Dial One for Scam: A Large-Scale Analysis of Technical Support Scams

Najmeh Miramirkhani
Oleksii Starov
Nick Nikiforakis
What are Tech Support Scams?
<table>
<thead>
<tr>
<th>Year</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008</td>
<td>Fake support cold calls</td>
</tr>
<tr>
<td>2013</td>
<td>A Twist: Scammers started to use malvertising</td>
</tr>
<tr>
<td>2014</td>
<td>IC3 issued a public service announcement</td>
</tr>
<tr>
<td>2014</td>
<td>Microsoft sued several campaigns</td>
</tr>
<tr>
<td>2015</td>
<td>FTC took down several big campaigns</td>
</tr>
<tr>
<td>2016</td>
<td>IC3 issued a public service announcement</td>
</tr>
<tr>
<td>2017</td>
<td>Got more aggressive and still an increasing threat</td>
</tr>
</tbody>
</table>
Tech Support Scam (Cold Calls)
### Tech Support Scam Evolution

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008</td>
<td>Fake support cold calls</td>
</tr>
<tr>
<td>2013</td>
<td>A Twist: Scammers started to use malvertising</td>
</tr>
<tr>
<td>2014</td>
<td>IC3 issued a public service announcement</td>
</tr>
<tr>
<td>2014</td>
<td>Microsoft sued several campaigns</td>
</tr>
<tr>
<td>2015</td>
<td>FTC took down several big campaigns</td>
</tr>
<tr>
<td>2016</td>
<td>IC3 issued a public service announcement</td>
</tr>
<tr>
<td>2017</td>
<td>Got more aggressive and still an increasing threat</td>
</tr>
</tbody>
</table>
Tech Support Scam (malvertising)

1. **WARNING**
   Dangerous Virus Detected. Data at Risk.
   Call 123-456-7890

2. There are different kinds of abuse possible

3. To assess whether these databases include phone numbers
   - First, we check our collected 1,524 scam domains and phone numbers.
   - Secondly, we query VirusTotal for these domains to see if they are detectable by various A V engines.

Surprisingly, out of 1,524 scam domains, only 108 (7%) were detectable by, on average, 3.25 A V engines on VirusTotal.

- For the 685 resolved IP addresses, only 28 (4%) were already blacklisted, on average, 38 days after first detection of a malicious domain.
- i.e., approx. 64% were detectable by, on average, 3.25 A V engines.

To avoid reverse engineering each app, we opted to install each app in an Android emulator and simulate calls originating from scam numbers: Should I Answer? (left), CallDetector (right) before A Vs. Moreover, since VirusTotal houses 68 different A V engines, we argue that the vast majority of A V users are involved in technical support scams, we scrape six websites crowdsourced relying on users to submit complaints. In recent years, in addition to websites that users can utilize to look for complaints for any of our ROBOVIC-detected scams, we scrape six websites.
Potential breaking attempt! please call:
+1-866-793-2591
<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008</td>
<td>Fake support cold calls</td>
</tr>
<tr>
<td>2013</td>
<td>A Twist: Scammers started to use malvertising</td>
</tr>
<tr>
<td>2014</td>
<td>IC3 issued a public service announcement</td>
</tr>
<tr>
<td>2014</td>
<td>Microsoft sued several campaigns</td>
</tr>
<tr>
<td>2015</td>
<td>FTC took down several big campaigns</td>
</tr>
<tr>
<td>2016</td>
<td>IC3 issued a public service announcement</td>
</tr>
<tr>
<td>2017</td>
<td>Got more aggressive and still an increasing threat</td>
</tr>
</tbody>
</table>
Tech Support Scam Evolution

2008  Fake support cold calls
2013  A Twist: Scammers started to use malvertising
2014  IC3 issued a public service announcement
       Microsoft sued several campaigns
2015  FTC took down several big campaigns
2016  IC3 issued a public service announcement
2017  Got more aggressive and still an increasing threat
A neverending story: PC users lose another $120M to tech support scams

