, Avast antivirus installed on our test machine immediately reacted to this by raising an alarm. The scammer hurriedly removed the executables and also cleared the event logs of the antivirus software.

In three cases, the cleanup and optimization phase was skipped altogether. Some scammers said the optimization and cleanup would be performed after the payment. There was also one quite interesting case where the scammer wasted about 20 minutes of his or her time trying to navigate in the Windows control panel. The language of our Windows operating system was Finnish and it was apparent that he or she wanted to change the language into English. Finally, the scammer gave up and said everything would be fixed after the payment. Generally speaking, it is quite obvious many of these "certified technicians" have a very limited knowledge on the Windows operating system. Instead, they often seem to follow a ready-made script and sometimes do not necessarily even fully understand that they are scamming people.

As general public has become more aware of technical support scams and scambaiting has gained popularity, scammers have also started to be more careful of their clients. This was highlighted very well in one of the support sessions when the scammer checked the history of our Google Chrome web browser and the contents of Windows prefetch folder (that shows the applications that have been used). It was quite clearly visible that we had not visited that many web pages and not many programs had been run in our clean system. Upon noticing this, the scammer declared "You are a scammer!" and tried to set a password for our computer using `Syskey`. `Syskey` is a utility that can be set to require the user to enter a startup password (see Figure 4). Therefore, the scammer could have blackmailed money from us in exchange for the password, resembling ransomware schemes [11]. Even though the scammer probably tried to do this because we had "scammed" him or her, using `Syskey` could also be an objective of some scam sessions [12]. Other scammers did not resort to this trick, however, and generally they were not visibly suspicious of whether our system was genuine.

It is worth noting that displaying the web browsing history without permission can be seen as a serious privacy infringement. We also observed scammers looking for other information like IP address of the machine (with `ipconfig`), sniffing open connections and devices in the local network, using the `tree` command to list the directories and files in the system, and as becomes apparent in the next section, possibly collecting the customer's full credit card information and other personal details. Clearly, collecting and selling many kinds of information about the victim can also be one of the scammers' objectives.

Phase 4: Making the payment

After the cleanup and optimization phase, the scammer hopes to have convinced the user to make a payment. We consider it noteworthy that in 8 out of 9 cases that proceeded to the payment phase, the scammer asked us to pay by filling in credit card information in a form while the remote connection was kept open. This means that not only will the scammers receive a payment but they are also able to see and steal the victim's credit card information. Only in one case, Paypal was used as a payment method and the credit card information was therefore not directly divulged to the scammer. In one of the cases, the scammer said she or he would close the remote connection while the credit card information was given, but the remote control application did not indicate that such an action was ever taken. These details are not surprising, as the victim's financial information has always been an important target for scammers [15].

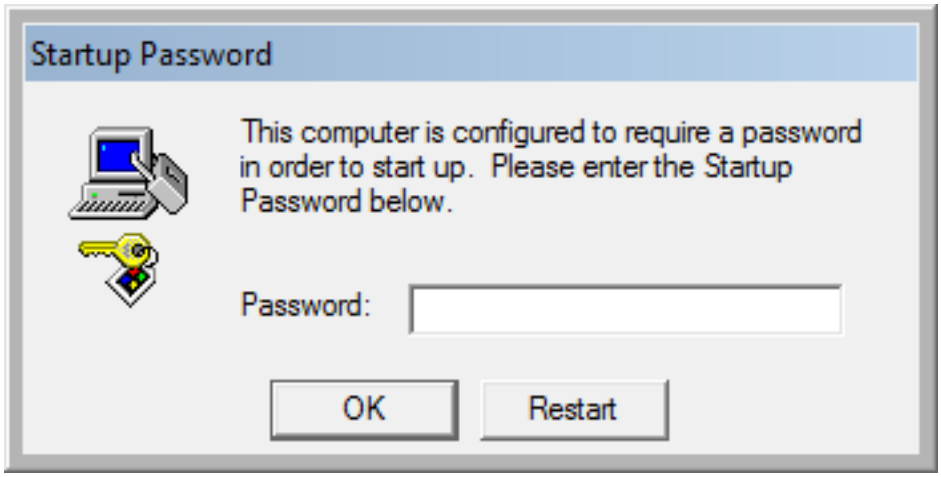


Fig. 4. A startup password set with `Syskey`.

