The DEF CON 23 Social Engineering Capture The Flag Report

www.social-engineer.org

sectf@social-engineer.org

Written by: Michele Fincher & Chris Hadnagy

Table of Contents

Executive Summary

Social-Engineer.org hosted the Social Engineering Capture the Flag (SECTF) contest at DEF CON 23 in Las Vegas, Nevada for the sixth year in a row in August of 2015. This year's competition targeted major telecommunications providers.

From over 100 entries, we selected 14 competitors from diverse backgrounds and experience levels to test their social engineering abilities via the telephone. Below is a table highlighting some basic statistics from this year's competition:

Target Companies	14
Competitors	14
Completed Calls	150
Total Points Scored on Reports	1696
Total Points Scored on Calls	6772

Table 1: Overview of the SECTF

As in years past, the overall goals of this contest were to raise awareness of the ongoing threat posed by social engineering and to provide a live demonstration of the techniques and tactics used by the potential malicious attacker. There were very strict rules of engagement in place to ensure no sensitive information on companies or individuals was disclosed. To further protect employees of target companies from potential negative repercussions, identities of those contacted is neither recorded nor retained.

It is important to note that the reporting of a target company's overall performance is a combination of points scored by their assigned contestant in both Open Source Intelligence (OSINT) gathering and live call phases of the contest. The scoring alone contained within this report does not necessarily indicate that one company is less secure than another company. However, it is an indicator of the potential vulnerabilities that exist and demonstrates that despite training, warnings and education, social engineering is still a very serious and viable threat to corporations.

Overview of the SECTF

The Social Engineering Capture the Flag (SECTF) is an annual event held within the Social-Engineer Village at the DEF CON Hacking Conference in Las Vegas, NV. The SECTF is organized and hosted by Social-Engineer.Org, the noncommercial, educational portion of Social-Engineer, LLC.

The competition was formed to demonstrate how serious social engineering threats are to companies and how even novice individuals could use these skills to obtain damaging information. The contest is divided into two parts, the information-gathering phase that takes place prior to DEF CON, followed up by the live call phase that occurs at the DEF CON conference.

Background and Description

The SECTF is a contest in which participants attempt to obtain specific pieces of information, called flags, from select private-sector companies. The purpose of the contest is to demonstrate how much potentially damaging information can be freely obtained either through online sources or via telephone elicitation.

Months prior to the DEF CON event, we solicited for individuals who wished to compete via our social media outlets and www.social-engineer.org website. This year we required participants submit a 90-second video outlining their goals for the contest. Our panel made selections based on a number of factors to include desire to learn as well as our perception of the contestant's intent. As this is an educational event, we wish our participants to have a very strong emphasis on ultimately helping the status of corporate security as opposed to the singular goal of "winning" an engagement. From over 100 applicants, we selected 14 contestants and randomly assigned them to a company.

Based on major trends and breaches during the year, we selected telecommunications as the target industry. These are brands that US customers rely on regularly that have access to both personal and financial information of the average consumer.

Contestants were not made aware of any other competitors or target companies other than their own prior to their show time at the live event.

In addition, we sent an overview of flags, rules, targets and other pertinent information to our legal counsel. We make this a practice every year to ensure we are staying within the legal boundaries we set for ourselves when we started this competition.

Contestants were given 3 weeks to gather as much information about their target company as possible and generate a report. They were allowed to use only Open Source Intelligence (OSINT) that could be obtained through search engines or tools such as Google, LinkedIn, Facebook, Twitter, Maltego, etc. During this information-gathering phase, contestants could attempt to capture as many of the pre-defined flags as possible. The information gathered was to be assembled into a professional social engineering report. Contestants were provided with a sample report to assist them, but were not required to use this template. In addition to the flags, points were also awarded based on the professionalism and quality of the report, with 10 bonus points awarded for reports submitted early.

Contestants were then assigned a time slot to perform their live calls on either Friday or Saturday during DEF CON 23 in Las Vegas, NV.

Great care was taken in the development of the contest to ensure maximum success for the contestants. Since the contest was held on the West Coast, companies whose headquarters were located on the East Coast were assigned earlier time slots. Furthermore, companies who were easily accessible during non-standard business hours, such as retail, were assigned Saturday time slots.

Contestants were placed in a soundproof booth and required to provide a list of phone numbers (obtained during the information-gathering stage) at the target company to call along with phone numbers they wished us to spoof. Caller ID spoofing is a method through which one's incoming phone number can be forged, or "spoofed". This is a tactic commonly used by social engineers to increase their credibility with recipients. This year the contestant's option to spoof was determined based on a coin flip.

This year we had 4 scheduled contestants who were no-shows. We solicited for volunteers from the audience and held a random drawing to select 2 replacement contestants. The stand-ins were provided extra time to review the target's report and prepare to make calls. In addition, we allowed spoofing for both in consideration of their last minute participation.

Each contestant was free to use their entire allotted 25-minute time slot to perform as many or as few calls as they wished. Although United States federal law only requires one party to be

notified in the event of recording a telephone call, many states (Nevada included) have created additional laws requiring both parties to consent. Since we could not obtain the consent of target companies without jeopardizing the integrity of the contest, no recording of any type was permitted (including that by the audience). Photographs were allowed with permission of the contestant.

Scoring was accomplished during each call by three judges. Based on very positive feedback from last year, we again took time after each contestant to discuss the calls with the audience. During that time, we analyzed the success of the calls, techniques used, and answered as many questions directed to either judging panel or contestant as time allowed. Subsequent to the contest, scoring and comments were reviewed along with the reports submitted prior to DEF CON to determine the winners.

It should be noted that all 14 contestants were required to place a $20 *fully refundable* deposit to reserve their spot at the contest. All contestants were refunded this deposit immediately after completing their call at the DEF CON portion of the contest.

Description of the 2015 Parameters

Overall, we attempt to keep the *major* parameters of the competition as consistent as possible from year to year. However, we do make changes to ensure that the contest continues to be challenging and educational for both contestants and audience.

Primary changes:

- Early report submissions were awarded 10 additional points
- The contestants were allowed 25 (versus 30 allotted last year) minutes to perform their calls
- The ability to spoof was determined via coin toss at the beginning of each contestant's time slot
- The target companies were all telecommunications companies
- Substitute contestants in the case of 2 no-shows was determined through a random drawing

Target Companies

The Social-Engineer staff, through an open nomination and voting process accomplished target selection. We made every attempt to ensure that no bias was introduced through attitudes or preconceived notions regarding any particular company. In general, we attempted to select Fortune 500 or larger companies from the telecommunications sector. Although the overall security of all companies is important, we believed that a continued emphasis on companies that have access to customer personal information was crucial. The vast majority of telecommunications providers require data such as date of birth and SSN to open accounts. As in previous years, we made the call for companies to be willing participants in the SECTF. No companies volunteered; therefore none of the companies chosen were aware of their selection prior to the DEF CON conference.