Court stops alleged scamming operations, but an end to the problem is elusive.

by Jon Brodkin - Nov 19, 2014 2:30pm EST
Growth of 200%

Symantec Report (2016)

Tech support scams

MILLION

JAN 2015  FEB  MAR  APR  MAY  JUN  JUL  AUG  SEP  OCT  NOV  DEC

$5.1 million in fines, retribution

Fraudsters masqueraded as Dell, Microsoft, McAfee, Norton and others
Research Goals

• Systematic study of Tech Support Scam ecosystem

• To investigate the:
  • Prevalence
    • # Domains, # Phone Numbers, and #Scam Campaigns
  • Details about the underlying infrastructure
    • Hosting providers, ASes, and Telecommunication companies
  • Evasion and social engineering techniques
    • Tools used, call-center infrastructures, and prices
Tool Design (Robovic)
At the same time, a necessary condition for gathering technical support-related data is the development of a reliable and highly automated detection tool with the technical support scam ecosystem. We describe ROBOVIC, the high-level view of our automated detection and collection of technical support scam pages.

Our tool for discovering and recording technical support scam pages is ROBOVIC. ROBOVIC uses a MITM proxy to record requests and responses, clicks on pop ups and logs the HTML code of the page. Finally, given the adversarial nature of technical support scams, we examine several heuristics, such as, having a redirection chain, showing consecutive alert dialogues, the presence of a phone number, and the presence of special characters in the URL. Note that we are not claiming equal probability, all scammers that are using advertising as a monetization method.

Figure 2 shows the high-level view of ROBOVIC's core components below:

- **Shortened URLs**
- **Typosquatting Models**
- **Popular Domains**
- **Scammers**
- **Advertising Networks**
- **Technical Support Scam Pages**
- **Other potential scam sources**

### Data Collection Methodology

Our study focuses on the collection of data for the given set of URLs and recording information about the resulting pages. To address the requirements of our study, 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 selected objects.

We deployed the ROBOVIC Crawler on three different sites: (our campus, Amazon's Elastic Compute Cloud, and on Windows OS). ROBOVIC uses a MITM proxy to record requests for the top 200 websites according to Alexa, and a set of 3,000 shortened URLs belonging to ten popular ad-based advertising networks. To find a sufficient number of high-toxicity, input streams of URLs, and the interactions of our crawlers with domain parking companies which will redirect a fraction of unused domain. Apart from hiding advertising profits from the domain owners, many domain parking companies have unused domain. We provided each instance with the use of the JavaScript-accessible, browser-provided function, we developed our crawler in such a way that allows the use of the JavaScript-accessible, browser-provided function, as well as a screenshot handler, as well as a screenshot of the page.

### Generality of our approach.

Methods [23] finding a large percentage of malvertising. Note that we are not claiming equal probability, all scammers that are using advertising as a monetization method.

### Technical Support Scams

The Crawler is in charge of browsing and collecting data for the given set of URLs and recording information about the resulting pages. To find a sufficient number of technical support scams, we analyze their unique characteristics. Therefore, as long as we visit typosquatting variants of popular domains, we discovered two pages which fit our definition of technical support scams and analyze their unique characteristics.
Collected Scam Domains

• Over 8 months
• Crawled 8 Million domains
• Resolved 5 Million domains
• Detected 22,000 scam URLs
• Extracted 8,600 unique scam domains
• 1500 phone numbers

Short and readable domains
- computer-warning-message[.]com
- donotclose[.]website
- input-error[.]net

Long with readable parts
- 10.computerhaveaseriousproblempleasecallon18776431254tollfree.yourcomputerhaveaseriousproblempleasecallon18776431254tollfree.yourcomputerhaveaseriousproblempleasecallon18776431254tollfree.browsersecurity16[.]club

URLs from CDNs
- 1073964613.rsc.cdn77[.]org
- 924983738.r.cdnsun[.]net
Weekly Scam Domains

The diagram shows the number of weekly scam domains detected by ROBOVIC instances over a 36-week period, starting from September 1, 2015. The x-axis represents the date, with three distinct periods: 15/10/01 - 16/01/01, 16/01/01 - 16/04/01, and 16/04/01 onwards.