TABLE I
THE DUBIOUS CHARACTERISTICS OF TECHNICAL SUPPORT SERVICES.

	Dubious website	Misusing tools	Privacy infringement	Tried to harm the system	Selling needlessly
Session 1	X	X	X	X	X
Session 2	X				X
Session 3	X	X			X
Session 4	X	X			X
Session 5	X	X	X		X
Session 6	X	X			X
Session 7	X	X	X		X
Session 8	X		X	X	
Session 9	X	X	X		X
Session 10	X	X			X

One time charges for fixing one incident varied from 29.99 to 89.95 dollars while longer periods of unlimited support (from 6 months to several years) usually cost several hundred dollars. Most scammers also offered support packages for several machines, naturally with additional fees. Explanations about what the service includes were usually quite vague:

> *"You will be getting unlimmited Fix, Support maintainance, Meaning whatever happens to your computer we will just fix it for you it doesent matter how many problems you might encounter .One whole year plan is $169.99 , WE also offer one time fix."*

Were these support sessions really scams?

As we never proceeded to actually make a payment, it is not really possible to estimate whether the services and applications provided after the payment were worth it or whether they were delivered at all. It is also difficult to draw a clear line between legitimate (but lousy) support service and a scam. After all, some of the "technicians" really did perform optimization and cleanup using system tools or other free tools available in the web, and maybe for some users, this service would be worth paying for already.

Still, we found all the technical support services to have at least some dubious characteristics. These findings are summarized in Table 1. In the table, a privacy infringement means prying on other private information other than credit card information (which would have been potentially stolen in 8 cases, as we have already seen). Examples include displaying browsing history or directory listings. Trying to harm the system means trying to install malware or running `Syskey`.

We see that 9 out of 10 scammers offered their products and requested a payment even though there was probably not much they could have done to speed up a system that was already quite optimized and clean. Granted, we had implied the computer is sometimes slow (as a way to engage the scammer in the first place), but a proper "certified technician" still should make sure what the state of the system is. In all sessions that proceeded to the payment phase, we were quite clearly told that purchasing the product would be advantageous for us.

We also saw that many of the scammers potentially stole private data like credit card numbers, lied about the meaning of the system tools, installed malware in the system (by installing malware or running `Syskey`), and had broken English even though they claimed to work in the USA. Moreover, as we

already mentioned, we only chose services claiming to have some connection to Microsoft or some other trustworthy brand, had a dubious reputation and a toll free number. 5 of 10 websites also disappeared in two weeks after our experiments. We think having several of these characteristics definitely place these support providers in the scam category, or at the very least in a gray area.

V. Conclusions

We have presented a qualitative analysis on technical support scams and discussed many of their distinctive characteristics. We concentrated on a scenario where the user goes online to look for help and finds a page claiming to provide technical support.

The scams in our study thus differ from the usual cold calls where the scammer calls the user and says that a virus has been detected in his or her system. The scam cases we encountered also clearly differ from the current trend of malvertisements (malicious advertisements) informing the user his or her machine is infected and immediate action is required [13]. Compared to these two schemes, the sites we chose were less aggressive.

Still, the actual support sessions seem to have similar aspects in all schemes. The sessions are questionable and involve misleading communication, finding issues that do not exist in the first place, and often involve serious infringement of the users' privacy. Some scammers also cause serious harm to the machine by installing malware or locking the system. At the very least, the scams involve semi-fraudulently selling products and services that do not provide much value to the user [6].

It might be interesting to study approaches that automatically recognize the common patterns in technical support sessions and warn the user of the potential danger. However, it appears this kind of social engineering is difficult to prevent technologically. Therefore it is important to educate the general public about the danger of technical support scams (see also [18]).

This kind of awareness raising should be possible for most users. For example, scam sites can be quite easily identified with some awareness on the topic. Suspicious and ambiguous characteristics like claiming to be from Microsoft but at the same time proclaiming itself to be a third party service in a small print are not that difficult to spot when one is aware of this possibility. Generally, because of their lo-tech nature, identifying technical support scams does not require that much technical know-how from the user compared to other threats.

Acknowledgment

The authors gratefully acknowledge Tekes – the Finnish Funding Agency for Innovation, DIMECC Oy and Cyber Trust research program for their support.