The target list (in alphabetical order):

1. AT&T
2. Century Link
3. Comcast
4. DirecTV
5. Dish Network
6. Frontier Communications
7. Sprint Corporation
8. T-Mobile
9. Time Warner Cable
10. U.S. Cellular
11. Verizon Wireless
12. Virgin Media
13. Vonage
14. Windstream Communications

Competitors

As in all previous years, one of our core rules is that ***no one*** is victimized. This includes those who choose to participate, those who are called, and the companies they work for. Our contestant's personal information is never revealed and they are only photographed if they provide explicit verbal permission prior to their live call segment at DEF CON. No video recording of contestants during their calls is ever permitted due to two-party consent laws in the state of Nevada.

There were 14 competitors selected from an original pool of over 100 applicants. Not all were skilled callers or experienced social engineers. For many, this was their first attempt at ever placing a deliberate social engineering-based call. Some of the contestants were red team or security specialists, but many were from other fields not related to social engineering or information security.

Flags

A "flag" is a specific piece of information that the contestants attempted to obtain in both the OSINT and live call portions of this competition.

The following table outlines the list of specific flags, their categories, and point values for 2015:

DEFCON 23 Social-Engineer.Org SECTF Flag List		
Logistics	**Rpt Pts**	**Call Pts**
Is IT Support handled in house or outsourced?	3	6
Who do they use for delivering packages?	3	6
Do you have a cafeteria?	4	8
Who does the food service?	4	8
Other Tech		
Is there a company VPN?	4	8
Do you block websites?	2	4
If website block = yes, which ones? (Facebook, EBay, etc.)	3	6
Is wireless in use on site? (yes/no)	2	4
If yes, ESSID Name?	4	8
What make and model of computer do they use?	3	6
What anti-virus system is used?	5	10
Can Be Used for Onsite Pretext		
What is the name of the cleaning/janitorial service?	4	8
Who does your bug/pest extermination?	4	8
What is the name of the company responsible for the vending machines onsite?	4	8

Who handles their trash/dumpster disposal?	4	8
Name of their 3rd party or in house security guard company?	5	10
What types of badges do you use for company access? (RFID, HID, None)	8	16
Company Wide Tech		
What operating system is in use?	5	10
What service pack/Version?	8	16
What program do they use to open PDF documents and what version?	5	10
What browser do they use?	5	10
What version of that browser?	8	16
What mail client is used?	5	10
Do you use disk encryption, if so what type?	5	10
Fake URL (getting the target to go to a URL) www.seorg.org	N/A	26
Employee Specific Info		
How long have they worked for the company?	3	6
What days of the month do they get paid?	3	6
Employees schedule information (start/end times, breaks, lunches)	3	6
What is the name of the phone/PBX system?	4	8
When was the last time they had awareness training?	5	10
Report Scoring		
Half points for any flag found from information gathering	**	**
10 points each for each realistic attack vector detailed in the report to a maximum of 50 points. Supporting evidence must be provided for each attack vector as to why it is realistic.	10-50	
Format, structure, grammar, layout, general quality of the report a maximum of 50 points.	0-50	

Table 2: Flag List for 2015

Scoring

Contestant report scoring for the OSINT phase was accomplished manually using the guidelines from Table 2. Flags obtained during this phase of the contest were worth **half-points.**

Scoring during the live telephone calls was accomplished using a proprietary application specifically designed for Social-Engineer. Flags captured during this portion of the event were awarded full points (please see Table 2). The same flag could be captured multiple times by the contestant either by contacting different targets on the same call (e.g., through being transferred) or on subsequent calls within the allotted 25 minutes. For example, if the contestant reached three different people and convinced all three to navigate to the website of the contestant's choosing (a flag worth 26 points), they would have received seventy-eight points. Every attempt was made to ensure consistency in scoring for all contestants, regardless

of the judge, although our scoring process does provide some subjectivity through the ability to include notes and comments for each contestant.

In addition to determining the SECTF winner based on points totals, we also conducted an analysis of how the target companies fared in response to a social engineering attack. It follows that the interpersonal skills and overall preparation of the contestant was highly predictive in the outcomes indicated by both scores as well as subjective assessments of performance by the judges. Unfortunately, a company cannot rely on the hope that a malicious social engineer will be inexperienced, unskilled, or unprepared upon which to base their sense of corporate security.

Rules of Engagement (R.O.E)

Contestants are held to very strict rules to ensure the protection of target companies as well as their employees. The core rules remained the same as in previous years. We did not allow the collection of sensitive data such as credit card information, social security numbers, and passwords. Only Open Source Intelligence (OSINT) was allowed. We did not allow physical (i.e. facility) or technical (i.e. network) penetration into companies. In addition, we did not allow the contestant to visit any location of their target or interact with any person from the target before the calls at DEF CON. We also specifically avoided sensitive industries such as government, education, healthcare, and finance.

The most important rule stressed to all contestants is that there was to be absolutely no victimization of any target companies. For more specific information on the ROE, please visit us here: http://www.social-engineer.org/ctf/def-con-23-sectf-rules-registration/.

Results and Analysis

High profile events in the last calendar year are illustrative of the fact that corporations, and specifically telecommunications companies, continue to be poor at protecting critical information. Unfortunately, this year's SECTF supported this trend as our contestants, both experienced and newcomers were able to obtain flags both through OSINT and the live calls. Our findings are detailed in the sections that follow. It should be noted that any comparisons to previous years' performance is for subjective trend analysis only. Since populations and sample sizes are not equivalent across years, statistical analysis is not appropriate and was not performed.

Open Source Intelligence Gathering

Preparation prior to any social engineering engagement is critical. It is this phase that is the most time-consuming and laborious, but can most often determine the success or failure of the engagement. The professional social engineer must be aware of all of the information-gathering tools freely available as well as the many accessible locations online that house valuable pieces of data.