- **Server** categories: Campus, Linode, and Amazon.
- **Campus Robovic** is the component of ROBOVIC responsible for tracking the data that ROBOVIC has collected. For this reason, we have collected a total of 15TB worth of crawling data.

### Analysis

1. **Discovered Scams**
   - The Liveness Checker is the final component of ROBOVIC which is responsible for tracking the data that ROBOVIC was exposed to during the monitored period. The website is hosted on a public cloud and we are not using any analytics software.

2. **Prevalence**
   - ROBOVIC attempted to resolve 8.4 million domains 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.

3. **Economic Impact**
   - The number of scam domains to which our campus-residing ROBOVIC instances responded correlates with the number of scam pages and phone numbers.

4. **Effect on Technical Support Scams**
   - Overall, our results indicate that, because ad networks and attackers are location-aware, proxy-less servers located on popular commercial clouds have only a small contribution to the total number of unique telephone numbers (see Figure 4). The website is hosted on a public cloud and we are not using any analytics software.

5. **Comparative Analysis**
   - In this section, we report on the data collected by ROBOVIC instances during our data-collecting period. One can see that while telephone numbers and domains are clearly correlated, the relationship between the two is not a 1-to-1 relationship.

### Data Collection

- **Prevalence**
  - ROBOVIC attempted to resolve 8.4 million domains 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.

6. **Mobile Advertising**
   - An alternative way of looking at the unique scam domains discovered by all three instances is to consider the number of domain names discovered by each of our three deployed instances. In terms of domain names, our campus-residing ROBOVIC discovered 95.7% of the domain names discovered by all three instances.

7. **Public Cloud Robovics**
   - ROBOVIC instances during our data-collecting period. One can see that while telephone numbers and domains are clearly correlated, the relationship between the two is not a 1-to-1 relationship.

- **Economic Impact**
  - The reason for this is that scams located on Amazon-residing ROBOVIC instances, contributing only 7.6% of the overall unique domains. Similarly, the same campus-names discovered by all three instances, with the Linode- and campus-residing ROBOVIC, discovered 95.7% of the domain names discovered by all three instances.

### Conclusion

- **Effect on Technical Support Scams**
  - Overall, our results indicate that, because ad networks and attackers are location-aware, proxy-less servers located on popular commercial clouds have only a small contribution to the total number of unique telephone numbers (see Figure 4). The website is hosted on a public cloud and we are not using any analytics software.

- **Comparative Analysis**
  - In this section, we report on the data collected by ROBOVIC instances during our data-collecting period. One can see that while telephone numbers and domains are clearly correlated, the relationship between the two is not a 1-to-1 relationship.

- **Mobile Advertising**
  - An alternative way of looking at the unique scam domains discovered by all three instances is to consider the number of domain names discovered by each of our three deployed instances. In terms of domain names, our campus-residing ROBOVIC discovered 95.7% of the domain names discovered by all three instances.

- **Public Cloud Robovics**
  - ROBOVIC instances during our data-collecting period. One can see that while telephone numbers and domains are clearly correlated, the relationship between the two is not a 1-to-1 relationship.

### Venn Diagram

- **Prevalence**
  - ROBOVIC attempted to resolve 8.4 million domains 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.

- **Comparative Analysis**
  - In this section, we report on the data collected by ROBOVIC instances during our data-collecting period. One can see that while telephone numbers and domains are clearly correlated, the relationship between the two is not a 1-to-1 relationship.

- **Mobile Advertising**
  - An alternative way of looking at the unique scam domains discovered by all three instances is to consider the number of domain names discovered by each of our three deployed instances. In terms of domain names, our campus-residing ROBOVIC discovered 95.7% of the domain names discovered by all three instances.

