Dial One for Scam: Analyzing and Detecting Technical Support Scams

Najmeh Miramirkhani, Oleksii Starov, Nick Nikiforakis
Department of Computer Science, Stony Brook University
n.miramirkhani@stonybrook.edu,
{ostarov, nick}@cs.stonybrook.edu

Abstract

In technical support scams, cybercriminals attempt to convince users that their machines are infected with malware and are in need of their technical support. In this process, the victims are asked to provide scammers with remote access to their machines, who will then "diagnose the problem", before offering their support services which typically cost hundreds of dollars. Despite their conceptual simplicity, technical support scams are responsible for yearly losses of tens of millions of dollars from everyday users of the web.

In this paper, we report on the first systematic study of technical support scams and the call centers hidden behind them. We identify malvertising as a major culprit for exposing users to technical support scams and use it to build an automated system capable of discovering, on a weekly basis, hundreds of phone numbers and domains operated by scammers. By allowing our system to run for more than 8 months we collect a large corpus of technical support scams and use it to provide insights on their prevalence, the abused infrastructure, and the current evasion attempts of scammers. Finally, by setting up a controlled, IRB-approved, experiment where we interact with 60 different scammers, we experience first-hand their social engineering tactics, while collecting detailed statistics of the entire process. We explain how our findings can be of use to law-enforcing agencies and propose technical and educational countermeasures for helping users avoid being victimized by technical support scams.

1. INTRODUCTION

Social engineering involves the psychological manipulation of a person to perform actions that are harmful, either to the person being manipulated, or to the organization that the person belongs to. In the context of computer security, attackers use social engineering to exfiltrate sensitive information from users, such as their credentials, and convince users to perform actions, such as executing an email attachment, that directly benefit an attacker. Despite the conceptual simplicity of social engineering, it is still one of the most popular ways of gaining access to protected resources [38,43].

A recent and understudied social engineering attack targeting everyday web users is a *technical support scam*. In a technical support scam, a webpage created by the scammer tries to convince users that their machines are infected with malware and instructs them to call a technical support center for help with their infection. The victimized users will then willingly provide remote access to their machine and, if the scammer successfully convinces them that they are indeed infected, pay the scammer a malware-removal fee in the range of hundreds of dollars. This scam has become so prevalent that the Internet Crime Complaint Center released a Public Service Announcement in November 2014 warning users about technical support scams [18].

Even though this type of scam costs users millions of dollars on a yearly basis [5,18], there has been no systematic study of technical support scams from the security community. Thus, while today we know that these scams do in fact take place and that scammers are successfully defrauding users, any details about their operations are collected in an unsystematic way, e.g., by victimized users recalling their experiences, and antivirus companies analyzing a handful of scams in an ad-hoc fashion [17,27,28].

In this paper, we perform a three-pronged analysis of the increasingly serious problem of technical support scams. First, we build a reliable, distributed crawling infrastructure that can identify technical support scam pages and use it to collect technical support scam pages from websites known to participate in malvertising activities. By deploying this infrastructure, in a period of 250 days, we discover 8,698 unique domain names involved in technical support scams, claiming that users are infected and urging them to call one of the 1,654 collected phone numbers. To the best of our knowledge, our system is the first one that can automatically discover hundreds of domains and numbers belonging to technical support scammers every week, without relying on manual labor or crowdsourcing, which appear to be the main methods of collecting instances of technical support scams used by the industry [27,28].

Second, we analyze the corpus of collected data and find multiple patterns and trends about the techniques used and the infrastructure abused by scammers. Among others, we find that scammers register thousands of low-cost domain names, such as, `.xyz` and `.space`, which abuse trademarks of large software companies and, in addition, abuse CDNs as a means of obtaining free hosting for their scams. We trace the collected phone numbers and find that while 15 different telecommunication providers are abused, four of them are responsible for 93.5% of the numbers. We show that scammers are actively evading dynamic-analysis systems located on public clouds and find that, even though the average lifetime of a scam URL is approximately 11 days, 43% of the domains were only pointing to scams for less than 3 days. Moreover, we identify potential campaigns of technical support scams, their unique characteristics, and estimate their life time finding that 69% of scam campaigns have a lifetime of less than 50 days, yet some survive for the entire duration of our experiment.

Third, we obtain permission from our IRB to conduct 60 sessions with technical support scammers, where we call the numbers discovered by our distributed infrastructure and give scammers access to disposable virtual machines, while recording the entire session. By interacting with scammers for over 22 hours and analyzing the collected data, we calculate precise statistics about the abused tools, the utilized social engineering techniques, and the requested charges. Among others, we find that scammers are patient (average call duration is 17 minutes), abuse a limited number of remote administration tools (81% of all scammers used one of two software tools), charge victims hundreds of dollars (average charge is $290.9), and are creative in their ways of convincing users that their machines are infected with a virus (more than 12 different techniques utilized). Moreover, we use a large number of volunteers to estimate the size of call centers operated by scammers and find that the average call center is housing 11 technical support scammers, ready to receive calls from victims.

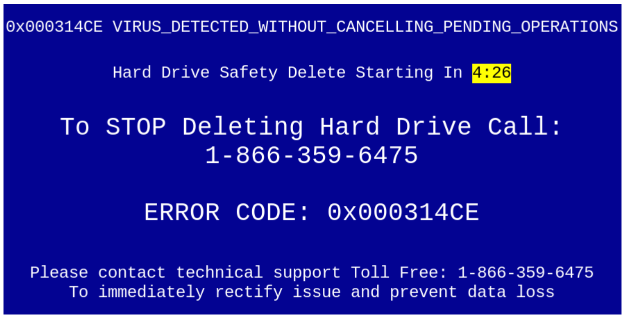
Finally, we explain why educating the general public about technical support scams should be easier than educating them about other security issues, and propose the development of an, in-browser, "panic button" that non-technical users would be educated to use when they feel threatened by the content of any given webpage.
Our main contributions are:

- We design and develop the first system capable of automatically discovering and collecting domains and phone numbers operated by technical support scammers.
- We perform the first systematic analysis of technical support scam pages and identify their techniques, abused infrastructure, and campaigns.
- We interact in an ethical and controlled fashion with 60 scammers and collect intelligence that can be used for both technical countermeasures as well as public education.
- We make a series of propositions for educating the public about technical support scams and for protecting users from abusive pages.

2. BACKGROUND

A technical support scam begins with a user landing on a page claiming that her operating system is infected with malware. Pages hosting technical support scams typically abuse logos and trademarks of popular software and security companies, or operating system UIs, to increase their trustworthiness. Figure 1 shows an example scam page. Instead of requesting from users to download software, as typical scareware scams did in the past [39], these scams request from the user to call a support center for help with their infection. The posted number is often a toll-free number which is clearly used to increase the chances that a user would actually dial it. Finally, the page is using intrusive JavaScript techniques in order to make it hard for the user to navigate away, such as, constantly showing `alert` boxes that ask the user to call the technical support number, and hooking into the `onunload` event, which is triggered when the user attempts to close the current browser tab, or navigate away from the current website.

Once a user calls the listed number, she will eventually reach a person requesting access to her machine in order to diagnose the problem. The user is instructed to download remote desktop software and allow the remote "technician" to connect to her machine. After connecting, the scammer, unfortunately, has full control over the user's machine. The scammer will then proceed to demonstrate the infection by showing errors and supposed problems that, in reality, are typical of any Windows installation. As soon as the scammer realizes that the user is convinced, he will then offer to fix the problem for a fee, typically in the range of hundreds of dollars which the user is asked to pay by giving her credit card number to the scammer. As one can clearly understand, the above scenario will, at best, result in the user paying hundreds of dollars for unnecessary services. At worst, the scammer can keep charging the credit card until the limit is reached, install malware and keystroke loggers on the user's machine, and use them to exfiltrate the user's private and financial information.



```
0x000314CE VIRUS_DETECTED_WITHOUT_CANCELLING_PENDING_OPERATIONS

Hard Drive Safety Delete Starting In 4:26

To STOP Deleting Hard Drive Call:
1-866-359-6475

ERROR CODE: 0x000314CE

Please contact technical support Toll Free: 1-866-359-6475
To immediately rectify issue and prevent data loss
```

Figure 1: *Screenshot of a technical support scam which mimics a Windows blue-screen-of-death to increase its trustworthiness.*

3. DATA COLLECTION AND ANALYSIS

In this section, we describe the design and implementation of Robovic, our tool for the automated discovery and collection of technical support scam pages.

3.1 Source of technical support scam pages

Even though technical support scams are a known phenomenon, the exact details of how a user ends up on a technical support scam page are less known. In order to study this phenomenon, we need access to a steady stream of URLs with high toxicity, similar to the needs of dynamic analysis frameworks for the detection of drive-by downloads [21].

We argue that most users are exposed to malicious content via malvertising. The constant stream of news of malvertising detected on popular websites [10, 24, 33], and the constant crackdown (and promises of crackdown) from advertising networks [4, 14, 15] make this clear. Therefore, even though a scammer could, in theory, try to lure individual users to click on direct links towards his scam pages, this behavior will not only result in a reduced number of victims but also in the faster identification and thus takedown of the malicious page. The natural non-determinism of advertising networks and the ability to trace the provenance of the current visitor, provide ample opportunities for scammers to reveal themselves to victims while hiding from search engines and security researchers.

In this paper, we take advantage of the results of specific recent studies which found that two types of services, namely, *domain parking* and *ad-based URL shorteners*, engage in malvertising practices that endanger users.

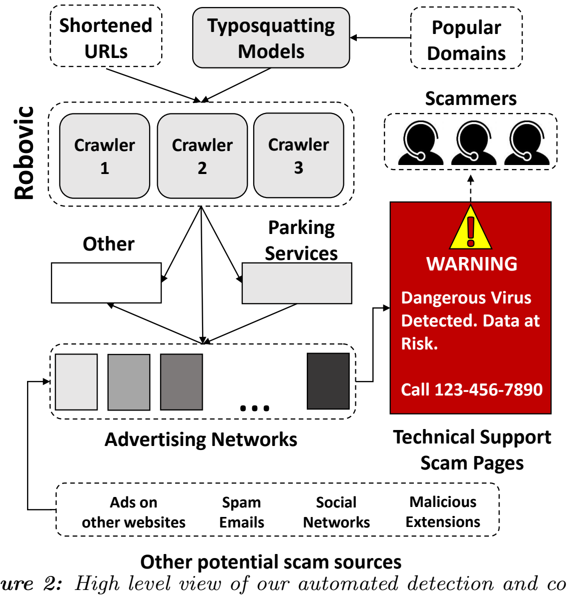


Figure 2: *High level view of our automated detection and collection tool of technical support scams (Robovic) and its interaction with the technical support scam ecosystem*

Domain Parking. Domain parking companies compile portfolios of tens of thousands of underdeveloped domain names which they use to show ads to the landing users. If a user clicks on an ad, the domain parking company will then, presumably, give a portion of the advertising profit to the owner of the unused domain. Apart from hiding advertising profits from the domain owners [2], many domain parking companies have been found to collaborate with dubious advertising networks which do not hesitate to occasionally redirect a user to a page with malware. In fact, Vissers et al., while researching the types of ads that users who land on parked websites are exposed to, discovered two pages which fit our definition of a technical support scam [44]. To find a sufficient number of parked domains that our crawlers can visit, we take advantage of the fact that prior research has shown that domain parking is the favorite monetization method of domain squatters [1,12,22,30,40,46]. Therefore, as long as we visit typosquatting variants of popular domain names, such as `twwitter.com` (note the duplication of the "`w`" character), the majority of our visits will end up on domain parking companies which will redirect a fraction of these visits to technical support scams.