The following table is a list of tools commonly used by professional social engineers as well as our contestants during the OSINT phase of the SECTF:

Google	Picasa Web	Spokeo
Maltego	WhoIs	YouTube
FriendFinder	WGet	FourSquare
Bing/Yahoo	Vimeo	Friendster
Twitter	Tineye	theHarvester
PiPl	WaybackMachine	Google Images
Bing Images	LinkedIn	Telnet
Facebook	Monster	EchoSec
Plaxo	GlassDoor	DuckDuckGo
Google Maps	Yelp	BackTrack
Wordpress	Craigslist	Kali Linux
Shodan	JigSaw	Pinterest

Table 3: Commonly-Used OSINT Tools

We were generally very impressed with the quality of the research, and the reporting by contestants continues to improve. One very interesting point that is consistent with last year's trend is that our competitors did not appear to locate as much OSINT on their targets as in past years. Historically, points scored by competitors during the OSINT portion of the contest far outweighed those scored during calls. This trend was completely reversed last year and it was observed again this year. Even adjusting for half versus full points awarded between OSINT and calls does not diminish the strength of the effect. The effect is even more notable given that two of the no-show competitors this year were not replaced, so the total call points for 2015 is

reflective of 12 targets versus the entire 14 that underwent OSINT investigation. Figure 1 illustrates the very similar point distribution profiles observed both last year and this year.

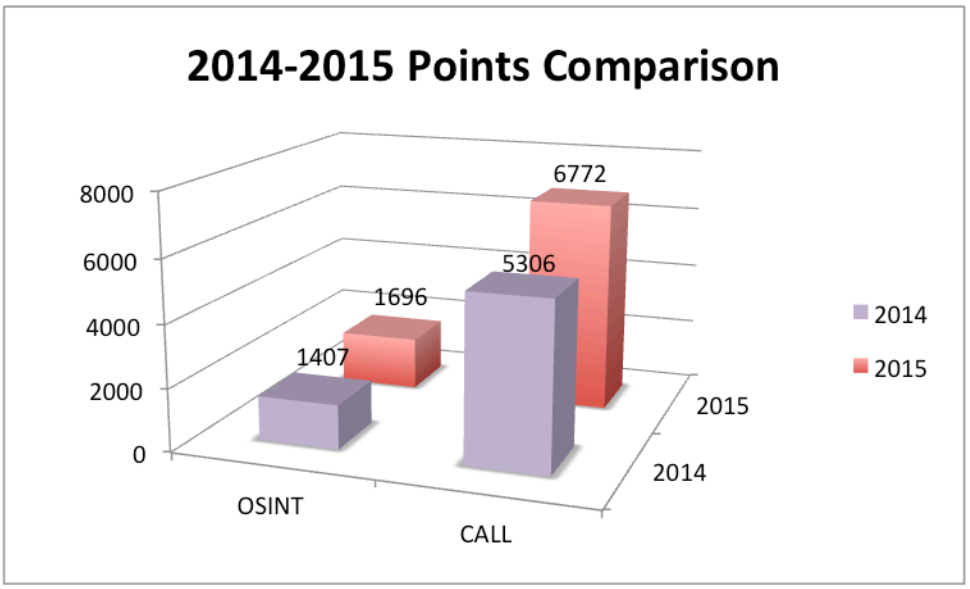

Figure 1: Comparison of OSINT/Call Points Awarded, 2014-2015

Please note the totals themselves are not comparable across years since the numbers of competitors and scoring conditions changed; this is only to illustrate the similar point distributions between 2014 and 2015.

Subjectively, we do not feel that the scoring is an indicator of the level of effort or attention to detail on the part of our contestants. Despite comparatively lower scores, the quality of information found was excellent and is still potentially very damaging to companies.

The following small list of this year's findings demonstrates that the danger posed by social engineering information gathering is extremely prevalent. Any of the following pieces of information could be used by a malicious attacker to further develop vishing, phishing, or onsite impersonation attacks. Major categories are as follows:

Employee Information

- Many of our contestants located employee data in a number of different locations. In some cases it was simply data aggregation sites or web forums, while in one particular case it was discovered that an employee union posted lists of their members online. The

information discovered included full names, user ID numbers, job titles, work start dates, full work addresses, direct phone numbers, pay schedules, break times, etc.

- Multiple employee email addresses and passwords were located as a result of recent data breaches.

Technologies

- Numerous lists of internal tool names and systems used by target companies were located.
- A company was discovered to allow anonymous FTP logins, meaning any remote user would be able to connect without providing credentials and access files available on the FTP server.
- Publicly facing websites of target companies provide the network SSID and password.
- A target company advertises the specific antivirus tool used for their customers.
- Documents were located that provide information about the target company's RFID system and badge layout.
- Publicly facing PHP Easter Egg discloses application versioning, installation paths, and application arguments.
- There was more than one instance in which companies placed logins either to the internal network or to mail clients on public-facing websites, which could allow unauthorized user access.
- One company's website error disclosed the operating system in use.
- The existence of, and SSIDs of, wireless networks were discovered through publicly available databases that catalogue wardriving data.

Physical Plant

- Publicly facing websites contain internal headquarter photographs.
- One company was found to post extensive corporate and contractor guides for accessing their facilities, to include how to obtain badging.

Contractor/Vendor/Other Companies

- The technology partner of a target company was found to have ISO image files of the company's computers openly accessible (this included POS, call center, and bill payment kiosks).

- Non-sanitized documents posted by one company were located. An inspection of metadata revealed significant information regarding the document's authors to include the emails of other corporate entities, suggesting a relationship that could be exploited.
- Media articles/general web pages were located, that identified third-party vendors and subcontracting companies working for the target companies.
- A publicly available document provided the name of the VOIP provider for the target company.

Special Notes

- Photo analysis from sources such as Google Earth, Instagram, Fouresquare, Facebook and Glassdoor proved to be especially useful for our competitors. A short list of items discovered includes: physical plant information such as location of security desks, location of break areas, technologies in use (including computers and badging), and third party vendor information.
- Social media accounts of numerous target employees were located. Employees often disclosed information to include details regarding technology, systems, and infrastructure employed at their companies, as well as other pertinent details such as pay schedule and specific job functions. Many employees (particularly executive level individuals) possess LinkedIn accounts that are not private, providing significant information to attackers.

Figure 2 provides a side-by-side comparison of points scored by competitors against their assigned company during the OSINT portion of the contest, out of a possible 225 points. The X-axis represents the competitors, and the Y-axis the point values for total points awarded for this phase of the competition.

