pindrop

Call me: Gathering threat intelligence on telephony scams to detect fraud

Aude Marzuoli, Hassan A. Kingravi, David Dewey,
Aaron Dallas, Telvis Calhoun, Terry Nelms, Robert Pienta
Data Science Team, Pindrop

1 Abstract

Robocalling, voice phishing and caller ID spoofing are common cybercrime techniques used to launch scam campaigns through the telephony channel that many people have long trusted. More than 660,000 online complaints regarding unwanted phone calls were recorded on the top six phone complaints websites in 2015. More reliable than online complaints, a telephony honeypot provides complete, accurate and timely information about unwanted phone calls across the United States. By tracking calling patterns in a large telephony honeypot receiving over 600,000 calls per month from more than 90,000 unique source phone numbers, we gathered threat intelligence in the telephony channel. Leveraging this data we developed a methodology to uniquely "fingerprint" bad actors hiding behind multiple phone numbers and detect them within the first few seconds of a call. Over several months, we recorded more than 100,000 calls and analyzed several million call records to validate our methodology. Our results show that only a few bad actors are responsible for the majority of the spam and scam calls and that they can be quickly identified with high accuracy using features extracted from the audio. This discovery has major implications for law enforcement and businesses that are presently engaged in combatting the rise of telephony fraud.

2 The current state of telephony fraud

2.1 Telephony is the weakest link in security.

Stronger online and mobile security, recent data breaches, and the rollout of chip cards in the US means cybercriminals are changing tactics, exploiting the weakest link in the security chain: telephony.

Telephony spam and fraud are major concerns because of the low level of security in the telephony channel compared to most other communication channels [1]. Email spam has led to a multi-billion dollar anti-spam industry [2]. On the other hand, phone spam and scams are typically perceived as a nuisance rather than a serious threat, and are therefore less studied and understood, along with their associated tactics and value chain. Attacks on the telephony channel have recently increased, and this trend can be attributed to the availability of IP telephony (Voice over Internet Protocol) [3]. Automated VoIP calls can now be made at no or low cost at scale, from the United States or overseas, similar to email spam. Cybercriminals are already exploiting the telephony channel to craft large-scale attacks such as voice phishing (vishing) [4] using techniques like spoofing [5] and robocalling [6]. Such attacks do not have a sole aim to extort money directly from victims who are tricked into sharing their credit card informatio.Rather, many spammers and scammers aim to enhance their existing incomplete profiles of victims, to use later to impersonate their victims at financial institutions, whether through the phone channel or online. Cybercriminals regularly exploit social engineering over the phone to reset online credentials in order to steal money from a bank account [7], surrender an insurance policy or take out a loan. Telephony has become the weak link even for web security.

2.2 VoIP allows bad actors to launch large attacks at low cost in the telephony channel.

Consumers across the United States are receiving an increasing volume of unwanted calls. The Federal Trade Commission (FTC) has received millions of complaints from US residents about unwanted and fraudulent calls [6]. Websites, such as 800notes.com [8], gather thousands of daily comment regarding unsolicited calls.

Large-scale phone scams now regularly make the news headlines. The most famous ones include:

- Scam 419 where the victims are convinced to send cash upfront by promising them a large amount of money that they would receive later if they cooperate [9];
- A purported debt relief operation that allegedly contacted consumers through prerecorded telemarketing calls, falsely claimed it would reduce their unsecured debt, but instead made unauthorized charges to their bank accounts [10];
- The tech support scam, where consumers were tricked into paying for the removal of bogus viruses on their computers and gave the scammers remote access to their computers [12,13];

- Deceptive and abusive debt collection practices relying on lies and intimidation techniques [11];
- The wangiri fraud scam where the victim's phone only rings once, then the victim calls back and gets charged for calling back [14];
- Swindlers who overloaded emergency dispatch centers because of a surge of automated calls (Telephony Denial of Service attack) [15].

Social engineering following voice phishing attacks leads victims to reveal confidential information, such as birthdays, personal addresses, and credit card numbers, which are later used to impersonate the victims and take over their financial or personal accounts [16].