Ad-based URL Shorteners. Ad-based URL shorteners are services that allow the users who shorten URLs to make a commission every time that other users visit their shortened URLs. Instead of immediately redirecting the short-URL-visiting users, ad-based URL shorteners force users to see an ad for a few seconds, before they can proceed to the intended, "long", URL. Nikiforakis et al. studied the ecosystem of ad-based URL shortening services and their ad-delivery methods [31], finding a large percentage of malvertising.

Generality of our approach. Note that we are not claiming that scammers explicitly collaborate with either domain-parking agencies, or ad-based URL shorteners. Instead, we use these two services as our gateway to malicious advertising, rather than as a method for identifying specific advertisers. As such, we argue that our methodology will be able to detect, with equal probability, all scammers that are using advertising as a way of attracting victims.

3.2 Tool design and implementation

Our tool for discovering and recording technical support scams is called Robovic (Robotic Victim). Our main objective is to collect as much data as possible about this highly profitable underground business, in order to conduct a systematic study of technical support scams and analyze their unique characteristics. At the same time, a necessary condition for gathering technical-support-related data is the development of a reliable and highly available infrastructure, that will provide us with enough uptime to be able to study temporal properties of technical support scams. Figure 2 shows the high-level view of Robovic, the high-toxicity, input streams of URLs, and the interactions of our tool with the technical support scam ecosystem. We describe Robovic's core components (Crawler, Liveness Checker, Detector) below:

Crawler. The Crawler is in charge of browsing and collecting data for the given set of URLs and recording information about the resulting pages. To address the requirements of our study, we extended OpenWPM which is a generic web privacy measurement platform [13]. More specifically, we implemented a custom browser extension to instrument the browser so that specific native JavaScript functions, like the aforementioned `alert` function, would be overwritten before loading a page, in a way that allows us to record the frequency of calls and exact messages displayed to users. In addition, our browser extension ensured the modification of the browser's user-agent properties to match a typical user browsing the web using a Microsoft Windows OS. Robovic uses a MITM proxy to record requests and responses, clicks on pop ups and logs the HTML code of all the nested iframes, the final URL, the text shown in alert boxes and the functions used in commonly abused event handlers, such as, the `onunload` handler, as well as a screenshot of the page. Finally, given the adversarial nature of technical support scam pages, e.g., the locking of a user's browser via the constant use of the JavaScript-accessible, browser-provided `alert` function, we developed our crawler in such a way that allows it to interact with these pages but not get trapped by them.

We deployed the Robovic Crawler on three different sites (our campus, Amazon's Elastic Compute Cloud [3], and on Linode's cloud [25]). We provided each instance with the same set of 10,000 possible typosquatting domains, which we obtained by applying the typosquatting models of Wang et al. [46] on the top 200 websites according to Alexa, and a set of 3,000 shortened URLs belonging to ten popular ad-based URL shorteners. The crawler instances initiate the crawling process at the same time each day and collect and store all the aforementioned data. Note that Robovic was originally relying just on domain parking in order to find technical support scams and we incorporated ad-based URL shorteners later in our study. We denote the exact date while analyzing the data in Section 4.

Detector. The Detector Module identifies the pages that are the most likely to be technical support scams based on a set of heuristic rules. We examined several heuristics, such as, having a redirection chain, showing consecutive `alert` dialogues, the presence of a phone number, and the presence of special keywords. After observing approximately a week's worth of collected data, we designed our heuristic which minimized false negatives and false positives as follows: If a page has any kind of popup dialogue, we check its content using an empirically constructed decision tree and based on the presence of carefully chosen sets of keywords, we score the page and mark it as malicious if the score is higher than a tuned threshold.

To gauge the accuracy of our heuristic, we use random sampling to select three days (from the 250 days that are crawlers are active) and manually analyze all page screenshots collected by Robovic (17K screenshots), during those days. Through this process, we verified that our heuristic was able to capture *all* technical support scams collected by Robovic. Interestingly, we identified some scam pages that would use HTML to draw fake alert boxes when a user visited them. Our heuristic, however, can still detect them as they switch back to the native JavaScript alerts when the user attempts to navigate away from the page (aiming to trap the user on the same page). This manual inspection makes us confident that our heuristic can account for most, if not all, of the technical support scams that Robovic was exposed to during the monitored period.

Liveness Checker. The Liveness Checker is the final component of Robovic which is responsible for tracking the lifetime of a scam page after it first appears in the crawler's feed. Every URL that the Liveness Checker receives from the Detector component, is added in a database of URLs that will be crawled on a daily basis. In addition, for every URL received, the Liveness Checker computes neighboring URLs that could be hosting a technical support scam page, e.g., removing GET parameters from a URL and iteratively reducing the resource-path until we reach the main page of a domain. On any given day, a scam is considered to be "alive" if any of the above URLs responds with a page that matches our aforementioned scam-page heuristic. The lifetime of any given scam domain is the longest time period, in terms of days, that begun and ended with a page marked as a technical support scam. We chose this definition to account for transient errors (support scam goes offline for one day) and for malvertising variance (same domain can first show a support scam, then a survey scam [7], and then again a support scam).

4. DATA ANALYSIS

In this section, we report on the data collected by Robovic during a 36-week period, starting from September 1, 2015. Robovic attempted to resolve 8.4 million domains and collected a total of 15TB worth of crawling data.

4.1 Discovered scams

Of the 5 million domains resolved by Robovic, 22K URLs were detected as technical support scam pages, belonging to 8,698 unique domains. Figure 3 (top) shows the weekly number of unique domains found by each of our three deployed Robovic instances during our data-collecting period. One can see that, as time passes, technical support scams are becoming increasingly common reaching more than 1,000 unique domains per week in April and May 2016. Interestingly, the number of phone numbers cannot keep up with that growth, suggesting that curbing the abuse of phone numbers will have a significant effect on technical support scams.

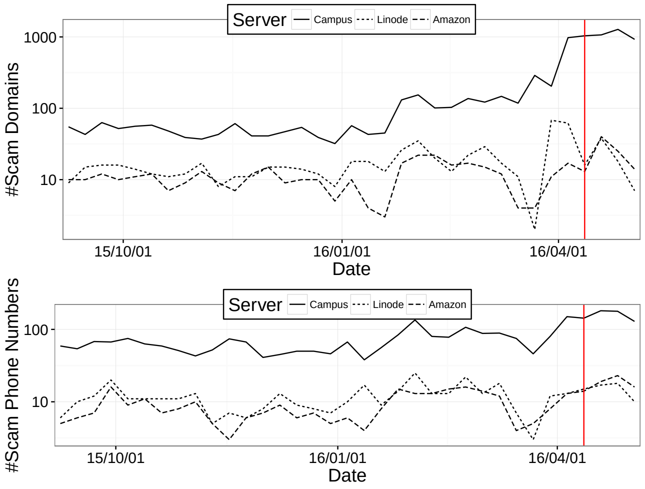


Figure 3: *Number of unique weekly technical support scam domains (top) and phone numbers(bottom) recorded by each* Robovic *instance during our 36-week monitored period. The vertical line denotes the week on which we adopted an extra source of malvertising pages, namely, that of shortened URLs.*

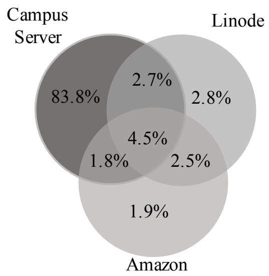


Figure 4: *Venn diagram of Unique Phone Numbers Detected by* Robovic *instances*

Another visible pattern is the great difference between the number of scam domains to which our campus-residing Robovic was exposed, compared to the Robovic instances located on Amazon's and Linode's hosting clouds. Since all crawlers were asked to crawl the same domains and none of the three Robovic instances experienced any downtime during our monitored period, the only reasonable explanation is that the dubious advertising networks responsible for redirecting a user from a typosquatting page to a technical support scam page are using a user's IP address as a way of straightforwardly evading crawlers located on popular commercial clouds.

An alternative way of looking at the unique scam domains discovered, is to consider the individual coverage of each of our three Robovic instances. In terms of domain names, our campus-residing Robovic, discovered 95.7% of the domain names discovered by all three instances, with the Linode- and Amazon-residing Robovic instances, contributing only 7.6% of the overall unique domains. Similarly, the same campus-residing Robovic instance, by itself, discovered 92.8% of the total number of unique telephone numbers (see Figure 4). Overall, our results indicate that, because attackers are location-aware, proxy-less servers located on popular commercial clouds, have only a small contribution in the discovery of scam pages and phone numbers.

Figure 3 (bottom) shows the number of unique telephone numbers discovered each day and exhibits a similar behavior as Figure 3 (top). Comparing the two figures together, one can see that while telephone numbers and domains are clearly correlated, the relationship between the two is not a 1-to-1 relationship. The reason for this is that scams located on different domains can be showing the same phone number, as well as the phone number on any given page can change between page loads. By inspecting some of the JavaScript code located in such pages, we found evidence of "on-the-fly", phone-number delivery. Specifically, we discovered snippets of JavaScript code which would read browser properties (operating system, user agent, and language) and send these to a remote host which responded with a JSON file containing a telephone number. A snippet of this code is shown in Figure 5. We consider this as evidence that the technical support scam ecosystem can be fairly elaborate, where the scammers that set up the pages and show the telephone numbers are not necessarily the same ones that are answering the phone.

Lastly, by analyzing the data collected by the Liveness Detector module of ROBOVIC, we discovered that the lifetime of scam domains forms a long-tail distribution. Specifically, 27% of the domain names are reachable only for a single day after they are first discovered by ROBOVIC, while 43% of the domains are reachable for up to three days. At the same time, 7% of the discovered domains were reachable for more than 40 days indicating that these are successful in avoiding unwanted attention and take-downs.

4.2 Relationship of domains and numbers

Of the total 8,698 unique scam domains collected by ROBOVIC, 17% are completely human readable making extensive use of words that either imitate a legitimate brand, or attempt to scare the victim. The five most frequently used words in domains were: `techsupport`, `alert`, `pc`, `security`, and `windows`. 83% of the domains contained at least one random string and 6% belonged to Content Delivery Networks (CDN) such as CDN77, CDNsun, KeyCDN, and MetaCDN.

Although the primary goal of CDNs is to provide high availability of static content, scammers abuse them as a way of obtaining free or near-free hosting for their scam pages. Content Delivery Networks, such as, CDN77, CDNsun, and KeyCDN offer free services without requiring a phone number or a credit card. In addition, every uploaded scam page gets its own random-string-including URL which can not be guessed and thus cannot be preemptively blacklisted (blacklisting the entire CDN-controlled domain would cause collateral damage).

Technical support scam domains are unusually long. A t-test on the distribution of domain length of 8K scam domains (with an average length of 76±56) and the top 8K Alexa domains (with an average length of 12±3.5) results in a very small p-value ($p<0.05$) which indicates that the difference is significant. By inspecting a sample of the scam pages hosted on long scam domains, we found that scammers make use of long domains to, among others, evade the built-in mechanism of the browsers for suppressing pop-ups. We discuss these techniques further in Section 4.3.