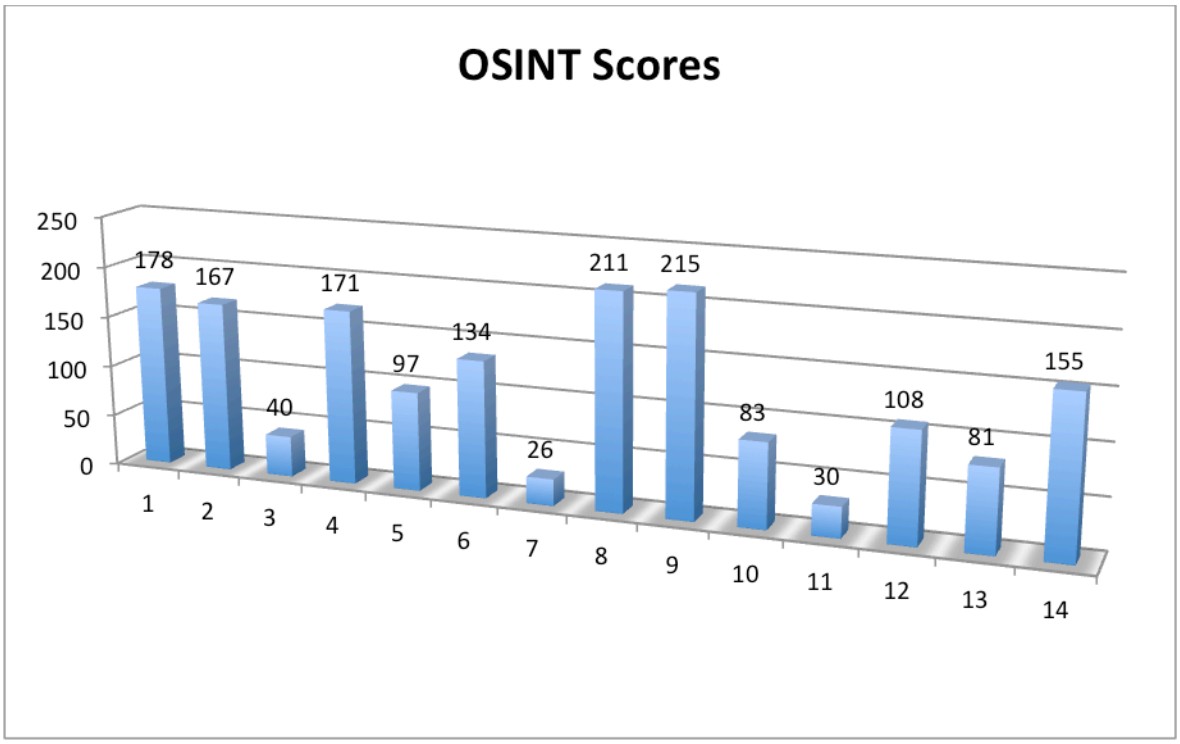

Figure 2: OSINT Scores by Competitor

The OSINT portion of our competition stresses a few key points. First, this emphasizes the overall importance of the information-gathering phase of any social engineering engagement. A thorough online investigation can provide an individual with a very good understanding of when, where, and how companies conduct business as well as the online activities of their employees through vectors such as social media. Second, any images found can be extremely useful for malicious attackers. For instance, if an attacker knows what buildings look like, the location of entrances and break areas, and perhaps even finds pictures of corporate badges, these are all potential vulnerabilities. Finally, our OSINT exercise stresses the issue of online data leakage by organizations. Network penetration was not allowed; the flags during the OSINT phase were obtained through information freely found online *without any live interaction with individuals at the target companies.*

Pretexting

We saw a continuation of past years' trend in which the vast majority of successful pretexts involved the impersonation of fellow corporate employees from either IT or human resources. Impersonating a fellow employee is a common pretext used by malicious attackers, taking

advantage of "tribe mentality." We inherently trust people who are part of our group or tribe. When a social engineer displays information to support that s/he is an internal employee, it is easier for the target to let their guard down and trust the person with what might normally be considered confidential information. This is also where good OSINT was key for contestants, allowing them to reference internal language, systems, or personnel in a quick and natural fashion.

Some interesting observations from this year's calls with respect to pretexts:

- Providing a clear reason for calling was critical. Contestants who did not clearly introduce themselves or their pretexts were unable to overcome questions and objections.

- Prudent use (not overuse) of authority was highly successful. Effective contestants used pretexts that relied on the authority of their positions and framed their requests in a fashion that did not allow for non-compliance (I'll just need you to answer a few questions, thanks so much for your help…").

- Caller ID spoofing to lend credibility to pretexts appeared to have very little relation to the success of calls. Figure 3 outlines the total of all call scores versus spoof status (determined by random coin toss). This effect is particularly interesting given that of the top 4 contestant call scores, only 1 was awarded the ability to spoof. Although professional social engineers rely consistently on caller ID spoofing, our finding may be an indicator that the ability to spoof has a greater effect on the caller's confidence and comfort level than the target's compliance.

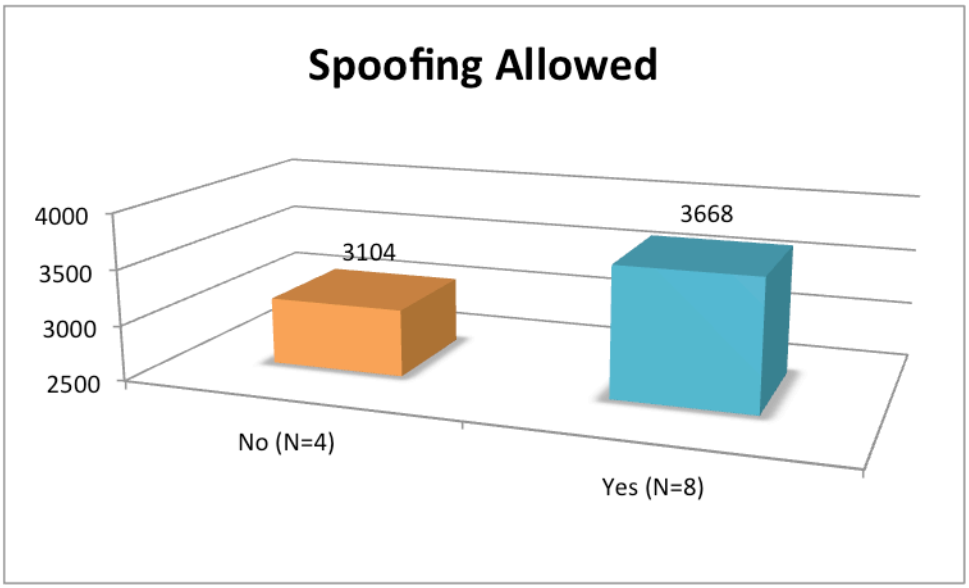

Figure 3: Spoofing Status vs. Call Scores Total

Live Call Performance

The live call portion of the SECTF is an interesting trial for the contestant. It is not only a test in mental agility and the ability to influence a person in real-time, but also a task that must be accomplished in front of a live audience. The luxury of time and true anonymity enjoyed in the OSINT phase are not applicable. It is for that reason we congratulate all of our contestants in completing this phase of the competition.

