SECTF

SOCIAL-ENGINEER.ORG

PO Box 62, Brooklyn, PA 18813 | 800.956.6065 | www.social-engineer.org

The DEF CON 24 Social Engineering Capture the Flag Report

Social-Engineer, LLC

Table of Contents

Executive Summary

Social-Engineer.org (SEORG) hosted the Social Engineering Capture the Flag (SECTF) contest at DEF CON 24 in Las Vegas, Nevada for the seventh year in a row in August of 2016. This year's competition targeted information security companies.

From over 150 entries, we selected 14 competitors from diverse backgrounds and experience levels to test their social engineering abilities. Below is a table highlighting some basic statistics from this year's competition:

Target companies	14
Competitors	14
Completed calls	160
Total points scored on reports	1698
Total points scored on calls	4352

Table 1: SECTF general summary

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 (SEORG), the noncommercial, educational division 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 important information. The contest is divided into two parts, the information-gathering phase that takes place prior to DEF CON, followed 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 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. We also asked participants to submit a 90-second video outlining why they should be included in 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 150 applicants, we selected 14 contestants and randomly assigned them to a company.

Contestants were not made aware of any other competitors or target companies other than their own prior to their call time at the live event. The target companies were not informed of their inclusion in the SECTF, nor was the industry announced prior to our contest. For this year, we selected information security as the target industry. These are brands that businesses rely on to assist their populations in the defense of confidentiality, integrity, and availability of information.

Contestants were given 3 weeks to gather as much information about their target company as possible and generate a formal report. They were allowed to use only Open Source Intelligence (OSINT) that could be obtained through search engines or tools such as Google, FOCA, 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 looking 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 24 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 more easily accessible during non-standard business hours 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.

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 previous years, we again took opportunities after each call to discuss the call with the audience. During that time, we analyzed the success of the 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 USD *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.

2016 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:

- The ability to spoof was allowed for all contestants
- The target companies were all information security companies

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 information security industry.

As businesses must focus on their core competencies, many do not have the internal resources for in-house information security teams. They must rely on the expertise of external service providers, and as companies responsible for the protection of client information, these providers must themselves be extremely cognizant of their own information security.

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. Akamai Technologies
2. Cisco Systems
3. Comcast Xfinity
4. Dell SecureWorks
5. Deloitte Touche Tohmatsu Limited
6. EMC Corporation
7. Fortinet
8. International Business Machines Corporation (IBM)
9. Oracle Corporation
10. Palo Alto Networks
11. RSA Security
12. Sophos Group
13. Symantec Corporation
14. SYNNEX Corporation

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 150 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.

Every year, we send an overview of flags, rules, targets and other pertinent information to our legal counsel. We do this to ensure we are staying within the legal boundaries we set for ourselves when we started this competition.

Table 2 outlines the list of specific flags, their categories, and point values for 2016:

DEFCON 24 SECTF Flag List		
	Report points	**Call points**
Logistics		
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

Table 2: Flag list for SECTF at DEF CON 24 in 2016

Scoring

Social-Engineer had a proprietary application developed for the purpose of scoring both the OSINT and live call portions of the competition. Flags obtained during the OSINT phase of the contest were worth half-points (please see Table 2). OSINT reports were scored prior to the live call event.

Scoring during the telephone calls was accomplished live using the same proprietary application mentioned above. Judges were able to input scores into a database for the flags as they were obtained. 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 by each judge for each contestant. At the end of the competition the scores were totaled by the application to determine the winning score.

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

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 for information gathering purposes 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 individuals or target companies. For more specific information on the ROE, please see our rules and regulations: http://www.social-engineer.org/ctf/def-con-sectf-rules-registration/.

Results and Analysis

High profile events as a result of malicious social engineering are illustrative of the fact that corporations 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

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
LexisNexis	WGet	FourSquare
FOCA	Vimeo	Friendster
Twitter	Tineye	theHarvester
PiPl	WaybackMachine	Google Images
Reddit	LinkedIn	Telnet
Facebook	Monster	EchoSec
Plaxo	GlassDoor	DuckDuckGo
Google Maps	Yelp!	Pinterest
Shodan	Craigslist	JigSaw

Table 3: Commonly used OSINT tools and websites

The quality and research dedicated to the reports continues to be impressive. However, continuing the trend from the previous two years, the scores for calls outperformed those for the reports. This reverses the trend set in the earliest years of the competition. Figure 1 shows a similar point distribution to last year’s competition. It should again be noted that points awarded for flag awarded during OSINT are worth half the value of those awarded during live calling.