The set of collected scam domains, after removing CDN entries, maps to 1,524 TLD+1 domains resolving to 685 unique IP addresses. This reduction in the size of hosting providers, confirms the use of shared-hosting as a way of getting cheap domains and hosting which can be easily changed to evade blacklisting. The majority of scam-page hosting is done in the US (88%), followed by a long tail of various countries, such as, India and Netherlands. While India is not an obvious hosting choice, we show that many scammers seem to be operating out of it (Section 5). We also mapped the IP addresses to AS names and found that 18% of the scam hosts are using Cloudflare to hide their hosting server.

```
var ran = false;
function loadNumber() {
  if (!ran) {
    //Default numbers in case script fails
    var default_number = "(877) 292-3084";
    var default_plain_number = "8772923084";

    //Initiates new instance of specific campaign
    var campaign = new Callpixels.Campaign({campaign_key:
          '43019bb72cd5ecc4e3b33902645dd4d6'});

    //Script collects information about the user and the
         affiliate ID of the scammer
    var tags = {};
    var source_host = 'https://gyazo.com/71487046
         b835616428700b7ce5f34915';
    var affiliate_id = '1';
    var clickid = 'Rb10lsa0kY';
    var browser = 'Firefox';
    var browserversion = '25.0';
    var country = 'US';
    var os = 'Windows';
      [..]
    //Populates an object with the gathered information
    tags = {
      a: affiliate_id,
      clickid: clickid,
      source_url: source_host,
      browser: browser,
      browserversion: browserversion,
      country: country,
      os: os,
      [...]
    };
    //Function that retrieves a dynamic number
    campaign.request_number(tags,
      function (matching_number) {
        //Stores the dynamic number in global variable
        number = matching_number.get('formatted_number');
        plain_number = matching_number.get('plain_number'
             );

        window.callpixels_number = matching_number;
      },
      function (error) {
        number = default_number;
        plain_number = default_plain_number;
      }
  );
  ran = true;
  //Shows the new number to victim user
  var number = "1 "+number;
  FormattedNumber1.innerHTML = number;
  [...]
}
window.onfocus = loadNumber();
```

Figure 5: *Partial JavaScript code that shows the dynamic fetching of a toll-free number based on the current victim's attributes, and the fallback logic in case the dynamic fetching fails.*

Since phone numbers are a crucial part of technical support scams, we used a public database of toll-free numbers [41] to get more information about them. There, we discovered that even though the 1,654 toll-free numbers belong to 15 different telecommunication providers, 93.5% belong to only four providers (Twilio, WilTel, RingRevenue, and Bandwidth) which indicates that scammers are abusing some providers

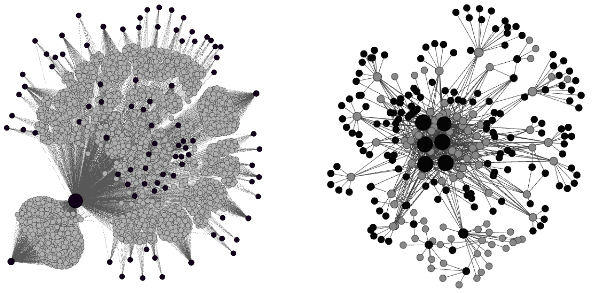


Figure 6: Two samples of technical support scam campaigns. The left graph shows the relationships between unique domains and phone numbers. The right graph shows the relationship between unique, TLD+1 domain names and phone numbers. Black and gray nodes represent phone numbers and domain names/TLD+1 domains respectively and size of a node is proportional to the node degree.

significantly more than others. Moreover, we discovered 77.5% of the phone numbers were activated less than one year ago and none of the vanity terms associated with the collected numbers is related to tech support.

To gain insights on the N-N relationship between scam domains and phone numbers appearing on scam pages, we plotted their network graph. In this graph, an undirected edge between a domain name and a phone number exists, if the phone number was advertised by the domain name during the time period of our experiment. The resulting graph contains 582 connected components of various sizes, of which 216 connected components have more than 5 nodes. A sample of the connected components is depicted in Figure 6 (left). As one can notice, the same numbers are reused across a set of domain names and, vice-versa, a domain may advertise different phone numbers over its lifetime.

To identify connected components which are more representative of scam campaigns, we merge the domain nodes that have the same TLD+1 domain name and replot the network graph. The new graph contains 434 connected components while the phone nodes and domain nodes have an average degree of 2.8 and 2.5 respectively. The maximum degree of phone nodes is 173, and the maximum degree of domain nodes is 34. One sample of a connected component in this graph which represents a technical support scam campaign is plotted in Figure 6 (right). One interesting characteristic of this subgraph is that the center six phone numbers are connected to almost all of the campaign's domain names. After investigating these specific scam pages, we discovered that these numbers are the default numbers that would be used by the scam page in case an error happens during the on-the-fly retrieval of a new phone number.

We estimate the life time of scam campaigns by adding timestamps to the nodes of the network graph. We define the lifetime of a campaign as the difference between the timestamps of the first and last domain or phone number joined to the subgraph of the campaign. As Figure 8 shows, the distribution of campaigns' lifetime is not normal and 69% of the campaigns have a lifetime of less than 50 days. Even though the average lifetime is 45 days, there are campaigns with a life time of more than 250 days (the whole duration of our experiment). Moreover, assuming that the size of a campaign is equal to the size of its graph, there is a positive correlation (r=0.5) between the lifetime of a campaign and its size. We can, therefore, conclude, that larger technical support campaigns tend to be active for a longer time.

Table 1: Characteristics of the top five campaigns. D: Domains, P: Phone numbers

#D	#P	TLDs	Prefixes	#IPs	#ASs	Country	Top AS or CDN	Lifetime (days)
3714	93	net, com	855, 844, 888, 877	35	3	US,NL	CloudFlare	64
513	96	biz, net, com, in, us, xyz, space, website, info, club , online, me, cf, ga, org, co, tk, ca, site	844, 877, 855, 866, 888, 800	93	20	US,IN, FR	Cloudflare, GoDaddy	250
173	359	space, info, com, org, net	888, 855, 844, 877	42	7	DE,FR,US	cdn77, cdnsun, metacdn, keycdn	235
145	164	info, help, online, website, com, xyz, in, net	888, 844, 877, 855, 800, 866	33	9	US, IN, NL	Amazon	185
68	15	net, com, org, info	844,888	1	1	US	1 and 1	250

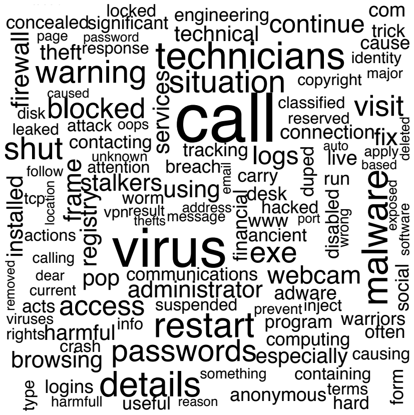


Figure 7: Word cloud based on the text contents of the gathered technical support scam pages

Finally, Table 1 shows the characteristics of the five largest campaigns and their estimated lifetime. As one can notice, the set of toll-free prefixes, TLDs and hosting infrastructure differs among campaigns with the two first campaigns, besides having rich and diverse infrastructures, hiding their hosting servers behind Cloudflare. One can also see that many of these campaigns use cheap TLDs, such as, .xyz, .space and .club, to generate many variations of scam domains.

4.3 Page contents

Scammers use specific words in the content of a scam page to convince the users that their machines are infected with a virus. Figure 7 shows the most frequent words used in the scam pages in the form of a word cloud, where size of each word is correlated with the number of times it appeared in our collected corpus of technical support scam pages.

Next to the specific words, scammers also abuse browser APIs to increase the effectiveness of their scams. In Section 2 we discussed how scammers abuse alert dialogues to make it hard for users to navigate away. At the same time, we are aware of the fact that many browsers give users the ability to suppress alert dialogues, if a page is abusing them. For instance, in Google Chrome, if a page uses two back-to-back alert dialogues, the browser adds to the second alert dialogue, a checkbox that the user can check to "Prevent this page from creating additional dialogs." 49% of the collected scams were using very long alert messages, padded with

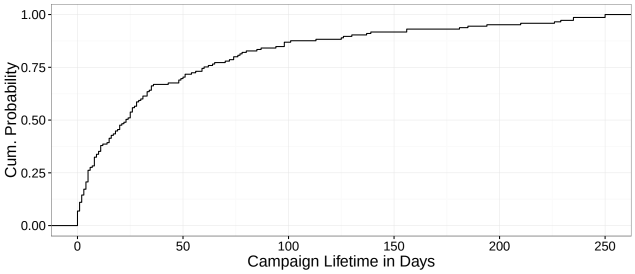


Figure 8: *CDF of the lifetime of scam campaigns.*

whitespaces and new lines in an attempt to elongate the `alert` dialogue to a point that the newly added checkbox would be out of the user's view. The rest were trying to bypass the `alert`-dialogue threshold, by using multiple event handlers, launching `alert` dialogues from each one, in combination with the creation of new pop-up windows and subdomains. It is also worthwhile to note that Internet Explorer does not offer such a mechanism and thus a malicious webpage can keep on launching `alert` dialogues without the user being able to stop them, or navigate away while a dialogue is shown.

Lastly, we observed that 87% of the discovered scam pages were using HTML audio tags, to automatically launch repeating audio clips that either sounded like an alarm, or were text-to-voice tracks, highlighting the severity of the problem and asking the user to call the listed technical support number.

5. INTERACTING WITH SCAMMERS

Even though the various measurements of the data collected by ROBOVIC (presented in Section 4) can be used to better understand the workings of technical support scam pages, they provide no insights on what happens when victim users, convinced that their machines are infected, call and interact with technical support scammers.

To shed light into this final but crucial part of technical support scams, in this section, we report on the data that we collected by posing as technically unsavvy users and calling 60 technical support scammers, while recording our entire interactions with them. During those interactions, we discover the way that scammers gain access to user machines, the methods and procedures that they use to convince the user of the purported infection, the average duration of each call, and the amount of money requested by each scammer.

5.1 Experiment Preparation

At its core, our study is an observational study. That is, we do not seek to apply different treatments to scammers and observe the effect of our treatments on their scams. We merely seek to observe the methods that they use in order to defraud an average individual, with no security-related computer knowledge. Even though this defrauding happens on a daily basis, we unfortunately have no means of tapping into these conversations while they happen. For this reason, we had to pose as victims and record our interactions with the scammers.

IRB Approval. Since scammers are human subjects, we applied to our institute's IRB and got permission to perform these recorded calls. Our approved application allows us to make use of deception (we are not revealing our true identities or intent to the scammers) and waive the requirement of consent (we do not ask the scammers whether they want to participate in our study). In addition, we convinced the IRB to allow us to avoid debriefing the scammers at the end of each call, to avoid information sharing from the side of the scammers that would place suspicion on future calls. Since scammers are already having these conversations with victims on a daily basis, our study does not incur any risk to their emotional, psychological, or physical wellbeing.

Observed Environment. The very first action that scammers perform after a victim user calls them, is convince the victim to give them remote access to their operating system. For our purposes, we made use of virtualization, where an installation of a Microsoft Windows 7 operating system was executing inside a Type-2 hypervisor. The use of virtualization not only allowed us to fully isolate a scammer's actions from critical infrastructure, but to also roll-back to a clean state of our operating system, after the end of each call.

From a small pilot experiment, we already knew that scammers become suspicious when the operating system to which they are given access, looks like it was recently installed. That is, a new installation of Windows with a default background image, no browsing history, and no desktop icons will, at the very least, make scammers suspicious. Even if the scammer decides to proceed anyway, it is likely that he will behave differently compared to his interactions with a real system, and thus our observations about their techniques may not be properly generalizable.