Figure 4 quantifies point values scored by the contestants against their assigned company during the live call portion of the contest. The X-axis represents the contestants and the Y-axis the point values awarded. It should be noted that there were 4 total no-shows, of which we replaced 2 for a total of 12 live call competitors.

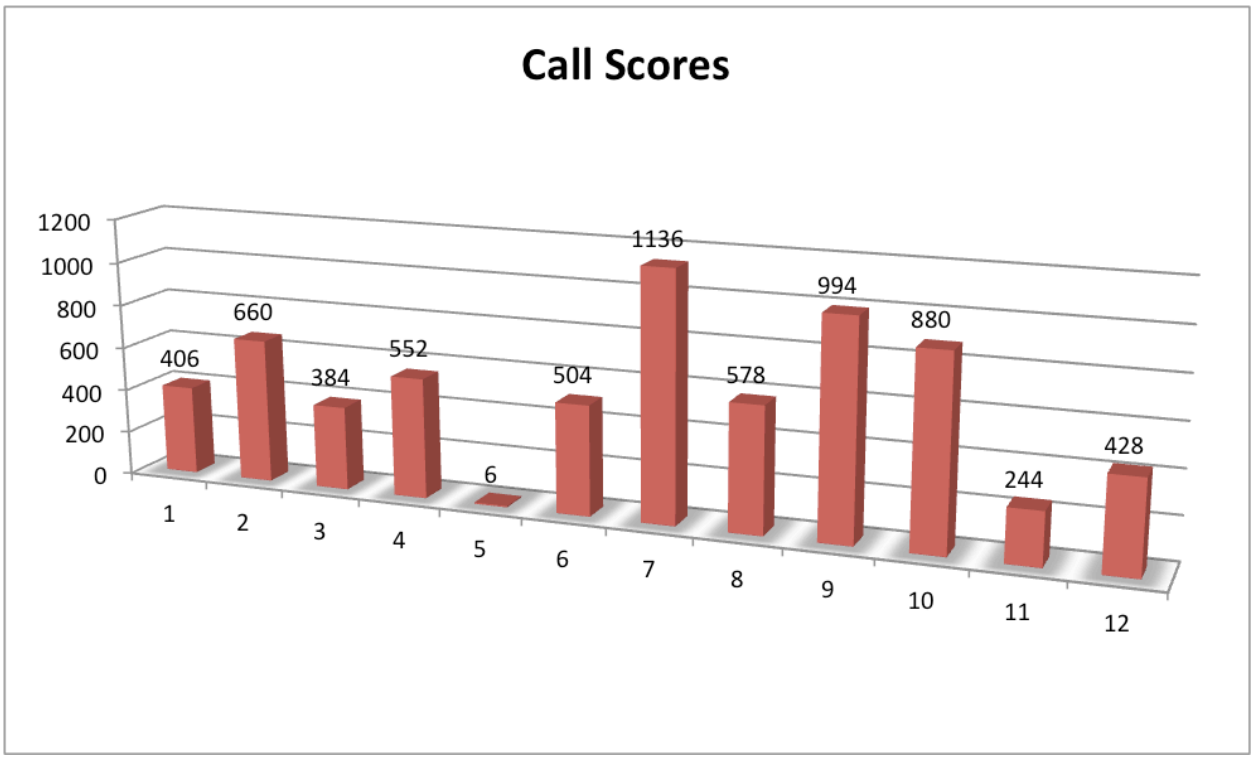

Figure 4: Live Call Scores by Competitor

By examining Figure 4, it is clear that performance of competitors varied widely; however, the majority of scores clustered around the average score of 564 (interestingly, this middle cluster includes both stand-in competitors). Again, of the top 4 scores, only 1 competitor won the ability to spoof.

The following are observations made during calls.

- Competitors who were the most successful:
    - Were very well prepared. They had conducted thorough OSINT and possessed more than enough possible targets/phone numbers to call. They were also familiar with internal terminology, systems, or processes.
    - Were extremely persistent. They did not end calls with initial objections, and in many cases, recalled the same targets to continue escalation of requests. One of our competitors did not obtain any flags until his very last call.

  - Dealt well with an unpredictable environment. This contest illustrates the difficulty of live calling. Our best competitors thought quickly on their feet and were able to adjust pretexts and questions even when the call appeared to be going poorly.
  - Were able to establish rapport with their targets. The most effective competitors sounded friendly and comfortable, despite competing in front of a live audience.
  - Organized their flags such that their requests flowed naturally based on pretext.

- Competitors who had the most difficulty:
  - Were vague with introductions and attempted to elicit flags prior to establishing who they were or why they were calling.
  - Abandoned the calls quickly after initial resistance was provided.
  - Had difficulty balancing how much time to spend on establishing pretext and rapport with actual elicitation. Although a clear introduction of the pretext and establishment of rapport are critical, some contestants spent an excessive amount of time explaining themselves as opposed to using their allotted time judiciously for collecting flags.
- Techniques:
  - A number of successful competitors escalated their requests from small to large.
  - One competitor added credibility to his pretext by stating that the call may be recorded for training purposes.
  - A number of successful competitors phrased their elicitations as confirmation of information they already knew (collected in the OSINT phase).
- Additional observations:
  - One competitor obtained almost all of her information from a security contractor of the target company, who had access to the corporate network. Although the testing of contractors is often not in scope in standard security penetration testing, organizations need to be aware that anyone who has access to internal information is a potential vulnerability.

- One target company's phone system disclosed the type of software and hardware in use and provided a directory that listed the full name and extension of personnel.

Competitor Summary

Although we had our typical range of novice social engineers to professional penetration testers, average performance for this year appeared to remain relatively stable compared to last year as demonstrated in Figure 5. However, since we make changes to the conditions, number of competitors, and scoring each year (e.g., extra points for "tag-outs" in 2014), these averages are only valuable in terms of identifying large trends such as the data reversal we saw in 2014 that has continued this year. The mathematical average is also impacted by outlying scores (either very high or very low), so are relatively limited in the information it conveys. One *can* surmise that perhaps competitors this year continued to emphasize call phase preparation and performance over the OSINT phase.