### Conclusion

- **Effect on Technical Support Scams**
  - Overall, our results indicate that, because ad networks and attackers are location-aware, proxy-less servers located on popular commercial clouds have only a small contribution to the total number of unique telephone numbers (see Figure 4). The website is hosted on a public cloud and we are not using any analytics software.

- **Comparative Analysis**
  - In this section, we report on the data collected by ROBOVIC instances during our data-collecting period. One can see that while telephone numbers and domains are clearly correlated, the relationship between the two is not a 1-to-1 relationship.

- **Mobile Advertising**
  - An alternative way of looking at the unique scam domains discovered by all three instances is to consider the number of domain names discovered by each of our three deployed instances. In terms of domain names, our campus-residing ROBOVIC discovered 95.7% of the domain names discovered by all three instances.
Scam Domains & phone Numbers

• Hiding backend servers (16% used Cloudflare)
• Anonymized registration information (55%)
• Abuse a small number of Telco companies
  • 80% of numbers belong to Twilio, RingRevenue (Invoca), WilTel
  • Prefer those that provide APIs
    • Scalable solution for the scammers’ business
• Number of phone numbers is much less than the number of domains
  • Phone numbers can link together domains of the same campaign
Fig. 6: which indicates that scammers are abusing some providers (united by supernetws{PMY}+@yahooNcom phone numbers. The right graph shows the relationship between domains and phone numbers appearing on scam pages, we plotted their network graph. In this graph, an undirected edge none of the vanity terms associated with the collected numbers of the phone numbers were activated less than one year ago and significantly more than others. Moreover, we discovered 77.5% of four providers (Twilio, WilTel, RingRevenue, and Bandwidth) telecommunication providers, more than 90% belong to only scams, we used a public database of toll-free numbers [29] to analysis systems, a large-enough corpus of scam domains may highlight that even though scammers attempt to hide from charmssprince@gmailNcom and the remaining 466 addresses we noticed patterns of simi-

TABLE I: Characteristics of the top five campaigns. D: Domains, P: Phone numbers

<table>
<thead>
<tr>
<th>#D</th>
<th>#P</th>
<th>TLDs Prefixes</th>
<th>#IPs/#ASs</th>
<th>Country</th>
<th>Top AS or CDN</th>
<th>Lifetime (days)</th>
</tr>
</thead>
<tbody>
<tr>
<td>888</td>
<td>877</td>
<td>1/1 US, NL</td>
<td>CloudFlare</td>
<td>64</td>
<td>Amazon</td>
<td>235</td>
</tr>
<tr>
<td>844</td>
<td>888</td>
<td>1/1 US, NL</td>
<td>CloudFlare</td>
<td>64</td>
<td>Amazon</td>
<td>250</td>
</tr>
<tr>
<td>844</td>
<td>877</td>
<td>33/9 US, IN, FR</td>
<td>CDN</td>
<td>Amazon</td>
<td>235</td>
<td></td>
</tr>
<tr>
<td>844</td>
<td>877</td>
<td>33/9 US, IN, FR</td>
<td>CDN</td>
<td>Amazon</td>
<td>250</td>
<td></td>
</tr>
<tr>
<td>844</td>
<td>877</td>
<td>33/9 US, IN, FR</td>
<td>CDN</td>
<td>Amazon</td>
<td>235</td>
<td></td>
</tr>
</tbody>
</table>

To gain insights on the N-N relationship between scam campaigns, we estimate the life time of scam campaigns by adding the lifetime of a campaign as the difference between the timestamps to the nodes of the network graph. We define 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. Even though the average lifetime of campaigns is not normal and 69% of the campaigns have a lifetime of less than 50 days. Moreover, assuming that the size of a campaign is equal to the number of nodes 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). The two largest clusters contained 60 and 83 unique, TLD+1 domain names and phone numbers. Black and gray nodes represent phone numbers and domain names/TLD+1 domains. The resulting graph contains 582 connected components of various sizes, of which 216 have a size of less than 5. This resulted in the formation of 192 clusters, including 65 clusters with at least two email addresses and 21 clusters with more than ten. The two largest clusters contained 60 and 83 unique, TLD+1 domain names and phone numbers.
Scam Campaigns