To ensure that our VMs look like realistic user systems, we artificially aged our virtual machine, by installing different applications, downloading images and documents and placing them on the Windows desktop, and browsing many popular video sites, gaming sites, and news sites. We changed our system clock between different sets of actions so that some of our actions would appear to have occurred in the past, e.g., the timestamps of installed programs and files, and the dates available in our browsing history, placed these actions up to two years before the beginning of our experiment. Since we limited our visits and downloads to popular websites and applications, and are thus confident that our virtual environments were free from malware.

Finally, we also removed obvious tell-tale signs of our virtualization environment by changing the appropriate Registry keys and the configuration of our virtual machine. We used techniques originally devised to defeat simple VM-detection used by modern malware [29], but made no attempt to comprehensively eradicate each and every VM "red pill" [32, 37].

5.2 Data Sources and Data Collection

To discover the phone numbers of technical support scammers, we randomly sampled the pages that ROBOVIC had discovered as scam pages, and ensured that we did not call any number more than once. Note that ROBOVIC discovers technical support scam pages which claim that users are infected and flood the user with alert boxes, in an attempt to make the user unable to navigate away from the scam website. As such, we are confident that we never called a legitimate technical support number.

We used VoIP software with conversation-recording capabilities, packet-capturing software residing outside the VM for capturing the network traffic of our virtualized operating system, and host-OS-residing screen recording software, for recording the visible actions of scammers, once they were given access to our VMs. After the collection of data from 60 different technical support scam calls, and the calculation of the statistics described in this section, we anonymized all copies of the collected data according to our IRB protocol.

5.3 Script for our interactions

Throughout our calls, we pretended to be average computer users who can use their PCs but have no computer knowledge beyond that. For example, we pretended not to know what an IP address is and, while we knew that having a virus is bad, we pretended not to know exactly what a virus does on our computer. We allowed the scammers to remotely connect to our system, following their instructions to the letter, and acted, to the best of our abilities, with shock, each time that a scammer would interpret something on our screens as the result of malware. Shortly after each scammer presented us with the pricing of his services, we either abruptly ended our calls, or found an excuse to politely hang-up. We never contradicted the scammers except during the last ten calls in order to discover how scammers react when users inform them that they are not convinced.

In a typical instantiation of this type of scam, once a victim calls the scammer and explains to him why she is calling, the scammer takes over the conversation. As such, we argue that even if each call is slightly different than the rest, the overall obtained results are aggregatable and generalizable to the population of technical support scam sessions. To quantify this phenomenon, we utilized a professional audio transcription service [36] to obtain the text of five randomly selected calls. The average number of words used by scammers in each call is 1,367 ±407, whereas the average number of words from the victims (ourselves) is 530±172. In addition to the scammers speaking, on average, almost three times as much as the victims, the standard deviation also shows that regardless of the exact call, the variation of our answers was small compared to the variation of the scammers questions. Two of these transcripts are available in this paper's appendix.

Lastly, we want to point out that we did not pay any scammer and therefore are unable to study scammers, *after* they have charged users for unnecessary services. We chose not to pay scammers primarily for ethical reasons. As described later in this section, the average amount of money that a scammer requests is almost $300. To get statistically significant numbers, we would have to pay at least 30 scammers and thus put approximately $9,000 in the hands of cybercriminals, a fraction of which would likely be used to fund new malvertising campaigns and attract new victims.

5.4 Results

Remote administration tools

Before a scammer can start convincing users that their machines are infected with malware, he must somehow get remote access to a user's machine. To that extent, the scammer must guide the user into downloading, installing, and allowing a remote administration tool which he will then use for his "support" session.

Even though all scams started with the scammer requesting us to open the Microsoft Windows "Run" dialogue, by holding our Windows Key and pressing "R", different scammers would then ask us to type different things: 58% of the scammers asked us to type the domain name from where we would eventually download the remote administration tool; 27% of scammers asked us to type the command "`hh h`" which opens up Windows help first. From there, we were instructed to click on the top-left icon and choose the option "Jump to URL" where we would type the URL of the remote administration tool. We theorize that scammers are taking advantage of the built-in browser of Microsoft Help, under the assumption that our main browser is locked by the scam's blocking `alert` dialogues. Alternatively, this method could also be used to bypass any browser extensions that would detect a suspicious site and alert the user. The rest of the scammers asked us to type "`iexplore.exe`" which launches Internet Explorer, a browser that is guaranteed to be available in all Windows operating systems.

Table 2: *Remote Administration Tools used by scammers for getting access to their victims' machines*

Remote Administration Tool	**Websites**	**Scammer abuse**

LogMeIn Rescue	`www.support.me`
	`www.lmi1.com`
	`www.logmein123.com`
		60%

CITRIX GoToAssist	`www.fastsupport.com`	21%
TeamViewer	`www.teamviewer.com` *Scammer-controlled*	12%

Other	`www.anydesk.com`
	`www.gethelp.us`
	`www.supremocontrol.com`
		7%

Table 2 shows the most popular tools abused by scammers for connecting to our machines. LogMeIn Rescue and CITRIX GoToAssist are web applications where a user visits one of the websites listed in Table 2, enters a code given by the scammer over the phone and downloads a binary that will eventually allow the attacker to remotely access and control a user's machine. TeamViewer and AnyDesk are stand-alone programs that a user must download and execute. Once the programs are running, both programs show a customer number and a PIN that a user must provide to the scammer in order for the scammer to connect to the user's machine.

In all cases, the scammers were abusing legitimate web applications and programs as part of their scams. Most of the aforementioned companies seem to be aware of this phenomenon and warn their users, typically through their websites, not to allow remote connections from people they do not trust. When these messages are pronounced, as in the case of TeamViewer, scammers incorporated these messages into their stories in order to put us at ease. Other scammers, chose to self-host older versions of the programs that did not include these warning messages, thereby avoiding the warnings altogether.

Utilized social-engineering techniques

The scammers used a variety of techniques to convince us of the purported infections and the need to purchase their support packages. Table 3 shows the most popular techniques used and the percentage of scammers that used each technique. We provide a brief explanation of the techniques that are not self-explanatory:

- **Stopped Services/Drivers.** 67% of scammers loaded the list of Windows services and showed us that many services were stopped. While this is the normal state of a Windows OS installation, the scammers claimed that hackers have stopped these services and that is why they were able to get access to our machines.
- **Event Viewer.** Event Viewer is one of the administrative tools of Windows that shows general information about a system that could be used for troubleshooting purposes. The

Table 3: Techniques used by support scammers in order to convince their victims of a malware infection

Technique	% Calls
Stopped Services/Drivers	67
Event Viewer	52
Specific Virus Explained	50
System Information	47
Action Center	40
Fake CMD Scan	40
Netstat Scan	40
Installed/Running Programs	35
Browsing History/Settings	27
Downloaded Scanner	17
Reliability/Performance	15
Other (Temp, Registry)	13

scammers treated the errors shown by this tool as a sign of hacker activity.

- **Virus details.** Some scammers, would conclude that our system is infected by a specific malware, such as "koobface" or "Zeus." They would then proceed to navigate our browser to pages (typically Wikipedia) explaining these threats and asked us to read out loud the section of each post describing the damage that the specific piece of malware does to its infected hosts.
- **Netstat scan.** 40% of scammers utilized the `netstat` utility to convince us that our machine is already occupied by hackers. Specifically, they claimed that each non-local, TCP connection listed in the output of `netstat` was an attacker who had either already connected to our machine (entries with an `ESTABLISHED` status), or was currently trying to connect (entries with a `TIME_WAIT` status).
- **Fake CMD scan.** One of the more creative techniques was the use of verbose command-line utilities as fake virus scanners. 40% of the scammers utilized a command such as "`dir /s`" which lists files and folders present on a specific path of the filesystem. While the program is producing output, the scammer types or copy-pastes text in the command-line window, that will only appear *after* the program is done executing. As such, at the end of the program's execution, the user suddenly sees text that claims that a virus has been discovered which he is likely to attribute to the "scanning" program that was just executing. This technique is likely one of the most convincing ones because i) it does not need interpretation (common messages used were "Virus detected" and "System at Risk") and ii) as far as the user is concerned, it is his own operating system that produces this message, rather than a downloaded third-party tool.
- **Performance.** Many scammers used system information tools to discover the type of CPU and amount of RAM memory available to our system. They then praised the hardware of our machine before proceeding to search for infections. This was typically done to convince us that spending money for the removal of malware was worth the cost since it would allow us to keep using our machine for many years before we would need to purchase a new one.

Overall, while we were able to identify tools and techniques commonly used by scammers, we were impressed with the scammers' creativity in finding status messages that were already present on our system and attaching a infection meaning to them. Figure 9 shows how often scammers used two social engineering techniques together. There, we use the recorded frequencies to calculate their respective conditional probabilities.

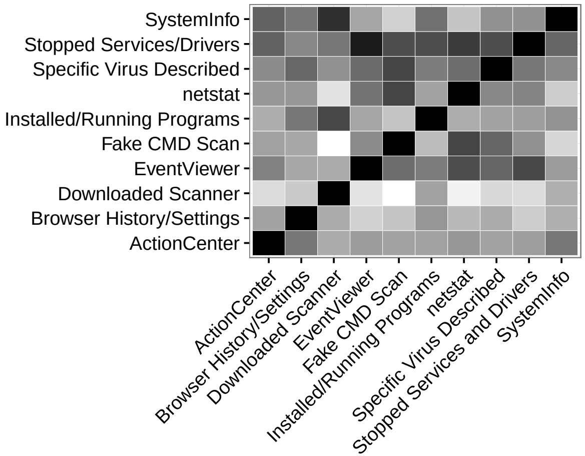


***Figure 9:** Heatmap showing the conditional probability (ranging from white to black) of the ten most often used social engineering methods. Note that because, in general, $P(A|B) \neq P(B|A)$ the heatmap is not symmetric along its diagonal.*

Duration of calls

Figure 10 shows the distribution of the time duration between the beginning of a technical support scam call, and the time when a scammer offered his services in exchange for money. The average duration of that interval is 17 minutes, and the distribution is approximately normal. In only a few cases, the scammers first told us the amount of money that they will be charging (around the second and third minute of our conversation) and *then* proceeded to "diagnose" our machine.

Overall, one can see that the scammers are by no means in a hurry to convince users and defraud them. They take their time to slowly guide their victims into installing a remote administration tool, clicking through all the security dialogues, and giving them access to their machines. Once they have access, they slowly work their way through different Windows tools, showing their output to users and interpreting that output for them. It is likely that scammers know that the more time they take to convince a user about an infection, the more successful they will be when they ask for a compensation for their services. Figure 10 also provides an indication of the amount of work necessary in order to obtain real-world data from technical support scam calls. Specifically, for the 60 calls recorded and analyzed, we spend more than 1,300 minutes (22 h) just interacting with scammers, excluding dropped calls, out-of-order numbers, analysis of the recordings, and verification of our findings.