3 Introduction to a telephony honeypot

3.1 Our telephony honeypot receives more than 600,000 calls per month from about 90,000 source phone numbers across the United States.

Honeypots have been used widely to collect threat intelligence in computer networks, with applications to email spam [17], malware [18], and more generally attacks on such networks [19]. However, there has been limited research on telephony honeypots. One of the first works done in this direction was the development of the Phoneypot by Gupta et al. [20]. However, it did not provide insight on the telephony fraud ecosystem. A priori, there may be thousands or just few bad actors perpetrating attacks on the telephony channel. Contrary to other communication channels, very little information on a phone call is readily available besides the source phone number (which may not be a legitimate or a valid number and cannot be trusted a priori), the time of the call, and sometimes its duration. Spammers and fraudsters using emails, social network platforms [21], or even SMS [22] usually leave a link to a website and semantic information is readily available in the corresponding email, tweet, or SMS. The sheer volume of unwanted calls combined with the fact that any phone number can be spoofed [23] makes telephony fraud identification a non-trivial task.

3.2 A telephony honeypot is more reliable than crowd sourced complaints and provides real-time, actionable insight.

Our telephony honeypot received about 8,000,000 calls in 2015 from approximately 880,000 distinct source phone numbers to nearly 80,000 distinct destination phone numbers. 58% of sources call once or twice. Therefore obtaining historical information on a given source to apply machine learning techniques is challenging. During most of 2015 (except for a few weeks when we conducted experiments), calls were never answered. The calls received are entirely unsolicited, and our destination phone numbers never placed any calls. In 2015, 660,145 online comments were scraped from the top five websites about phone numbers complaints, reporting 74,000 source phone numbers as unwanted callers (see Table below).

Data set	Number of calls /comments	Number of source phone numbers	Maximum number of calls/comments per source phone number
Honeypot	8,000,000	880,000	21,329
Online comments	660,000	74,000	2,156

The honeypot and the online comments are both partial observers of the telephony world, hence we examine whether the observations from these two sets are related. The source phone numbers calling the honeypot and those getting complained about in the online comments significantly overlap. 1.8% of source phone numbers from the honeypot and 21% of source phone numbers reported in the online comments are identical. In the honeypot, these sources placed 36% of all calls, with an average of 145 calls per source. In the comments set, these sources were responsible for 66% of all comments, with an average of 26 comments per source. In summary, identifying the bad actors behind 1.8% of sources in the honeypot has the potential to address 66% of online complaints.

4 Fingerprinting bad actors hiding behind several phone numbers

4.1 We extract sets of calls with their associated phone numbers that correspond to the same spam/scam campaign.

Once a call is recorded, its audio is transcribed to a text file using Kaldi [24]. Kaldi is a free open-source speech recognition toolkit. Transcripts are imperfect and contain spelling and grammatical mistakes, but identical recordings are transcribed into very similar transcripts.

The transcripts are then pre-processed before we apply natural language processing techniques. Stop words, such as prepositions or adverbs, are removed from transcripts. The remaining words are lemmatized (i.e. the endings of the words are removed) and each transcript is stored as a bag-of-words. In machine learning and natural language processing, topic models are algorithms used to analyze large volumes of unlabeled text documents. They uncover patterns and thematic structures in document collections. LSI [25] is a dimensionality reduction technique that projects documents and document queries into a space of smaller dimension, called the “topic space”, than the original space of dictionary words they were expressed in. The intuition behind LSI is that there is a set of independent underlying variables that span the meanings behind the data.

Once each transcript has been mapped to a lower dimensional projection, these projections can be compared in the space of topics. Cosine similarity is computed between the projections of any pair of transcripts, which is normalized between 0 and 1, with 1 indicating identical projections.

From the pair-wise similarity scores computed across the whole corpus, an n by n similarity matrix is constructed. The similarity matrix obtained for both recordings experiments are pictured in Figure 1. The darker the blue dot between row i and column j, the more similar transcript i is to transcript j . The fact that the diagonal of the matrix is dark blue is expected, since each transcript is maximally similar to itself.