- Phone Number
- Domain Name
Life Time of Campaigns

Fig. 6: Two samples of technical support scam campaigns. The left graph indicates that scammers are abusing some providers' phone numbers. The right graph shows the relationship between unique domains and phone numbers appearing on scam pages, we plot 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 1,581 toll-free numbers belong to 15 different telecommunication providers, more than 90% belong to only four providers (Twilio, WilTel, RingRevenue, and Bandwidth) even though the 1,581 toll-free numbers belong to 15 different domain names and, vice-versa, a domain may advertise different phone numbers. There, we discovered that these numbers are the default numbers that scammers use to convince the users that their machines are infected with a virus. We note that one single domain may advertise more than six phone numbers, or six phone numbers can be connected to almost all of the campaign's subgraph. As Figure 6 shows, the distribution of the first and last domain or phone number joined to the same TLD+1 domain and replot the network graph. The average size of a node is proportional to the node degree.

Table I shows the characteristics of the top five campaigns. D: Domains, P: Phone numbers, V: Variations of scam domains. In Figure 6, we consider the case of technical support scam campaigns, we merge the domain nodes that have the same TLD+1 domain and replot the network graph. The Economic metric and grouped together addresses with a distance of 2.5 respectively. The maximum degree of phone nodes is 173, of domain nodes is 34. One sample of 582 connected components of various sizes, of which 216 connected components have more than 5 nodes. A sample of 582 connected components of various sizes, of which 216 connected components have more than 5 nodes. This resulted in the formation of 192 clusters, 65 clusters with at least two email addresses and the maximum degree of domain nodes is 34. One sample of 582 connected components of various sizes, of which 216 connected components have more than 5 nodes. This resulted in the formation of 192 clusters, 65 clusters with at least two email addresses and the maximum degree of domain nodes is 34.

Cumulative distribution function (CDF) of the lifetime of scam campaigns.

Fig. 7: Campaign Lifetime in Days

<p>|</p>
<table>
<thead>
<tr>
<th>Cumulative Probability</th>
<th>Campaign Lifetime in Days</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.25</td>
<td>20</td>
</tr>
</tbody>
</table>
Phone-TLD+1 Relationship

Generates Phone Numbers Dynamically

- Phone Number
- Domain Name
Pay Per Call Marketing

Publishers

1. WARNING
2. WARNING
3. Toll-free Number
4. Call
5. Call

Call Buyers

Prevalence
Modus Operandi Detection
Economic

Toll-free Number
844123456
866123456
800123456
Meeting the Scammers
Environment set up

• Obtained permission from our IRB
• 60 interactions with the scammers
• Environment:
  • Artificially aged Windows 7 virtual machine
  • Tunneling the traffic through VPN
  • VoIP software with believable CallerID
  • Capturing network traffic, recording the screen and conversations
Scammers’ Tools & Techniques

Social Engineering Techniques

Scammers’ Tools & Techniques

- Stopped Services/Drivers
- Event Viewer
- Specific Virus Explained
- System Information
- Action Center
- Fake CMD Scan
- Netstat Scan
- Installed/Running Programs
- Browsing History/Settings
- Downloaded Scanner
- Reliability/Performance
- Other (Temp, Registry)
Scammer Physical Locations & Profit
Location of Scammers’ Servers

- US (88%)
- India (3%)
- Netherlands (1%)
- Singapore (1%)
Location of Call Centers

- **India** (85%)
- **US** (10%)
- **Costa Rica** (5%)
Number of Victims

- Monitoring Traffic of Scam Servers:
  - Misconfiguration of scam servers revealed their traffic
    - 142 scam domains were found which had misconfiguration
    - We monitored misconfigured servers every one minute over two months
  - Total visits: 1.7 million unique IPs
  - Max #visitors/domain: 138K unique IPs
Location of Victims