Since scammers control the vast majority of the conversation (see sample transcripts in Appendix) we opine that the distribution of time shown in Figure 10 will be generalizable to the population of victims. Therefore, this distribution can be of immediate value to telcos and the FTC. Specifically, given a list of numbers operated by scammers, telcos can straightforwardly produce metadata of their customer base that has called any one of the numbers of technical support scams. The FTC can then prioritize take-down action by focusing on the scammers with whom victims were interacting for more than 41 minutes, that is, the mean of our distribution plus three standard deviations. Since the duration distribution is approximately normal, the mean ± three standard deviations should capture approximately 99.7% of

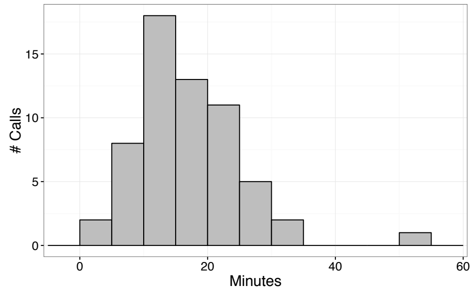


Figure 10: Distribution of the time duration between the beginning of a call, and the time when technical support scammers presented us with the pricing options for their services

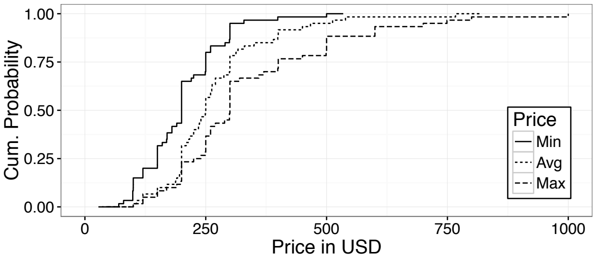


Figure 11: Requested charges for repairing our purportedly infected machines. Since most scammers offered us more than one support packages, we plot the ECDFs for minimum, average, and maximum amount requested.

all pre-charge calls. As such, anyone interacting for more than 41 minutes, is likely a defrauded victim.

Price of services

Once scammers felt confident that we were convinced that we are in need of their help, they then informed us about the price of their services. Most scammers offered us two to three different options with support packages ranging from a one-time fix, to multi-year support, ranging anywhere from $69.99 to $999.99. Figure 11 shows the ECDF of the amount requested, split in its minimum, average, and maximum (average for any given scammer is the average price of all offered support packages). The average support price across all support packages and all scammers is $290.9 with most scammers staying under $500 for all of their support packages.

The prices of support packages were structured in a way where the middle one made the most financial sense. In fact, the times that we pretended to be willing to purchase their support and requested the cheapest option, the scammers would typically try to reason with us that the middle one was a better value-for-money offer.

Freelance scammers or organized call centers?

At the outset of our study, we did not know whether technical support scammers are individual freelancers who supplement their income by single-handedly operating a technical support scam, or are part of an organized call center. Through the process of interacting with 60 different scammers, we are now convinced that most, if not all, scammers are part of organized call centers.

Next to anecdotal evidence that we gathered during our interactions (e.g. on one occasion, due to technical difficulties with our VoIP software, we called the same number three times in a row, and were greeted by a different person all three times), we conducted the following experiment: We replayed each recorded call and, instead of focusing on the scammer talking to us, we instead focused on background noises. While some scammers muted their microphones when they were not speaking, the majority did not. On 62% of our calls, we were able to hear other people in the background, often recognizing phrases about security and malware that the scammer had just used in his own narrative. Therefore, our results indicate that the majority of scammers work in call centers, a fact which is corroborated by a recent interview of a technical support scammer on Reddit [35].

Estimating the size of call centers

Motivated by our earlier finding that the majority of scammers operate out of call centers, we wanted to estimate the size of these call centers, i.e., how many scammers are “hiding” behind a single toll-free phone number.

To this end, we gathered 20 volunteers and explained to them the concept of technical support scams, the methods that scammers use, and the typical narratives of conversations with scammers. Each volunteer was given a sheet of ten toll-free phone numbers operated by scammers (randomly selected by our pool of numbers) and a list of fake personae which they could assume when talking to the scammers (in our experience the majority of scammers request the caller’s name and address before proceeding). The ten toll-free numbers were the same for all volunteers and they were instructed, guided by our signals and a projected stopwatch, to start calling each number at the same time. If a scammer would answer the phone, the volunteers were instructed to keep them occupied for 90 seconds. If a volunteer would get a busy tone, they were instructed to keep trying to call that same number for 90 seconds. Finally, if the volunteer would be placed in a waiting queue, they were again supposed to wait for 90 seconds until the 90 seconds expired. Under the reasonable assumption that a scammer cannot be speaking to two people at the same time, this experiment essentially allowed us to get a lower bound of the size of a call center by counting the number of people that were able to reach a scammer (either immediately or after waiting in a queue) in the measured 90-second period.

The average number of volunteers who were able to speak with a scammer across all ten studied phone numbers was 11, with the smallest call-center housing 5 scammers, and the largest one 19. Our results show that technical support scammers can belong to various operations, ranging from small scale ones (call centers with 5 or 6 people) all the way to call centers that essentially occupied all of our volunteers (call centers with 18 or 19 people). As before, we argue that our method that can be straightforwardly operationalized by the FTC and other law-enforcement agencies, for identifying the largest players in the technical support scam ecosystem, and focusing on them first.

Scammer Location

Even though scammers access a user’s machine via a remote administration tool that typically involves a centralized server relaying commands between the user and the scammer, it is possible that some tools still leak the scammer’s real

IP address to the user. To discover whether the remote administration tools utilized by scammers fit that description, we installed the tools on our machines and connected to them from another known IP address, while capturing the network traffic. We then analyzed the traces from our own connections and created packet signatures that reveal the connecting user's IP address.

Using this method, we recovered the IP address of 41 out of the 60 recorded technical support scams. By geolocating these IP addresses, we discovered that 85.4% of them were located in different regions of India, 9.7% were located in the US, and 4.9% were located in Costa Rica. While we cannot know with certainty that the scammers were not using VPNs located in these countries, we argue that they most likely are not since the recovered IP addresses do not belong to known VPN providers but rather to residential and corporate ISPs. In addition, the accent of the vast majority of the speakers with whom we interacted was Indian, matching our geolocation results. We reason that India is the most prevalent country, both because of the relatively low average wage [45], but also because India is already a popular choice for outsourcing call centers of English-speaking countries [19, 20]. Consequently, we do not know whether the people running these call centers are the responsible ones, or are merely working for a third-party scammer who has outsourced the last part of the scams to them.

Scammer Demeanor

In general, scammers exhibited a kind demeanor. They would patiently guide us through the steps for downloading their remote administration tool, giving us step-by-step instructions for the entire process. They would take no computer knowledge for granted, even to the point of explaining us that the Windows key is the one that "looks like a flag", between the Ctrl-key and the Alt-key on the bottom left of our keyboard. More than one scammer, after having explained to us that we are infected with malware, would open up Wikipedia pages trying to educate us of the meaning of words, such as, "trojan", "koobface", and "browser hijacker."

To quantify how a scammer's behavior changes when faced with an expert user, in the last ten of our calls, after the scammers showed us "signs" of infection and offered their services in return for money, we contradicted them by explaining that we did not believe them. 60% of the scammers remained calm and polite, and tried to convince us of the legitimacy of their company by showing us their websites and other online information. The remaining 40% became rude and soon after that terminated the call, with one scammer setting a password to our virtualized operating system before logging out.

Summary of findings

Through our interactions for over 22 hours with 60 scammers, we were able to precisely quantify many aspects of this last part of technical support scams. We discovered that scammers abuse popular remote administration tools (81% of scammers rely on two specific software products), to gain access to user machines where they then patiently attempt to convince users that they are infected with malware. We found that, on average, a scammer takes 17 minutes, using multiple social engineering techniques mostly based on misrepresenting OS messages, to convince users of their infections and then proceeds to request an average of $290.9 for repairing the "infected" machines. We explained the reasons why we are convinced that most scammers operate out of call centers, estimated the size of an average call center, and, using geolocation of the collected network traces, we found that scammers are likely to be operating out of some specific countries, more than others.

6. DISCUSSION AND FUTURE WORK

Given our findings in sections 4 and 5, in terms of the prevalence of technical support scams, the social engineering techniques used by scammers once a victim is convinced to interact with them, and the final cost to users, we argue that technical support scams is a real and dangerous threat to the modern web. In contrast with other cybercrime methods, such as the stealing of credit card numbers and banking credentials, technical support scams do not need any additional monetization effort since, if the scam is effective, the victimized users will be *willingly* accepting the charges and *voluntarily* providing their private and financial information, over the phone, to scammers.

Even though systems that can automatically discover and detect these scams as soon as they arise, like ROBOVIC, are crucial, we opine that the threat of technical support scams can only be comprehensively subdued with the education of the public and additional help from browser vendors. In this section, we briefly describe these two areas of intervention.

User Education

User education has long been a problem of security mechanisms and its lack has often been abused by attackers through social engineering. While certain problems, e.g., the expiration of an SSL certificate, or the problem of mixed inclusions, are admittedly hard to explain to a non-technical person, we argue that explaining the concept of technical support scams, is an easier endeavor. This is because, in technical support scams, there are no exceptions that the user must remember. A webpage cannot, by browser design, know that a user is infected and should never be using a flood of alerts with threatening messages to communicate with users. As such, educating the public that these pages should not be trusted is highly unlikely to cause harm to legitimate businesses, even the ones involved in remote technical support.

Public service announcements are already used by multiple countries as a way of raising awareness for health and safety issues, and would be an ideal vehicle for educating users about the dangers and characteristic signs of technical support scams. Even though the Internet Crime and Complaint Center called its warning of technical support scams a "Public Service Announcement" [18], the announcement was only available via specific websites and thus far from the reach of the general population. At the same time, even though non-technical people can be educated to recognize technical support scams, we must also provide them with a simple way of navigating their browser to safety, away from webpages that abuse blocking, browser-provided APIs, such as the `alert` function, to keep users from navigating away.

Browser Support

Given our reliance on the web, modern browsers try to provide high availability to users and a large degree of control to websites. In addition to blocking UIs, one specific feature that is, in general, desirable but has inadvertently become a tool in the hands of scammers is the remembering of open tabs in the case of a crash. Specifically, if we assume that, a non-technical user is trapped on a technical support scam page and, in a moment of desperation, reboots his machine, the browser will remember all the open tabs, including the one with the technical support scam, upon reboot. As such, the user will still be trapped and much more likely to call the scammers. Trying to outrun `alert` dialogues or killing the browser process and clearing recent history should not be something that we expect from everyday users.

To help users navigate to safety, we propose the idea that browser vendors could all adopt one universal shortcut that users can utilize when they feel threatened by a webpage. Depending on the design, the browser can choose either to immediately close the current tab, or close all tabs and navigate the browser to a known safe page. The browser should ignore all event handlers and provide no way that a webpage could detect its unloading in time to launch a new window of the intruding webpage. Ideally, this shortcut combination would be communicated to the public through the aforementioned PSAs, allowing users to both recognize and defend against technical support scams. Lastly, we want to point out that such a shortcut could be useful beyond technical support scams, helping users quickly navigate away from websites that they find intrusive, such as shock sites, as well as helping them defend against any webpage that is trying to forcefully keep them from navigating away.

7. RELATED WORK

Our study was inspired by a series of blog posts and a whitepaper from an antimalware company which qualitatively analyzed technical support scams [17, 27, 28]. While these, and other blog posts have, in the past, analyzed a handful of scams, their studies are ad-hoc and their results are not generalizable. To our knowledge, no blog post has ever produced a repeatable methodology for finding scam pages in the wild, nor tried to cluster phone numbers and their respective domains, using a corpus of thousands of domain names and phone numbers. Similarly, because of the ad-hoc nature of their interviews with scammers, no one has ever reported the distribution of the time that scammers take, the size of an average call center, or the amount of money that they charge, all of which can be of immediate use for prioritized take-down action.