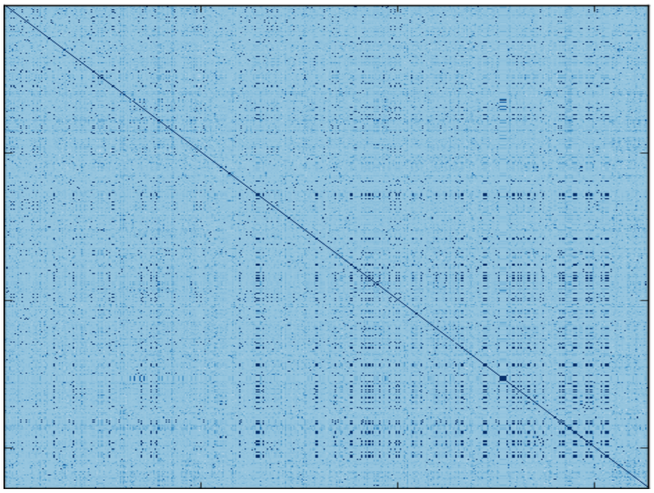

Figure 1: Raw similarity matrix between all pairs of transcripts. A dark dot indicates that transcript i is similar to transcript j.

Initially, we tried clustering on transcripts directly, instead of clustering on projections in the topic space. However, because many transcripts from different spam and scam recordings use identical words even though the recordings are different, it was not effective. Hence we introduce the extra step of performing a dimensionality reduction before clustering. Clustering algorithms address the classical unsupervised learning problem of finding a partition for a given set of items. There are often many ways to partition the data. Spectral clustering [26] is a powerful non-parametric technique to uncover structure in data using the spectrum of a pairwise similarity matrix. The results of applying spectral clustering on the similarity matrix are shown in Figure 2. The data suggests that a set of phone numbers are fraudulent when all their calls cluster, indicating that all the callers are either playing the same recording or they are humans reading from the same script. A good cluster is a cluster with very high average intra-cluster similarity, i.e. corresponding to a group of identical recordings. A dark square block in Figure 2 corresponds to a subset of identical transcripts (which are all perfectly similar to one another). Then the corresponding source phone numbers propagating the same scam or spam campaign behind the corresponding calls can be identified.

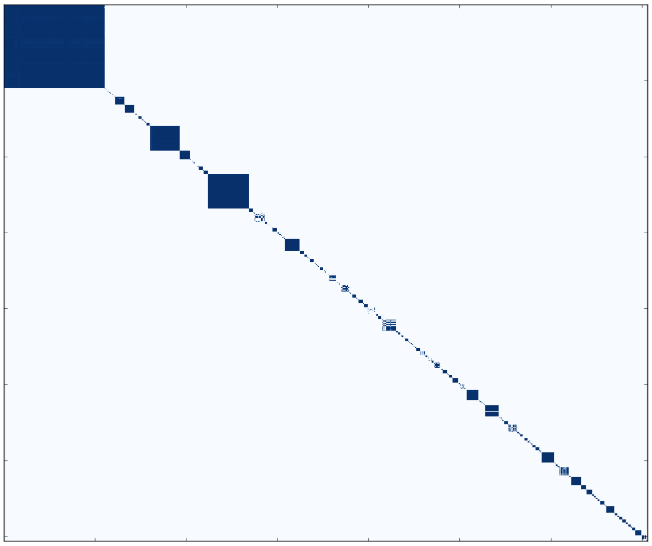

Figure 2: Spectral clustering results. A dark dot indicates that transcript i is similar to transcript j.

4.2 By building models of the audio signature, or "phoneprints", of any telephony infrastructure used by spammers/scammers, we show that only a few telephony infrastructures are responsible for the majority of robocalls.