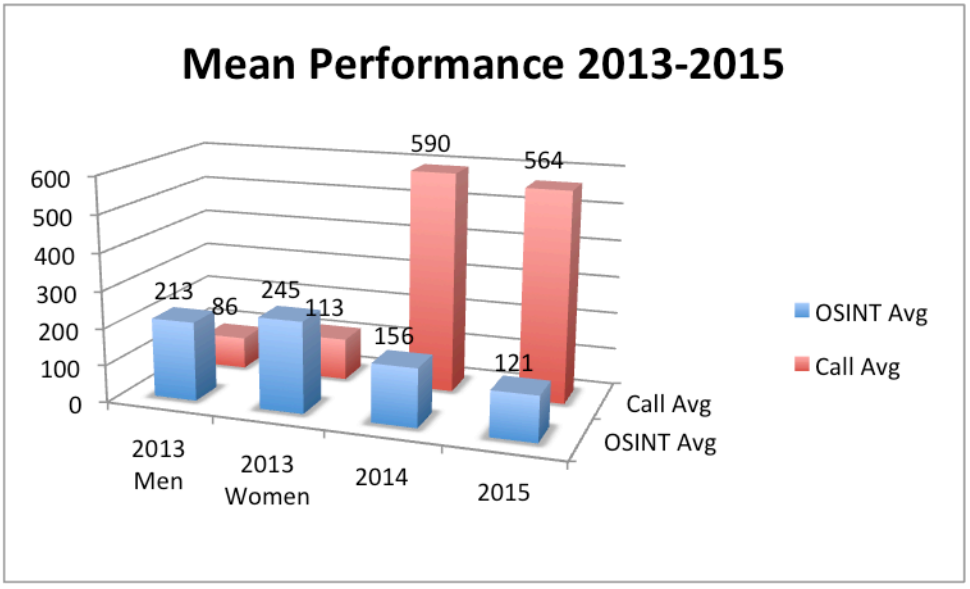

Figure 5: Mean Performance for SECTF, 2013-2015

Final Contest Results

At the conclusion of the live call portion of the contest, the judging panel met and reviewed all scores. Figure 6 is a tally of OSINT scores, call scores, and grand total by company. The higher score denotes that a higher number or value of flags were surrendered, and is indicative of poorer performance on the part of the company. Please note that live call no-shows for both

Time Warner and ***Comcast*** were not replaced, so their performance is comparable to other companies only for the OSINT phase of the competition.

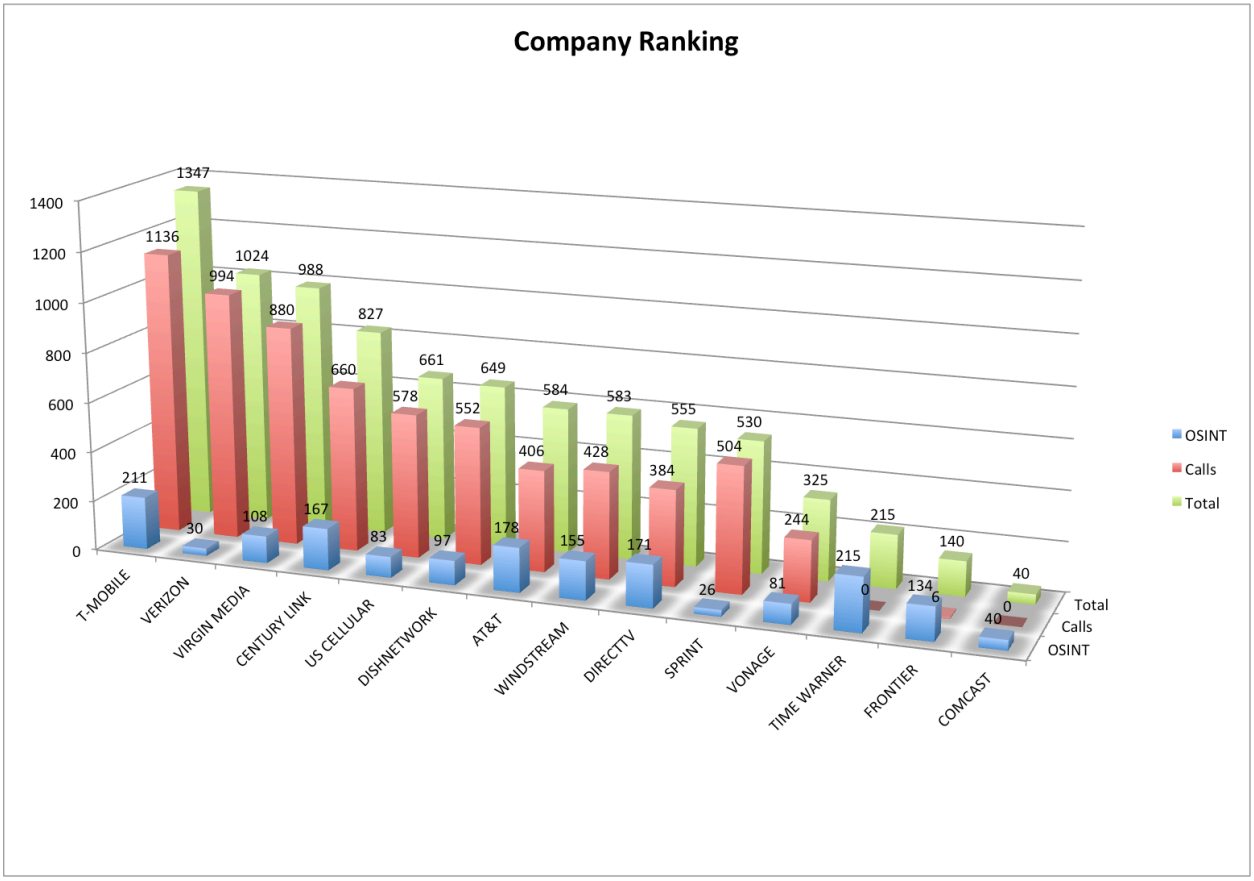

Figure 6: Company Ranking

Even a cursory examination of the scores confirms the heavy reliance by competitors on call scores over OSINT for placement this year. In every applicable situation, the target company either revealed or surrendered at least some information.

In summary, overall performance of companies in order of ***best*** to ***worst*** *(this does not include the two companies that were not called)*:

1. Frontier Communications
2. Vonage
3. Sprint Corporation

4. DirecTV
5. Windstream Communications
6. AT&T
7. Dish Network
8. U.S. Cellular
9. Century Link
10. Virgin Media
11. Verizon Wireless
12. T-Mobile

We do not release additional information regarding specific vulnerabilities of the companies to the general public.