In contrast with the aforementioned studies, our work is the first systematic, quantitative study investigating technical support scams, by i) designing and deploying a distributed crawling infrastructure for an 8-month period, ii) using this infrastructure to identify thousands of domains and phone numbers and analyzing their techniques and underlying infrastructure, and iii) conducting a controlled, IRB-approved experiment to obtain *precise* information about the social engineering techniques used by scammers and statistics about the process, the tools used, the call-center infrastructures, and the amount of money charged.

Even though we are not aware of any other work that has investigated technical support scams, we argue that these scams are a cross-over between traditional *scareware*, and scams perpetrated over the telephone [42] instead of over the Internet, such as *vishing* (Voice Phishing).

Scareware.

Scareware refers to software, typically fake AVs, which attempt to scare the user into performing one or more harmful actions. Cova et al. [9] tracked 6,500 domains involved in the distribution of fake AVs and discovered that 65% of the web servers behind these domains were exclusively serving malicious content. The authors clustered multiple fake AVs as part of the same campaign, with the largest campaign being responsible for 23.5% of the 6,500 tracked domains. Rajab et al. [34] use Google's SafeBrowsing data to discover over 11,000 domains offering fake AVs with up to 90% of the discovered scams relying on social engineering for getting installed on a user's computer. Stone-Gross et al. [39] approach the phenomenon of fake antivirus software from an economic angle. The authors show that fake AV scammers can earn hundreds of millions of dollars in antivirus license fees and discover the presence of affiliate networks where scammers are paid a commission for each fake AV installation. Dietrich et al. [11] describe how perceptual hashing could be used to automatically cluster malware that depend on visual interfaces including fake antivirus programs and ransomware [23]

Telephone Scams.

Maggi performed the first study of vishing by analyzing the data submitted by 360 users who had fallen pray to vishing attacks and were willing to recount their experience [26]. The researcher discovered that most source numbers were unique and that the scams were perpetrated both by human scammers who were trying to exfiltrate information, such as, a user's credit card number, as well as robotic callers that would redirect a victim to a human scammer only after the victim would press a specific key on her phone. In a later study, Costin et al. [8] investigated the role of phone numbers in cybercrime and used phone numbers to cluster different types of scams, using data from another crowdsourced website listing scams. The authors utilized HRL (Home Register Location) queries and showed that the average scammer kept, almost always, their phone online. Unfortunately, HRL queries are only applicable to mobile phones, thus we cannot utilize them for tracking toll-free numbers. Christin et al. [6] analyzed a type of scam that was mostly targeting Japanese users by threatening to reveal their adult browsing habits if they would not pay a certain amount of money to scammers. Among others, the authors took advantage of the phone numbers made available by scammers in order to cluster multiple scams as part of larger campaigns. Note that in all three studies, the authors used publicly available data to perform their analyses. Contrastingly, in this paper, because of the absence of available datasets, we designed and developed RoboVic, the first tool able to automatically discover hundreds of instances of technical support scams on a weekly basis.

Gupta et al. described the architecture of a phone honeypot and presented the intelligence gathered by deploying 39,696 phone numbers which attracted 1.3 million calls over a period of seven weeks [16]. The authors discovered that older phone numbers attracted a higher number of calls than newer phone numbers, and showed how the rate of calling can be used to differentiate between different types of unwanted calls, e.g., the ones done by a telemarketer, versus a debt collector. While their system could, in principle, be used to discover the older variant of technical support scams (where unsuspecting users receive unsolicited calls from scammers) the type of technical support scams that we investigated in this paper needs an active component, such as Robovic, to actively discover pages and numbers.

8. CONCLUSION

Despite the tens of security mechanisms available on a typical modern computing environment, the user is, and will likely continue to be, part of the trusted computing base of the system. Therefore, as long as an attacker can use social-engineering methods to convince the user to perform a series of malicious actions, most technical countermeasures become moot.

In this paper, we reported on the first systematic investigation of technical support scams. By designing and implementing the first system capable of automatically discovering technical support scams, we collected a corpus of thousands of unique domains and telephone numbers engaged in technical support scams, clustered them in campaigns, and showed that scammers abuse specific browser APIs to make it hard for users to navigate away from a technical support scam page. By interacting with 60 different scammers for more than 22 hours, we precisely identified the social engineering techniques used, the remote administration tools abused, and the amount of money that scammers are charging. We presented evidence that places technical support scammers in call centers in English-speaking countries with low wages, showing that the ecosystem of technical support scams is complex and comprised of more than one parties. Lastly, we discussed the need for user education and proposed a simple feature that browser vendors could adopt to assist users in navigating away from malicious pages.

9. REFERENCES

[1] Agten, P., Joosen, W., Piessens, F., and Nikiforakis, N. Seven months' worth of mistakes: A longitudinal study of typosquatting abuse. In *Proceedings of the 22nd Network and Distributed System Security Symposium (NDSS)* (2015).

[2] Alrwais, S., Yuan, K., Alowaisheq, E., Li, Z., and Wang, X. Understanding the Dark Side of Domain Parking. In *Proceedings of the USENIX Security Symposium* (2014).

[3] AWS | Amazon Elastic Compute Cloud (EC2) - Scalable Cloud Hosting. https://aws.amazon.com/ec2/.

[4] Bing Ads. Low quality ad submission & escalation. http://advertise.bingads.microsoft.com/en-us/report-spam-form.

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

[6] Christin, N., Yanagihara, S. S., and Kamataki, K. Dissecting one click frauds. In *Proceedings of the 17th ACM conference on Computer and communications security* (2010), ACM, pp. 15–26.

[7] Clark, J. W., and McCoy, D. There Are No Free iPads: An Analysis of Survey Scams as a Business. In *LEET* (2013).

[8] Costin, A., Isacenkova, J., Balduzzi, M., Francillon, A., and Balzarotti, D. The role of phone numbers in understanding cyber-crime schemes.

[9] Cova, M., Leita, C., Thonnard, O., Keromytis, A. D., and Dacier, M. An analysis of rogue av campaigns. In *Recent Advances in Intrusion Detection* (2010).

[10] Cyphort. Special Report: The Rise of Malvertising. http://go.cyphort.com/Malvertising-Report-15-Page.html.

[11] Dietrich, C. J., Rossow, C., and Pohlmann, N. Exploiting visual appearance to cluster and detect rogue software. In *Proceedings of the 28th Annual ACM Symposium on Applied Computing* (2013).

[12] Edelman, B. Large-scale registration of domains with typographical errors, September 2003.

[13] Englehardt, S., Eubank, C., Zimmerman, P., Reisman, D., and Narayanan, A. OpenWPM: An Automated Platform for Web Privacy Measurement. 2015.

[14] Google. How we fought bad ads in 2015. https://googleblog.blogspot.com/2016/01/better-ads-report.html.

[15] Google's Anti-Malvertising Team. Anti-malvertising.com. http://www.anti-malvertising.com/.

[16] Gupta, P., Srinivasan, B., Balasubramaniyan, V., and Ahamad, M. Phoneypot: Data-driven understanding of telephony threats. In *Proceedings of the 22nd Network and Distributed System Security Symposium (NDSS)* (2015).

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

[18] Internet Crime Complaint Center (IC3) | New Twist to the Telephone Tech Support Scam. http://www.ic3.gov/media/2014/141113.aspx, 2014.

[19] Call Centers in India - Call Center Services Providers Companies in India. http://www.callcentersindia.com/.

[20] Call Centers in India | Outsource Call Center - Outsource2india. https://www.outsource2india.com/why_india/articles/call_centers_india.asp.

[21] Invernizzi, L., Comparetti, P. M., Benvenuti, S., Kruegel, C., Cova, M., and Vigna, G. Evilseed: A guided approach to finding malicious web pages. In *IEEE Symposium on Security and Privacy* (2012).

[22] Khan, M. T., Huo, X., Li, Z., and Kanich, C. Every second counts: Quantifying the negative externalities of cybercrime via typosquatting. In *Proceedings of the 36th IEEE Symposium on Security and Privacy* (2015).

[23] Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., and Kirda, E. Cutting the gordian knot: A look under the hood of ransomware attacks. In *Proceedings of the 12th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)* (2015).

[24] Kirk, J. Malicious advertisements on major sites compromised many, many PCs. http://www.pcworld.com/article/2879732/malicious-advertisements-on-major-sites-compromised-many-computers.html, 2015.

[25] SSD Cloud Hosting - Linode. https://www.linode.com.

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

[27] Malwarebytes Labs. PSA: Tech Support Scams Pop-Ups on the Rise. https://blog.malwarebytes.org/fraud-scam/2014/11/psa-tech-support-scams-pop-ups-on-the-rise/.

[28] Malwarebytes Labs. Tech Support Scams âĂŞ Help & Resource Page. https://blog.malwarebytes.org/tech-support-scams/, 2013.

[29] Mikael, @nsmfoo. Modifying VirtualBox settings for malware analysis 2013 ed. http://blog.prowling.nu/2013/08/modifying-virtualbox-settings-for.html, 2013.

[30] Moore, T., and Edelman, B. Measuring the perpetrators and funders of typosquatting. In *Financial Cryptography and Data Security* (2010), vol. 6052, pp. 175–191.

[31] Nikiforakis, N., Maggi, F., Stringhini, G., Rafique, M. Z., Joosen, W., Kruegel, C., Piessens, F., Vigna, G., and Zanero, S. Stranger danger: exploring the ecosystem of ad-based url shortening services. In *Proceedings of the 23rd International World Wide Web Conference (WWW)* (2014).

[32] Paleari, R., Martignoni, L., Roglia, G. F., and Bruschi, D. A fistful of red-pills: How to automatically generate procedures to detect cpu emulators. In *Proceedings of the USENIX Workshop on Offensive Technologies* (2009).

[33] Pauli, D. Malware menaces poison ads as Google, Yahoo! look away. http://www.theregister.co.uk/2015/08/27/malvertising_feature/.

[34] Rajab, M. A., Ballard, L., Mavrommatis, P., Provos, N., and Zhao, X. The nocebo effect on the web: an analysis of fake anti-virus distribution. In *USENIX workshop on large-scale exploits and emergent threats (LEET)* (2010).

[35] I worked at a tech support scam phone room AMA. https://www.reddit.com/r/AMA/comments/3766m1/i_worked_at_a_tech_support_scam_phone_room_ama/, 2015.

[36] Rev - Transcription, Captions, Translation. https://www.rev.com/.

[37] Rutkowska, J. Red Pill... or how to detect VMM using (almost) one CPU instruction. http://repo.hackerzvoice.net/depot_ouah/Red_Pill.html.

[38] Schwartz, M. J. Social Engineering Attacks Cost Companies. http://www.darkreading.com/vulnerabilities-and-threats/social-engineering-attacks-cost-companies/d/d-id/1100278?

[39] Stone-Gross, B., Abman, R., Kemmerer, R. A., Kruegel, C., Steigerwald, D. G., and Vigna, G. The underground economy of fake antivirus software. In *Proceedings of the 10th Workshop on Economics of Information Security (WEIS)*. 2011.

[40] Szurdi, J., Kocso, B., Cseh, G., Spring, J., Felegyhazi, M., and Kanich, C. The long "taile" of typosquatting domain names. In *23rd USENIX Security Symposium (USENIX Security 14)* (2014).