Pindrop's Phoneprinting ™, a patented technology, analyzes phone calls to identify malicious behavior and verify legitimate callers. Phoneprinting takes an audio call and breaks it down into 150 unique call features to create an audio fingerprint of a telephony infrastructure. Fraudsters often change phone numbers, but it is much harder to change the audio characteristics that Pindrop uses to create a unique identifier for the call audio characteristics. Phoneprinting is highly resilient and detects the techniques fraudsters use to hide their true number or impersonate a legitimate caller. In addition, this technology identifies multiple callers associated with the same phoneprint, allowing enterprises to detect and track fraud rings. Phoneprinting is the only technology that can see through these attacker tactics.

Phoneprinting compares the information reported with Caller ID to the true device and location information to find anomalies that indicate spoofing. Fraudsters are practiced in the art of manipulating people into giving up confidential information or breaking normal security procedures. Phoneprinting exploits the information the caller cannot control, such as spectrum (quantization, frequency filters, codec artifacts), noise (clarity, correlation, signal to noise ratio), and loss (packet loss, robotization, dropped frames).

By using clustering on the similarity matrix between transcripts, we obtain clusters of transcripts, and hence clusters of audio recordings. Phoneprinting clusters of recordings from different source phone numbers enables us to overcome the fact that most phone numbers only call once or twice in the honeypot. The experiments we conducted showed that phoneprinting clusters provides better results than phoneprinting a phone number alone, especially for robocallers and telemarketers. The intuition behind this is as follows: if several calls are placed from a given phone infrastructure, their audio features tend to be highly similar in the audio feature space. Bad actors tend to use several distinct phone numbers to perpetrate the same scam. Indeed, we saw in the honeypot the exact same recording being played by several phone numbers. Even if the caller is relying on spoofing to hide behind several source phone numbers, if he or she calls from the same infrastructure, the audio features of the call recordings will be highly similar. Hence, the hypothesis is that clusters in the topic space will also tend to cluster in the audio space, except that the semantic information associated with the transcript space will allow for more accurate groupings.

To prove this point, audio features are extracted from recordings associated with clusters with high similarity in the topic space, and are systematically phoneprinted. Across fifty phoneprints, the average training TPR obtained was 85.5%, and the average testing FPR was 0.25%. The maximum training TPR was 98%. Our results show that phoneprinting a cluster may perform very well even with less than two calls per source phone number on average. Another advantage of the methodology developed is that it enables catching bad actors hiding behind "restricted" or "anonymous" phone numbers, or spoofing phone numbers. Several clusters from the random recordings data set contained "anonymous" calls. When the caller calls again, from any phone number, he or she will be flagged as the same caller by extracting the audio features.

About one third of the unsolicited calls received by our honeypot are robocalls. The remaining calls are a combination of telemarketing calls or real persons calling a number that previously belonged to an individual or a business. Now comes the most surprising result of this study, which has deep implications for defense strategies. After clustering calls, the largest 38 clusters account for 51% of robocalls. Said otherwise, 51% of robocalls are placed by only 38 distinct telephony infrastructures, and we have identified their audio signature. Even if the bad actors operating these infrastructures change the said infrastructure, it will only take a few robocalls to be able to build a new audio signature. This means that the massive nuisance and threat that robocalls represent for consumers can be tackled. The next steps of this research effort will focus on locating these infrastructures using the audio signature.

5 Tracking of scam campaigns in time

A recent survey [27] found that in 2015, 11% of U.S. consumers lost money to a telephone scam. The survey estimates 27 million U.S. consumers lost approximately $7.4 billion to the schemes, that is an average of $274 per victim. Depending on the spam or scam campaign, different populations are targeted, from seniors concerned about life insurance or burial policies, to households struggling with financial issues, to businesses trying to increase their visibility.

We have identified more than a dozen variants of "Google scams", impersonating different Google products, from Google maps to Google plus, and have been tracking their life cycle over several months. The results show the different tactics used by scammers to get victims to pick up the phone and divulge personal information, from asking you to pay a small fee upfront to pretending that you need to verify information.