- US (33%)
- Canada (7%)
- Australia (26%)
- Singapore (1%)
- New Zealand (5%)
Scammers’ Profit

Average price of Tech Support Scam Package ($290)

* 

Number of Victims (1.7 million unique IPs)

* 

Conversion Rate (2% as a similar scareware)

Scammers’ profit = ~ $9.7 million in 2 months
(a lower bound)
Defense: Sufficiency of Current Blacklists
## Blacklists: Phone Numbers

<table>
<thead>
<tr>
<th>Website</th>
<th>Database</th>
<th>Coverage</th>
<th>Claimed Size</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>mrnumber.com</td>
<td>19.9%</td>
<td>1.5 billion numbers</td>
</tr>
<tr>
<td></td>
<td>800notes.com</td>
<td>18.5%</td>
<td>Unknown</td>
</tr>
<tr>
<td></td>
<td>numberguru.com</td>
<td>1.0%</td>
<td>29 million lookups</td>
</tr>
<tr>
<td></td>
<td>badnumbers.info</td>
<td>0.2%</td>
<td>968,639 complains</td>
</tr>
<tr>
<td></td>
<td>callersmart.com</td>
<td>0.1%</td>
<td>5.9 million lookups</td>
</tr>
<tr>
<td></td>
<td>scamnumbers.info</td>
<td>0.1%</td>
<td>31,162 numbers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mobile App</th>
<th>Should I Answer?</th>
<th>0.5%</th>
<th>640 million lookups</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Truecaller</td>
<td>0.5%</td>
<td>2 billion numbers</td>
</tr>
<tr>
<td></td>
<td>Hiya</td>
<td>0.3%</td>
<td>100 million numbers</td>
</tr>
<tr>
<td></td>
<td>CallDetector</td>
<td>0.1%</td>
<td>100,000 complaints monthly</td>
</tr>
<tr>
<td></td>
<td>Mr. Number</td>
<td>0.1%</td>
<td>1.5 billion numbers</td>
</tr>
<tr>
<td></td>
<td><strong>Together</strong></td>
<td><strong>27.4%</strong></td>
<td>-</td>
</tr>
</tbody>
</table>
Blacklists: Domain Names

- 6 Blacklists (370K domains and IP addresses Together)

- 93% Detected Before Robovic
- 7% Detected After Robovic
- 0% Not Blacklisted

- hpHosts
- SANS suspicious domains
- malwaredomains
- malwaredomainlist
- Malc0de database
- abuse.ch
Why do blacklists not work?

• Tech Support Scams are highly dynamic
  • 30% of the domains are alive less than a day
  • Abusing CDNs to get fresh URLs
  • Majority of phone numbers registered recently
  • Phone numbers are generated dynamically
Defense against Tech Support Scam

• User Education
  • Explaining the concept of technical support scams is easier
  • Raising awareness through public services

• Browser Support
  • Average users do not know how to kill the browser process and clearing recent history
  • One universal shortcut to close unsafe pages
Summary

- Tech support scams pose a serious threat
- We conducted the first systematic study of tech support scams
- Reported prevalence of the scam and evasion techniques based on the collected corpus of thousands of domains and phone numbers
- Clustered campaigns and estimated their life time
- Interacted with 60 different scammers and identified the social engineering techniques
- Underline the need for user education and support from the browser vendors
Dial One for Scam:
A Large-Scale Analysis of Technical Support Scams

Najmeh Miramirkhani
Stony Brook University
nmiramirkhani@cs.stonybrook.edu

Oleksii Starov
Stony Brook University
ostarov@cs.stonybrook.edu

Nick Nikiforakis
Stony Brook University
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

Even though this type of scam costs users millions of dollars on a yearly basis [1], [2], 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