[41] TollFreeNumbers.com: The Internet's Toll Free Search Engine for Vanity 1-800 Numbers. http://www.tollfreenumbers.com.

[42] Tu, H., Doupé, A., Zhao, Z., and Ahn, G.-J. SoK: Everyone Hates Robocalls: A Survey of Techniques against Telephone Spam. In *Proceedings of the IEEE Symposium on Security and Privacy* (May 2016).

[43] Verizon. Data breach investigations report. http://www.verizonenterprise.com/DBIR/2014/, 2014.

[44] Vissers, T., Joosen, W., and Nikiforakis, N. Parking Sensors: Analyzing and Detecting Parked Domains. In *Proceedings of the 22nd Network and Distributed System Security Symposium (NDSS)* (2015).

[45] Average wages by country, in purchasing power parity dollars. http://www.statista.com/statistics/226956/average-world-wages-in-purchasing-power-parity-dollars/, 2012.

[46] Wang, Y.-M., Beck, D., Wang, J., Verbowski, C., and Daniels, B. Strider typo-patrol: discovery and analysis of systematic typo-squatting. In *Proceedings of the 2nd conference on Steps to Reducing Unwanted Traffic on the Internet*, SRUTI'06.

APPENDIX

A. SAMPLE OF TRANSCRIBED CONVERSATIONS WITH SCAMMERS

```
Scammer:  Thank you for calling technical support. How
     may I assist you?
Victim: Hi, good morning. I think I have a problem with
     my computer because I was browsing the Internet and
     then it suddenly told me that I was infected with a
     virus and it asked me to call this number.
Scammer:  OK. Can you confirm for me, first of all, what
     Microsoft device you are using?
Victim: I am using Windows 7. I do not know if that is
     what your question is.
Scammer:  Yeah, that was the question. Windows 7, all
     right. First of all we will try close that warning
     page, all right? And we will try to fix the access,
     all right? And make sure this does not happen again.
Victim: OK. I think the warning closed because I think
     the browser said it had to end the process, so I
     just wrote the number down before it could close, so
      ... the site is closed but I am still afraid I have
      a virus.
```

```
Scammer:  OK. So what you have to do is look at you
     keyboard. Do you see a Windows button there?
Victim: Is it between the Control and ALT?
Scammer:  Yes, correct.
Victim: Yes, I see it.
Scammer:  You have to press and hold that. You have to
     press and hold that button. And then press R. R as
     in Richard, simultaneously.
Victim: OK. I did it, yes.
Scammer:  What do you see now?
Victim: I see this little window that says "run."
Scammer:  All right. Type in there W, W, W, dot. L as in
     lemon. M as in Mary. I as in indigo. Number one. Dot
      com.
Victim: And should I click OK?
Scammer:  OK. Yeah.
Victim: OK.
Scammer:  What do you see now? If you see restore option
     do not click on restore, OK?
Victim: OK. I see a page; there is a support connection.
Scammer:  All right, I am going to generate a six-digit
     code, OK? You have to type that code into that box.
     Plus, you have to write it in a paper because this
     code will be your case number for Microsoft, all
     right?
Victim: OK, I will write it down.
Scammer:  All right, the code is: 5, 4, 9, 2, 2, 5.
Victim: OK, let me type it in. 5, 4, 9--
Scammer:  Sorry?
Victim: I am typing it in.
Scammer:  It is 5, 4, 9, 2, 2, 5. OK?
Victim: I did that. And then what should I do?
Scammer:  No click on start download.
Victim: OK. I did this.
Scammer:  Now what do you see?
Victim: So a download started and it is at the bottom of
     my Chrome Internet.
Scammer:  Uh-huh. You have to double-click on it and run
     that file, OK?
Victim: OK, let me try.
Scammer:  Uh-huh.
Victim: OK. There is a page that opened, a small other
     window, that says "net creative mind."
Scammer:  OK, now within 2 seconds you will see some pop-
     ups on your screen. It will say "Do you want to
     allow this file?" You have to click on "allow access
     ," "yes," and "OK," all right? All the positive
     things.
Victim: OK, so "allow access." OK. Hit "yes."
Scammer:  One more pop-up will come. You will see my name
      there: [inaudible 00:03:54]. You have to press "OK"
      there.
Victim: OK. Give me one second.
Scammer:  Yeah, it will come in five seconds, all right?
Victim: OK.I see your name. Now I see the dialogue. So I
     should click "OK" on this?
Scammer:  Yeah. All right, can you see I am moving this
     now?
Victim: Yes.
Scammer:  OK, I have access. Now let me check what is
     going on, OK? I am going to close this.
Victim: Right. Thank you.
Scammer:  And, can you tell me, how old is this computer?
Victim: It is about 2 and a half years if I am not
     mistaken.
Scammer:  And this is your personal computer?
Victim: Yes.
Scammer:  Or multiple users?
Victim: I use it but my neighbor also uses it sometimes
     if their computer is not working.
Scammer:  OK, what is your full names?
Victim: Nathan Sanders.
Scammer:  Can you spell that?
Victim: Yes.
Scammer:  What was your first name?
Victim: Nathan. That is: N, A, T, H, A, N. And my last
     name is Sanders: S, A, N, D, E, R, S.
Scammer:  Sanders, OK. All right, I am going to first of
     all check your system, all right?
Victim: All right.
Scammer:  OK, it is Windows 7. Plus, you have a very good
      [inaudible 00:05:28], 3.19 gigahertz, your RAM is 2
     GB. Now, all in all, you have a good configuration,
```

but your rating is very low. You received 1 out of 10.

Victim: Yeah, yeah, I do not know why.

Scammer: But this configuration it can be more faster. Has this computer slowed down recently?

Victim: Yes. Yeah, slowly. I mean, you know, over the months it is becoming more slower.

Scammer: OK. OK. I am going to check into it, why it is happening, OK. You will see a black box now.

Victim: Yes, I see it.

Scammer: Now this thing is going to scan. This is your command prompt. This thing is going to scan your driver, all of the bio section, and most important your network area.

Victim: Uh-huh.

Scammer: This might take a little bit of time, so I need your patience, all right?

Victim: OK.

Scammer: Thank you. And can you confirm for me what kind of browsing do you do? Do you do online shopping?

Victim: Yeah, occasionally. I mean, you know, I check the news, I check the mail, and sometimes I buy something.

Scammer: OK. OK. And do you often witness online advertisements popping up every single time on your browser?

Victim: Yes, I do. I do, I do.

Scammer: OK. Now that is happening because, first of all, you are not using any protection in your computer. There is no protection. No firewall protection, no anti-virus protection, no network protection, and most important no pop-up protection. And that is what is happening in your computer. What is happening is a lot of viruses are coming and going because there is no protection, right? And I see a lot of junk files stored into your computer.

Victim: I see. Yeah, I see a lot of things going through this thing but I do not know what they are.

Scammer: A lot of them are junk files. These IP areas, you know? IP address areas. [inaudible 00:07:40] your network area. OK, the scan has completed.[inaudible 00:07:49]. The second one says network issue. OK, apart from this device, do you have any other device available?

Victim: No, not really.

Scammer: [inaudible 00:08:04]

Victim: No. That is my only computer.

Scammer: Do you have any WiFi devices?

Victim: I do not really know what is WiFi. I connect to the Internet, and I pay AT&T for it.

Scammer: OK, OK. All right. Now all these errors and warnings are coming from your registry. You see it says "viruses detected; system at risk."

Victim: Oh, wow. That is...wow. OK.

Scammer: It is confirmed that virus is detected, OK? Now we will be going on into your registry area. I am going to [inaudible 00:08:43]. Now this is also the reason why your computer is also slowing down day by day, right? And viruses are coming in. You do a lot of office work, right?

Victim: Yes.

Scammer: Word documents in your computer.

Victim: Yeah.

Scammer: Mm-hmm. OK, do you see this page?

Victim: Mm-hmm.

Scammer: This is your registry area, OK? Let us see what is going on. This might also take a little bit of time, OK? So just ... Oh my god. Wow.

Victim: What happened?

Scammer: All right, do you see this number them: 69?

Victim: Yes.

Scammer: You have more than 50 errors in warning in your computer stored in [inaudible 00:09:36]. Most of them are critical, you see?

Victim: I see. I guess that is bad. I do not really know.

Scammer: And it has been in your computer from 2014. It took a little pause, right? It took a little pause, but it started again.

Victim: Right.

Scammer: You see? And that is how hacking works. A lot of potential hacking processes going on. You see this [inaudible 00:10:00] event?

Victim: Mm-hmm, I do.

Scammer: This is potential hacking. Now, it means that this device, and your network, is compromised, OK? Which further means that if you have done any online shopping or any online [inaudible 00:10:16] and if you have shared any details, it can be easily hacked, right? Plus, you have a lot of rough files in folders. It can not be deleted because that is how hacking works. They just play with the computers, right? And the most important thing is that you can not delete that, you see? There is no option to delete them successfully.

Victim: Right.

Scammer: They just multiply every single time, and because of these errors ... [inaudible 00:10:49] critical issue. What is happening is a lot of your Microsoft services are stopping by itself. You are not stopping them but they are stopping, see?

Victim: I see.

Scammer: Stop, stop.

Victim: Yeah, that is true. I see.

Scammer: Stop, stop, stop. A lot of them. And most of them are ... yeah, and most of them, you notice, are Microsoft. Now you can imagine that if Microsoft service are not running, your Windows will suffer, right? Because they are the same product. Now, that is why your computer is slowing down and because you do not have protection, you have virus in your computer. You do not have an IP router so we are having an identity threat issue right now, OK? So we have to block your IP so that it is not visible, all right? So in the future this thing does not happen again, all right?

Victim: OK.

Scammer: So what we will do is we will transfer this session to our level-three people, OK? Level-three tech guys. I am the level-one. It will be transferred to the level-three guys, and once they have the access they will, first of all, install some software into your computer, right? Because you can see we can not delete them manually, neither can you run the service. You see? You can not enable it manually.

Victim: Right.

Scammer: So they will install them and the first thing they will do is make this number 0, and make your device, your network, your identity secure, OK? Second thing: running all the services that can not start. You will run them, and the final thing would be removing junk files from your browser and from your storage area, OK? These are the three whole things which our tech guys will work on.

Victim: I see.

Scammer: And this might take around 14 to 15 minutes, OK?

Victim: OK. Is that the service from Microsoft, or--how does it work?

Scammer: Yeah. Yeah, this is the Microsoft technical floor. We will transfer it to the level-three people, OK?

Victim: OK.

Scammer: And they will work on it, and they will complete it. But, Nathan, I have to tell you before transferring it that there will be a charge in it, right? I hope you understand that because, first of all, you have no warranty, second of all, you have no protection, and, third of all, it is an identity threat issue, OK?

Victim: I see, yeah.

Scammer: Yeah, yeah. So if you just want to go over the fixing it would be 99 dollars. We will remove all these errors and warnings, add a blocker, and remove all junk files and run all the services, OK? But, Nathan, I would strongly recommend you--with fixing--go with a year support or so, right? Because in the year support, first thing you are getting is an anti-virus, OK? Which is compatible, and it is for a lifetime, which will protect your device from viruses and a lot of malicious things coming from your Internet. It will protect you for a lifetime. Second of all, you will get network security, right? And network security would protect your identity and, most important, your IP. And, third, we will add some proper blockers, so that in the future you

do not see those advertisements that you see, right? Every time? They will not happen again.
Victim: OK.
Scammer: And the fourth thing is that you are getting a one-year warranty and a one-year tech support. And that would be 299, OK?
Victim: Oh, OK. I see.
Scammer: Yeah. So, do you want to go for a one-time support or a one-year support?