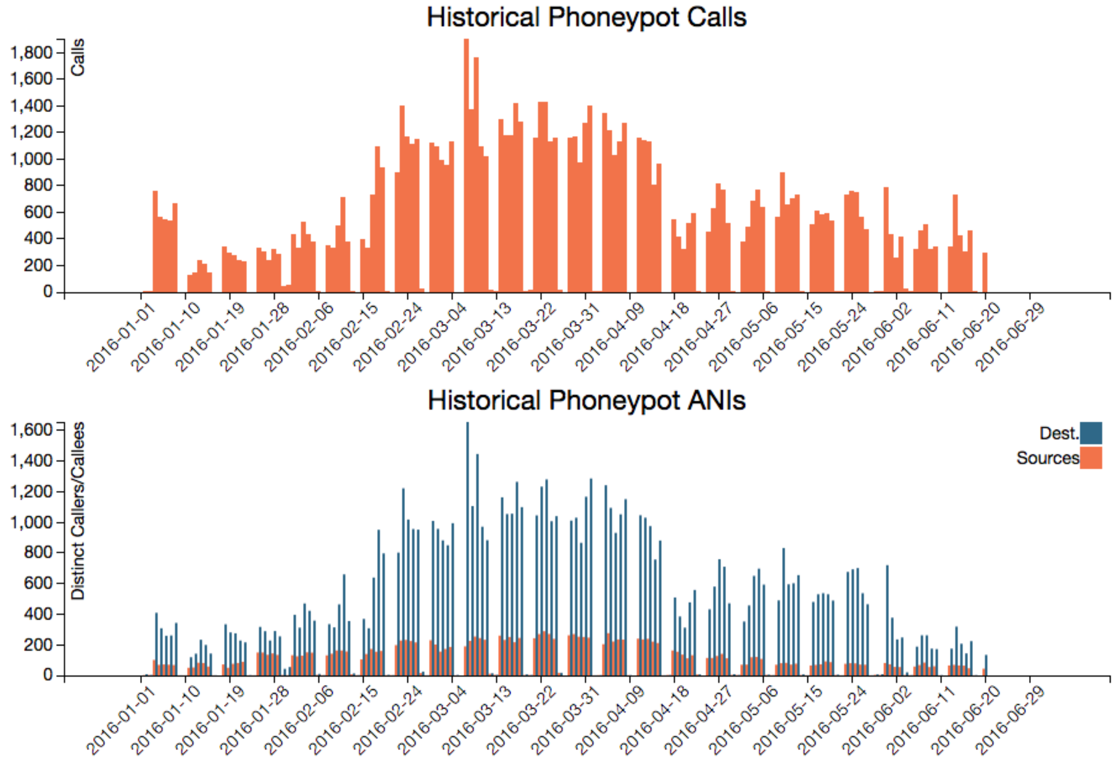

Figure 3: Honeypot traffic related to Google from January to July 2016.

The following is a transcript of a Google-related robocall: "Hi this is Sharon your local Google specialist. We have a front page position available for a business like yours and can guarantee front page placement with unlimited clicks 24 hours a day at a flat rate on Google. Press the one key right now to see if you qualify and are interested in receiving calls from companies who are locally searching for your type of business. Please press one now or press the two key to be removed. Thank you."
253 source phone numbers played this particular recording during 27,928 calls to 17,160 destination phone numbers between January and July 2016. The corresponding traffic is typical of massive robocalling in the US, as shown in Figure 4. Most destinations are only called once, and if called twice, it is typically by different source phone numbers. We obtained a phoneprint performance of 93.4% TPR at 0.4% FPR for the corresponding cluster of calls.