NOTE - *We do provide this information directly to the involved companies upon request.*

One positive aspect of the live call portion of the SECTF each year is to see when a company shuts down the contestant. That is, the person from the target company follows appropriate security protocol and does not answer any questions or hangs up on the call. Each year when a person from a target company stops a contestant, the room breaks out into applause.

This year we did have calls during which:

- The target claimed to not be able to answer questions posed and disconnected.
- The target passed the call to a manager after being told a false employee number by our competitor.
- The organization demonstrated responsiveness to a detected intrusion by denying our competitor a request (navigate to unknown URL) that had been readily granted during the first few calls.

Despite these positive notes, overall, this year's contest proved once again that potentially damaging information on organizations is still either easily accessible online or discovered via telephone calls by even the most novice competitor.

Figure 7 illustrates the number of times each flag was obtained during both OSINT and live call phases. While not all flags were requested the same number of times, this is at least an indicator of likely vectors into an organization. Inspection will reveal that the most commonly obtained flag this year was what operating system was in use at the company, followed by browser version and whether or not IT support was in-house or outsourced. These informational flags have the potential for dangers via malicious attackers using this information for a technical attack of known vulnerabilities, or to perpetrate believable attacks using phishing, additional vishing, and via onsite impersonation attempts.

The take-away here is that social engineering is not the endgame, but is used as the entry point to perpetrate theft of identity or resources. The motivated individual will compile information from a number of different sources and create believable attacks that are difficult to recognize and resist.

It is interesting to note that EVERY applicable flag was surrendered at least once by the target companies.

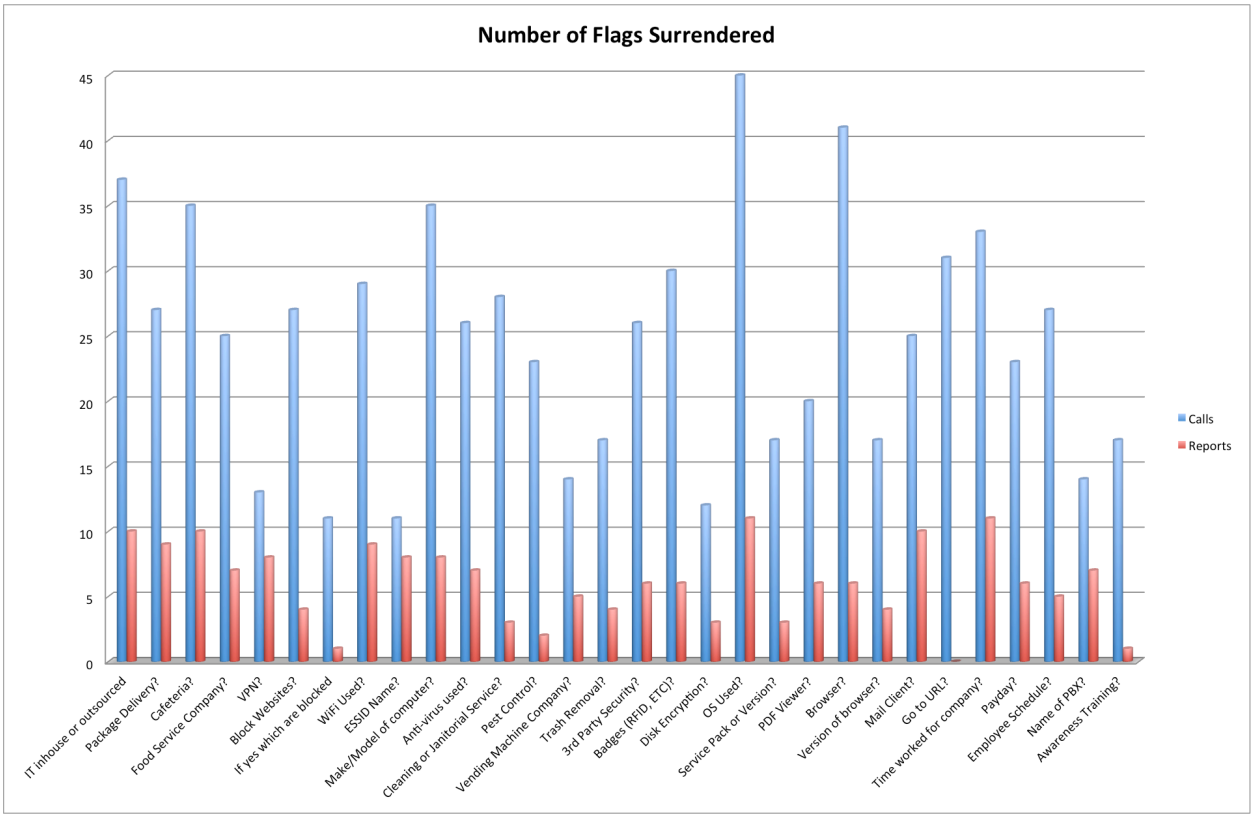

Figure 7: Frequency of Flags

Discussion

This was once again an interesting and informative year. Based on all of the data and our own observations, we can conclude a few points. First and foremost, social engineering continues to be a security risk for organizations. This is our sixth consecutive year hosting this event; in that time and despite numerous high-profile security breaches that occurred this year, we have not seen consistent improvements that directly address the human element in organizational security.

Even as companies are reportedly investing more in security awareness training and policy development, the results again this year support our belief that overall, companies are still doing a relatively poor job. Not all of our competitors used effective pretexts or were allowed to spoof to add credibility to their calls; however, all were able to obtain flags. This means *all* contacted companies provided potentially sensitive information to an unverified caller. It does not appear that employees are being educated to understand the value of the information they

hold or how to appropriately protect it. Rather than accept a request at face value, employees need to be trained and encouraged to question, challenge, and make good decisions.

If the training task is too difficult to overcome immediately, then at minimum, employees need to have proper protocols in place that allow them to question callers. For example, if all employees were forced to verify themselves with an employee ID or other daily code, this could greatly reduce the risk of telephone-based attacks and the need for employees to decide for themselves the correct course of action. If an organization creates an ambiguous situation either through unclear policies or inadequate training, employees will make choices that are easier and less uncomfortable (e.g., disclosing information as opposed to politely declining to answer).