References

[1] C. Arthur. Microsoft drops partner accused of cold-call scam. https://www.theguardian.com/technology/2011/sep/22/microsoft-drops-partner-accused-scam. Accessed: 2017-04-13.

[2] B. Bright. Bing bans tech support adsbecause theyre mostly scams. https://arstechnica.com/information-technology/2016/05/bing-bans-tech-support-adsbecause-theyre-mostly-scams/. Accessed: 2017-04-13.

[3] J. Brodkin. A neverending story: PC users lose another $120M to tech support scams. http://arstechnica.com/information-technology/2014/11/ ftc-windows-tech-support-scams-tookanother-120-million-from-pc-users/. Accessed: 2017-04-04.

[4] J. Brodkin. Hello, I'm definitely not calling from India. Can I take control of your PC? https://arstechnica.com/tech-policy/2012/10/hello-im-definitely-not-calling-from-india-can-i-take-control-of-your-pc/. Accessed: 2017-03-27.

[5] O. Cox. Technical Support Phone Scams. https://www.symantec.com/connect/blogs/technical-support-phone-scams. Accessed: 2017-03-27.

[6] R. Cringely. Tech support or extortion? You be the judge. http://www.infoworld.com/article/2619722/cringely/tech-support-or-extortion–you-be-the-judge.html. Accessed: 2017-04-13.

[7] FTC. FTC Obtains Court Orders Temporarily Shutting Down Massive Tech Support Scams. https://www.ftc.gov/news-events/press-releases/2014/11/ftc-obtains-court-orders-temporarily-shutting-down-massive-tech. Accessed: 2017-04-04.

[8] D. Harley, M. Grooten, S. Burn, and Johnston C. My PC has 32,539 errors: how telephone support scams really work. In *Virus Bulletin Conference*, 2012.

[9] T. Hunt. Scamming the scammers catching the virus call centre scammers red-handed. https://www.troyhunt.com/scamming-scammers-catching-virus-call/. Accessed: 2017-03-27.

[10] C. Johnston. 'Hello, I'm from Windows and I'm here to help you'. https://www2.virusbtn.com/virusbulletin/2011/01/hello-i-m-windows-and-i-m-here-help-you/. Accessed: 2017-04-13.

[11] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda. *Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks*, pages 3–24. Springer International Publishing, 2015.

[12] B. Krebs. Microsoft Partner Claims Fuel Support Scams. https://krebsonsecurity.com/2014/11/microsoft-partner-claims-fuel-support-scams/. Accessed: 2017-04-13.

[13] Zhou Li, Kehuan Zhang, Yinglian Xie, Fang Yu, and XiaoFeng Wang. Knowing your enemy: Understanding and detecting malicious web advertising. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, pages 674–686. ACM, 2012.

[14] N. Lodhi. Beware of Microsoft Tech Support Scammers. http://www.business2community.com/tech-gadgets/beware-microsoft-tech-support-scammers-0755581. Accessed: 2017-04-13.

[15] F. Maggi. Are the con artists back? a preliminary analysis of modern phone frauds. In *10th IEEE International Conference on Computer and Information Technology*, pages 824–831, 2010.

[16] Malwarebytes. Tech Support Scams Help & Resource Page. https://blog.malwarebytes.com/tech-support-scams/. Accessed: 2017-03-27.

[17] Microsoft. Microsoft takes action against tech support scammers. https://blogs.microsoft.com/on-the-issues/2014/12/18/microsoft-takes-action-tech-support-scammers. Accessed: 2017-04-04.

[18] N. Miramirkhani, O. Starov, and N. Nikiforakis. Dial one for scam: A large-scale analysis of technical support scams. In *The Network and Distributed System Security Symposium*, 2017.

[19] Z. Whittaker. We talked to Windows tech support scammers. Here's why you shouldn't. http://www.zdnet.com/article/why-you-should-never-talk-to-windows-tech-support-scammers/. Accessed: 2017-04-04.

[20] Wired. A guide to trolling a tech support scammer . http://www.wired.co.uk/article/how-to-troll-a-scammer. Accessed: 2017-03-27.

[21] L. Zetser. Conversation With a Tech Support Scammer . https://zeltser.com/tech-support-scammer-conversation/. Accessed: 2017-04-04.