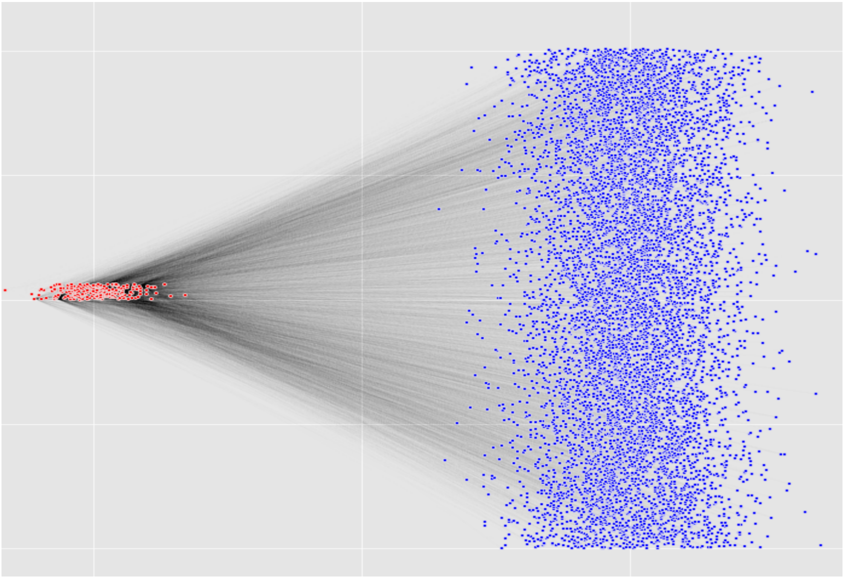

Figure 4: Honeypot traffic related to "Sharon, your local google specialist". A red dot represents a source phone number; a blue dot a destination phone number in the honeypot, and an edge represents a phone call playing this recording.

The following is another transcript of a Google-related robocall: "This is an important call regarding your Google business listing. We need to verify your contact information. Press one now to verify your Google business listing. Press seven to remove yourself from the verification system. "

410 source phone numbers played this particular recording during 34,048 calls to 26,841 destination phone numbers between January and July 2016, as shown in Figure 5. We obtained a phoneprint performance of 92.7% TPR at 0.2% FPR.

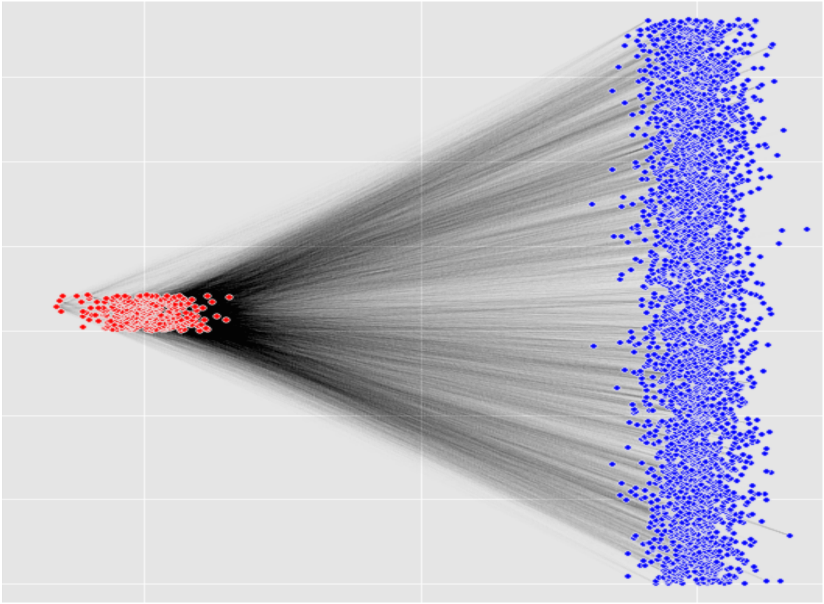

Figure 5: Honeypot traffic related to “your Google business listing”. A red dot represents a source phone number; a blue dot a destination phone number in the honeypot, and an edge represents a phone call playing this recording.

A completely different robocalling behavior is observed for debt collectors. One particular debt collector, which is not necessarily legitimate, plays the following recording: “This call is from XXXX outsourcing, a debt collector. Please return my call at 866-XXX-XXXX. “ 7 source phone numbers played this particular recording during 1,301 calls to 92 destination phone numbers between January and July 2016, as shown in Figure 5. Contrary to the previous examples, this particular robocaller relies on targeted harassment tactics, calling the same destinations over and over for months.