Our second conclusion is that companies are still allowing sensitive data to be posted online. In direct opposition to security is the basic nature of conducting modern business. All companies deal with security challenges, but many of these are magnified in the Business to Consumer sector. The nature of the sector is such that clear communication with, and accessibility by, consumers is mandatory. This places companies in a position where they need to make their resources highly available, and perhaps vulnerable.

In addition to monitoring corporate information, another challenge for all organizations is the inability to completely control the social media and other postings of current and past employees. Our competitors clearly found valuable information through these sources, and they are certainly used by professional social engineers to craft phishing, vishing, and onsite impersonation attempts. Although it is unlikely that this vulnerability can ever be completely mitigated, clear policies and training can assist making employees aware of the risk in which they place both themselves and their companies by over sharing information.

We sincerely hope our findings are useful in making the telecommunications industry safer, and a secure place in which to conduct business.

Mitigation

The ongoing goal of the SECTF is to raise awareness of the threat that social engineering presents to both organizations and individuals. The crux of this report is to inform companies of the dangers associated with malicious social engineers as well as how they can mitigate vulnerabilities and protect against these attacks.

Based on our practice and in reviewing the trends over the past several years, we would expect the use of social engineering to continue to be a significant threat to organizations. Technical controls are only part of a solution that should include ongoing education and auditing as a standard practice to defeat malicious attackers.

Below are a few suggestions for potential mitigation of this threat.

1. Defensive actions

The OSINT phase of the contest revealed how much data on a target company can be gathered through the simplest online searches. Companies must balance the business requirements of managing their brands with the risks associated with having open and approachable communications with their employees and the world. To further complicate the issue, corporate policies on information handling as well as employee social media use can often be either vague or unrealistic.

Companies need to set clear definitions of what is and is not allowed with regard to the handling and posting of information, particularly with respect to social media. Individuals will often not make the connection that personal life being discussed in an open social forum can be leveraged to breach their employers. In addition, clearly defined policies on how, where, and what kind of information can be uploaded to unsecured areas of the Internet can go a long way to safeguarding companies.

Finally, companies MUST help their employees understand what information is valuable and how to think critically about its protection. Guidelines, policies, and education can help the employees understand the risks associated with information exchange in both their personal and professional lives, creating a security-focused culture.

2. Realistic testing

One of the most necessary aspects of security is the social engineering *risk assessment* and *penetration test*. When a proper *risk assessment* is conducted by professionals who truly understand social engineering, real-world vulnerabilities are identified. Leaked information, social media accounts, and other vulnerable aspects of the company are discovered, cataloged, and reported. Potential attack vectors are presented and mitigations are discussed.

A social engineering *penetration test* increases the intensity and scrutiny; attack vectors are not simply reported, but executed to test a company's defenses. The results are then used to develop awareness training and can truly enhance a company's ability to be prepared for these types of attacks.

We conclude that if the companies targeted in this year's competition possessed regular social engineering risk assessments and penetration testing, they might have been more aware of possible attack vectors and been able to implement education and other mitigation to avoid these potential threats.

3. Security awareness education

One of the areas that appear to be lacking across the board is quality, meaningful, security awareness education. Educating the population to meet compliance requirements is not sufficient. In our experience, there is a definite relationship between companies that provide frequent and relevant awareness training and the amount of information that company surrenders. An organization that places a priority on education and critical thinking is sure to possess a workforce that is far more prepared to deal with malicious intrusions, regardless of the attack vector.

Security awareness training needs to be practical, interactive, and applicable. It also needs to be conducted on a consistent basis. It doesn't require that a company plans large events each month, but annual or biannual security reminders should be sent out to keep the topic fresh in the employees' minds. In addition, we have found through our practice that companies who employ ongoing phishing and vishing awareness campaigns through real world testing often fare better at these threats than those that do not. Many times, the difficulty lies in businesses making training and education a priority to the extent that appropriate resources are allocated to ensure quality and relevance. Security education really cannot be from a canned, pre-made solution. Education needs to be specific to each company and in many cases, even specific to each department within the company. Companies who truly understand the challenges and rewards associated with high quality training and education will find themselves most prepared for the inevitable.

These are just three of the many strategies that can be utilized to improve and maintain security and prepare for the attacks being launched on companies every day. Our hope is that this report helps shed light on the threats presented by social engineering and opens the eyes of corporations to how vulnerable they really are.

A Note About The Social-Engineer Village

DEF CON 23 brought back the Social-Engineer Village by popular demand. In addition to hosting the SECTF, we created a four-day event to entertain and educate DEF CON attendees on all things social engineering. This year we offered a "Mission SE Impossible" challenge that simulated an office break-in and emphasized the critical thinking skills necessary to perpetrate successful corporate espionage. We also hosted a number of presentations by well-known social engineers to provide our audience with their unique perspectives in the field, the Social Engineering CTF for Kids, as well as our own live SEORG podcast.

Based on an overwhelmingly positive response, the Social-Engineer Village will return in 2016 and will once again host the Human Track at DEF CON 24. We will be releasing a Call for Papers along with our call for 2016 SECTF contestants in coordination with DEF CON announcements. Please watch our website www.social-engineer.org and our social media accounts @HumanHacker @SocEngineerInc, and https://www.facebook.com/seorg.org for the most current information.

Conclusion

This was another excellent year for the SECTF. Our contestants continue to evolve and mature; time and again proving that social engineering is a skill that can be used by anyone at any level. The unfortunate finding, of course, is that based on our small sample, companies are not significantly better prepared to repel social engineering attacks than they were at the inception of this contest six years ago. It is our hope that this will change as we continue to expand our event and stress ongoing preparation, not just the attention garnered at DEF CON.

If you, or your organization, have any questions regarding any aspect of this report please contact us at: sectf@social-engineer.org.

About Social-Engineer, LLC

Social-Engineer, LLC. is the leading authority in the art and science of social engineering. We started as Social-Engineer.Org, an educational organization, developing the world's first social engineering framework and going on to offer the latest SE news through our newsletter, blog, and podcast. While maintaining this educational portion to our organization, we eventually evolved into Social-Engineer, LLC, hosted at http://social-engineer.com, a professional training and services provider supporting clients in government and private industry.

Our goal always has been, and continues to be, "Security through Education"

Sponsors

The 2015 Social Engineering Capture the Flag contest would not have been possible without the generous support of the following organizations:

SOCIAL-ENGINEER

www.social-engineer.com

SECURECOG

www.securecog.com

TRUSTEDSEC
INFORMATION SECURITY MADE SIMPLE

www.trustedsec.com

PhishLine
Measured Security Awareness

http://www.phishline.com/

pindrop security

www.pindropsecurity.com