Scammer: [ringing] Thank you for calling technical support, how can I help you?
Victim: Uh, good morning. Um, I think I may have a problem with my computer, because I was just looking at, at the internet and websites and suddenly told me that I am infected. And it asked me to call you.
Scammer: If you can sir, can you just read the error message which you are getting on the screen.
Victim: So it said, 'Warning, you may have been infected with a, with virus' and it said no, don't attempt to remove it by yourself, not that I would know how. Um, and then it asked me to call this number, and then I think the browser closed. It said, you know, 'Does not respond, do you want to close?' And I closed.
Scammer: All right, and so do you have any virus protection or something, to protect your computer?
Victim: Um, how, how do I check that?
Scammer: Sir, you might have paid someone, for example, through AVG, Norton, Mcafee, Kaspersky-
Victim: I see-
Scammer: Antivirus companies.
Victim: I, I don't remember-
Scammer: Any of them-
Victim: When I got it. I don't remember if when I bought the computer there was some offer with it. I haven't really paid for software since I bought my computer.
Scammer: Oh, okay. And so how old is your computer?
Victim: It's a bit less than two years old.
Scammer: And which windows are you using, windows 7, 8, or 10?
Victim: I believe it's 7.
Scammer: Okay, all right. So, sir, in order fix the issue what I'll do, I'll take the remote access of the computer, we'll check the problems, check the pop ups which you are getting. And sir as there is no security at the moment-
Victim: Uh huh.
Scammer: Paid security, premium security, so there could be charges as well. Because we will be providing you, in order to fix your computer, [00:02:00] the Microsoft securities, the antivirus provided by the Microsoft. He is the manufacturer. All right?
Victim: I see.
Scammer: [inaudible 00:02:09] corporation so there could be charges, all right?
Victim: Right. Uh, yeah, I guess so, we - you can tell me I guess how much.
Scammer: Uh, sir, if you want to go for the one time fix and 1 year technical support, all right, that is just $99.
Victim: Uh huh.
Scammer: And if you want complete for 1 year package, including network security, Microsoft Tools and Microsoft antivirus, for 1 year, that will cost you $149.99, including all 3 softwares, and the best part is they are by the Microsoft.
Victim: Right.
Scammer: Plus the 1 year technical support. And, 1 year technical support means, anything goes wrong in 1 year-
Victim: Uh huh.
Scammer: Anything, software issues computer related issues you just have to call us and there will be no charge to fix that. All right sir.
Victim: Right. Yeah,
Scammer: So that's something, right?
Victim: Uh huh.
Scammer: Uh huh, sorry.
Victim: I, they are a little bit expensive for my budget, even the- your cheapest option, that's, that's true. I don't know if I need it of course.
Scammer: Then you can go for the 1 time fix, that is $69.99, that is a 1 time fix.
Victim: $69.
Scammer: Yes sir. That is a minimum, $69.99, that is a 1 time fix. In that you will get the technical support for 7 days, like anything goes wrong apart from the issue which you have got today, and the issues that you are getting today, we insure that. All right, in future if you get that kind of issue in future-
Victim: Uh huh.
Scammer: There will be no charge to fix that. But if there are different issues, any kind of different issues-
Victim: Uh huh.
Scammer: Then only after 7 days there could be charge, and we would be providing you with the software with that as well.
Victim: I see.
Scammer: And the 1 time fix.
Victim: I see.
Scammer: All right?
Victim: All right.
Scammer: So shall we proceed, or uh, that's all upon you.
Victim: Yeah. Um, yeah I mean, you know, of course if I need, you know if I really need- if my computer really needs it then I guess I could get the $69.99.
Scammer: Yes, exactly. All right, no issue sir. Now, are you in front of the computer?
Victim: Yes I am.
Scammer: All right. And, it's a laptop or a desktop?
Victim: [00:04:00] It's a desktop.
Scammer: All right, so please look on the keyboard, at the left bottom of the keyboard.
Victim: Uh huh.
Scammer: And there, do you know how windows, what it looks like-
Victim: Yes, four squares-
Scammer: Windows button, the start button it looks like the flag, exactly you got it. So you're going to press and hold down that windows button, along with letter R, for Romeo, at the same time all right?
Victim: Okay. Yes, I did that.
Scammer: Press both, yes, windows as well as the letter R.
Victim: Uh huh. Yes, I got a little window that says 'Run.'
Scammer: Just type in there H-H- space-H.
Victim: Okay.
Scammer: You did that?
Victim: Should I click okay?
Scammer: Yes sir. H-H-space-H then click okay.
Victim: Okay, I did that.
Scammer: Now, do you see anything else?
Victim: Yes, there's another window in the top right that says, uh, uh-
Scammer: [inaudible 00:04:59], this page can not be displayed.
Victim: Yes.
Scammer: Can you maximize it?
Victim: Yes.
Scammer: Please do that.
Victim: Okay.
Scammer: Now sir, on the top left of that window you will see a yellow colored caution mark, with a small logo on it.
Victim: Right.
Scammer: Just click on it.
Victim: Okay.
Scammer: And then sir you will see jump to url, just set the second last option over there.
Victim: [inaudible 00:05:29]
Scammer: Jump to url.
Victim: Yes. Okay.
Scammer: Just click on that jump to url.
Victim: I clicked it, and there is another little window now.
Scammer: Okay, now type in there www.-
Victim: Yes.

Scammer: Lmi1, like L for Lima, M for Maria, I for Indiana, 1.com.

Victim: Click okay?

Scammer: Yes sir. [00:06:00] Lmi1.com.

Victim: Correct. Uh, okay.

Scammer: Now what do you see on the screen sir?

Victim: Uh, let's see. So it's working... Um, says support connection.

Scammer: All right, now let me just generate the code for you, from the Microsoft department. Just be hold , let me get the the code, 6 digit code all right?

Victim: Sure.

Scammer: [silence] Sir, I have got the code, please note it down.

Victim: Okay.

Scammer: That is 534-

Victim: 534, yes-

Scammer: 128.

Victim: Okay.

Scammer: And click on start download.

Victim: All right. Should I click on run, or save, or cancel?

Scammer: Run it. Sir, run it.

Victim: Okay. It says 'Do you want to run the software, [crosstalk 00:07:24]

Scammer: Run the software, yes exactly right.

Victim: Okay. Uh, use account control is enabled on this PC, please click okay-

Scammer: All right, you'll click okay.

Victim: And then it says, uh, do you want to allow the following program to make change-

Scammer: Allow it sir, allow it.

Victim: Okay. [silence] I [00:08:00] see. There's a little window, it says support session established with technician.

Scammer: All right, now press okay. Press okay over there.

Victim: Okay.

Scammer: You will see okay over there, press okay.

Victim: I clicked on okay.

Scammer: You did that?

Victim: Yes.

Scammer: All right now the Microsoft department do have the access of your computer, so just be hold, let me take the access on the different software-

Victim: Okay.

Scammer: And do not touch anything meanwhile.

Victim: Sure.

Scammer: Yes, thank you. [silence] All right sir, I do have the access now, do you see the team viewer?

Victim: Uh, yes I do.

Scammer: Yes, now this is the software from which I do have the remote access of your computer. Now let me check which antivirus you have at the moment in your computer. Oh, I don't see any of them.

Victim: I see. What does that mean?

Scammer: Sir, antivirus means a security virus protection software for your computer.

Victim: I see.

Scammer: Don't worry, we will provide you that, all right?

Victim: All right.

Scammer: You don't have to pay extra. Yes. This is the virus protection, no antivirus, windows update not there.

Victim: Right.

Scammer: Windows defender is not there. And the first and the foremost thing is network access protection. Network access protection isn't, so it is not running. That is turned off, all right? So this is something, all right?

Victim: Did I turn that off? Or did someone turn it off? I mean, I don't know.

Scammer: Sir, because of the viruses, your network protection has been turned [00:10:00] off. Because of the viruses in the computer. Okay?

Victim: I see.

Scammer: This is the reason, that is turned off. And now let me check how many viruses are there, in this computer.

Victim: Uh huh.

Scammer: [silence] Sir do you see that?

Victim: Yes I do.

Scammer: These are the viruses in your computer. They are 71! Seriously, that means a lot.

Victim: Wow.

Scammer: 71. And this is the last an unauthorized connection got that access off your computer. 10:31, I guess a while ago. If it's 12:52-

Victim: Right.

Scammer: And it is 10:31. So this is the thing which is going on at the moment, now let me check the services of the computer. Sir, do you see the services have been stopped? Stop, stop, stop.

Victim: Yes I do.

Scammer: Yes sir, these are the things that are going on at the moment, so many Microsoft services have been stopped right now on your computer. So there is something actually major, it should be turned on. It should be in running condition. But unfortunately they are not running, they are stopped right now. Okay?

Victim: I see.

Scammer: And, and do you see this thing, the [inaudible 00:11:31] agent, that is stopped?

Victim: Yes.

Scammer: So this is the main thing actually, if I were to have been, you know. I, if I wanted it to get it turned on from here, let me just scroll it from here . Do you see this network access is not running , that is off.

Victim: Yes, yes.

Scammer: If I wanted to turn it on, then I have to turn it on from here. Here is the option. But unfortunately, it is stopped from here as well. So this is something, all right?

Victim: All right.

Scammer: Everything has been stopped right now. Let me open the task [00:12:00] manager of this computer, and check the services. Oh, here they are. Let me just make it bigger. Now this is something, so is running, stop, stop, stop, stop, stop, stop, stop.

Victim: Right.

Scammer: Again, some of the services are running, some of the services have stopped right now. So this is something, going on with your computer. That is the reason there are charges upkeeping for the premium securities which I will provide you. All right sir?

Victim: Uh huh.

Scammer: So let me just scroll it down more, yeah stop, stop, stop, stop, you have a lot of things been going on. So these are the things all right? So now, you want to go for 1 time, all right?

Victim: Uh huh.

Scammer: Let me just open, yes, the notepad. Let me generate the computer, generate the problem sheet for you, here it is. And you see that, net framework system failure, and the computer has slow speed, network got compromised, browser got hijacked, that is the reason you are facing the pop ups.

Victim: I see.

Scammer: Security is not there, a virus protection security, network is also jammed, that has been compromised. Configuration negatively impacted, and trojans attack [inaudible 00:13:10].

Victim: Wow.

Scammer: All right. In order to fix this you need to put three softwares in your computer, that is Microsoft security installation, and Microsoft tools. First one is the antivirus from the Microsoft, all right? And the second one is, the tools to block the pop ups and viruses. And the third one is most- first and foremost thing, that is the network protection requirement, that is not there, all right? We need to put that on the server which you are using-

Victim: Uh huh.

Scammer: To protect this computer, in order to block all the pop ups in future, and unauthorized connections to your computer, all right?

Victim: Uh huh.

Scammer: Here, all right. Now let me just go and write it, 1 time fix, that is $69.9- sir, it's only about $20- it's $30 extra, why you are not going for $99.99? [00:14:00] You'll get 1 year service-

Victim: Right.

Scammer: 1 year service. So this, it’s all upon you. Because I don’t have to force you, that’s all, you know, that’s according to your budget. But, you know , after spending just $30 more, you will get it for 1 year, so this is the benefit you will get. Being a technician I would recommend you-

Victim: Right.

Scammer: To go for this, and everything is all upon you.