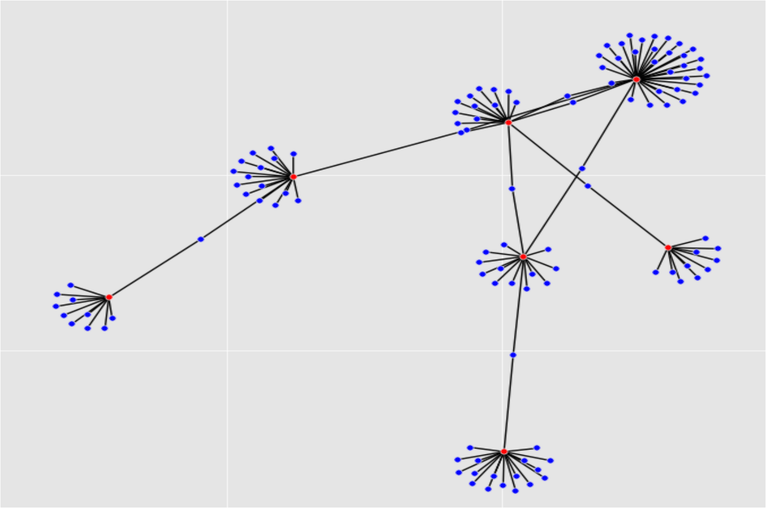

Figure 6: Honeypot traffic related to a particular debt collector. A red dot represents a source phone number, a blue dot a destination phone number in the honeypot, and an edge represents a phone call playing this recording.

6 Closing remarks

We gathered threat intelligence in the telephony channel by tracking calling patterns in a large telephony honeypot receiving over 600,000 calls per month from more than 90,000 unique source phone numbers. Applying machine learning, we automatically group robocalls by scam-type using semantic information collected from the call audio. Leveraging this data we developed a methodology to uniquely “fingerprint” bad actors hiding behind multiple phone numbers and detect them within the first few seconds of a call.

Over several months in 2016, our honeypot received over one million calls from more than 210,000 source phone numbers. We recorded about 100,000 calls from 44,000 source phone numbers. About one third of these calls were robocalls. Our results show that 51% of the robocalls recorded can be attributed to only 38 distinct telephony infrastructures and that they can be quickly identified with high accuracy using features extracted from the audio.

7 References:

[1] Results of worldwide telecom fraud survey, (accessed December 1, 2015). http://www.cfca.org/pdf/survey/CFCA2013GlobalFraudLossSurvey-pressrelease.pdf.

[2] DHAMIJA, R., TYGAR, J. D., AND HEARST, M. Why phishing works. In Proceedings of the SIGCHI conference on Human Factors in computing systems (2006), ACM, pp. 581–590.

[3] KEROMYTIS, A. D. A comprehensive survey of voice over ip security research. Communications Surveys & Tutorials, IEEE 14, 2 (2012), 514–537.

[4] OLLMANN, G. The vishing guide. http://www. infosecwriters.com/text resources/pdf/IBM ISS vishing guide GOllmann.pdf, IBM, Tech. Rep (2007).

[5] MUSTAFA, H., XU, W., SADEGHI, A. R., AND SCHULZ, S. You can call but you can't hide: Detecting caller id spoofing attacks. In Dependable Systems and Networks (DSN), 2014 44th Annual IEEE/IFIP International Conference on (2014), IEEE, pp. 168–179.

[6] How does a robocall work?, (accessed January 31, 2015). https://www.ftc.gov/sites/default/files/documents/public_events/robocalls-all-rage-ftc-summit/pdf-0113-robocalls-infographic.pdf

[7] Lifecycle of a Phone Fraudster, (accessed January 31,2015). www.blackhat.com/docs/us-14/materials/us-14-Balasubramaniyan-Lifecycle-Of-A-Phone-Fraudster-WP.pdf

[8] Directory of Unknown Callers, (accessed December 1, 2015). http://www.800notes.com/

[9] 419 Scam Directory, (accessed December 1, 2015). http://www.419scam.org/

[10] FTC Action Halts Debt Relief Marketing Operation, (accessed December 1, 2015). https://www.ftc.gov/news-events/press-releases/2012/09/ftc-action-halts-debt-relief-marketing-operation

[11] FTC and Federal, State and Local Law Enforcement Partners Announce Nationwide Crackdown Against Abusive Debt Collectors, (accessed December 1, 2015). https://www.ftc.gov/news-events/press-releases/2015/11

[12] FTC Halts Massive Tech Support Scams, (accessed December 1, 2015). https://www.ftc.gov/news-events/press-releases/2012/10/ftc-halts-massive-tech-support-scams

[13] FTC, Pennsylvania and Connecticut Sue Tech Support Scammers That Took More Than $17 Million From Consumers, (accessed
December 1, 2015). https://www.ftc.gov/news-events/press-releases/2015/11

[14] PSA: Missed Call From A Mystery Number? Be Careful. (accessed December 1, 2015). http://techcrunch.com/2014/02/02/missed-call-scam/

[15] Swindlers Use Telephones, With Internet Tactics, (accessed December 1, 2015). http://www.nytimes.com/2014/01/20/technology/swindlers-use-telephones-with-internets-tactics.html?_r=0

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

[17] RAMACHANDRAN, A., AND FEAMSTER, N. Understanding the network-level behavior of spammers. ACM SIGCOMM Computer Communication Review 36, 4 (2006), 291–302.

[18] DAGON, D., QIN, X., GU, G., LEE, W., GRIZZARD, J., LEVINE, J., AND OWEN, H. Honeystat: Local worm detection using honeypots. In Recent Advances in Intrusion Detection (2004), Springer, pp. 39–58.

[19] FAWCETT, T., AND PROVOST, F. Adaptive fraud detection. Data mining and knowledge discovery 1, 3 (1997), 291–316.

[20] GUPTA, P., SRINIVASAN, B., BALASUBRAMANIYAN, V., AND AHAMAD, M. Phoneypot: Data-driven understanding of telephony threats. In 22nd Annual Network and Distributed System Security Symposium, NDSS 2015, San Diego, California, USA, February 8-11, 2014 (2015), The Internet Society.

[21] THOMAS, K., MCCOY, D., GRIER, C., KOLCZ, A., AND PAXSON, V. Trafficking fraudulent accounts: The role of the underground market in twitter spam and abuse. In USENIX Security (2013), Citeseer, pp. 195–210.

[22] JIANG, N., JIN, Y., SKUDLARK, A., HSU, W.-L., JACOBSON, G., PRAKASAM, S., AND ZHANG, Z.-L. Isolating and analyzing fraud activities in a large cellular network via voice call graph analysis. In Proceedings of the 10th international conference on Mobile systems, applications, and services (2012), ACM, pp. 253–266.

[23] CASTIGLIONE, A., DE PRISCO, R., AND DE SANTIS, A. Do you trust your phone? Springer, 2009.

[24] POVEY, D., GHOSHAL, A., BOULIANNE, G., BURGET, L., GLEMBEK, O., GOEL, N., HANNEMANN, M., MOTLICEK, P., QIAN, Y., SCHWARZ, P., SILOVSKY, J., STEMMER, G., AND VESELY, K. The kaldi speech recognition toolkit. In IEEE 2011 Workshop on Automatic Speech Recognition and Understanding (Dec. 2011), IEEE Signal Processing Society. IEEE Catalog No.: CFP11SRW-USB.

[25] WIEMER-HASTINGS, P., WIEMER-HASTINGS, K., AND GRAESSER, A. Latent semantic analysis. In Proceedings of the 16th international joint conference on Artificial intelligence (2004), Citeseer, pp. 1–14.

[26] NG, A. Y., JORDAN, M. I., WEISS, Y., ET AL. On spectral clustering: Analysis and an algorithm. Advances in neural information processing systems 2 (2002), 849–856.

[27] Consumer Affairs, Survey: 11% of adults lost money to a phone scam last year. https://www.consumeraffairs.com/news/survey-11-of-adults-lost-money-to-a-phone-scam-last-year-012616.html