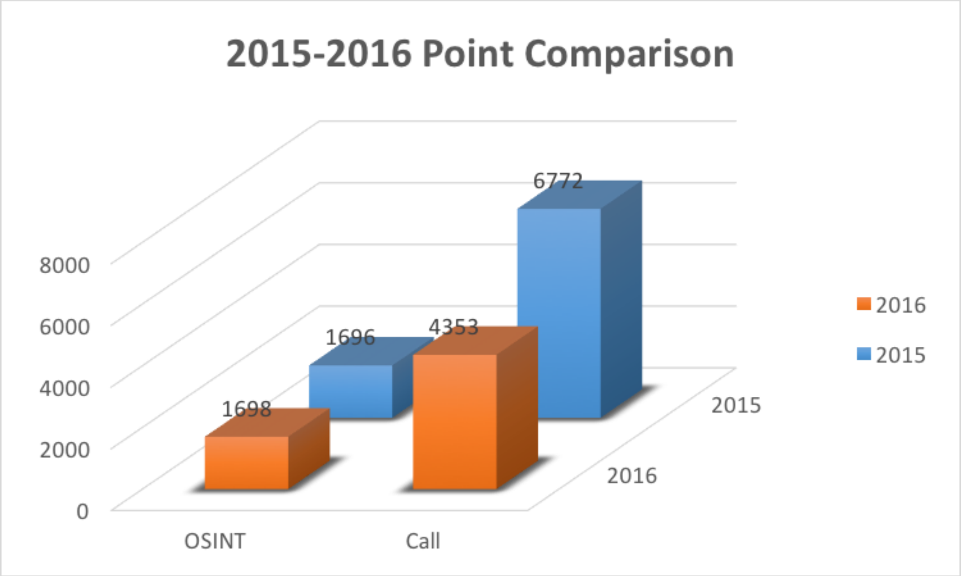

Figure 1: Comparison of OSINT/Calls Points Awarded 2015-2016

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

- Key personnel were discovered to be sharing personal information via social media – activities, interests, purchasing habits, home location, relationship status and friends/family members.

- Several contestants were able to find employees posting pictures from their desks on social media. These contained views of the computers used by the employees, and in some cases views of the employee’s computer screen with sensitive information displayed on it.

- Employees listed very detailed information on their experience and background on social media.

- Some contestants were able to find several posts from target employees discussing work schedule.

Technologies

- Information on operating systems as well as hardware was discovered by several contestants during the OSINT portion. This would allow an attacker to select exploits specifically targeted at a company's infrastructure.

- Information on system architecture, operating systems, and hardware devices used by several targets was found by looking on job postings.

- Multiple contestants were able to locate a full map of their target company's VPN. This would expose the VPN portal to potential attacks.

- Several pictures disclosed the make and model of the WiFi access points by the target companies.

- One target displayed the make and model for their routers, firewall, and several other pieces of hardware used to secure enterprise data.

Physical Plant

- Onsite cafeteria was discovered to be open to the public, making both facilities and employees vulnerable.

- Information regarding office spaces was readily available (e.g., building owners, officer managers, vacant offices, other tenants).

- Several images from inside the offices of target companies were displayed via social media.

- Many details about the physical space were located using tools such as Google Maps (e.g., location of ATMs, security, etc.).

Contractor/Vendor/Other Companies

- A vendor listed a target as their customer for cafeterias.

- Many companies employ contractors, many who are supplied through well-known contracting companies.

- A Google Street View image discovered by a contestant displayed the name of the trash pickup company used by a target company.

- One target company received a reward for recycling/compost from their trash pickup company.

- A janitorial service listed a target company as a client on their website.

Special Notes

- 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.

- Security badges were prominently displayed in several pictures discovered. This would allow an attacker to create a very realistic copy to use in an impersonation attempt.

- One contestant was able to discover a lease agreement between the target company and the landlord available online.

- The ESSID and password for onsite wireless was made public via a tweet by an employee for one target

- A contestant was able to use knowledge gained from observing Google Earth images of a target location in his call to obtain a several flags.

We recognize that much of the information listed above is beyond the control of the organizations and individuals concerned. However, it is important to be aware of information freely available in order to mitigate possible exploitation by malicious 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.

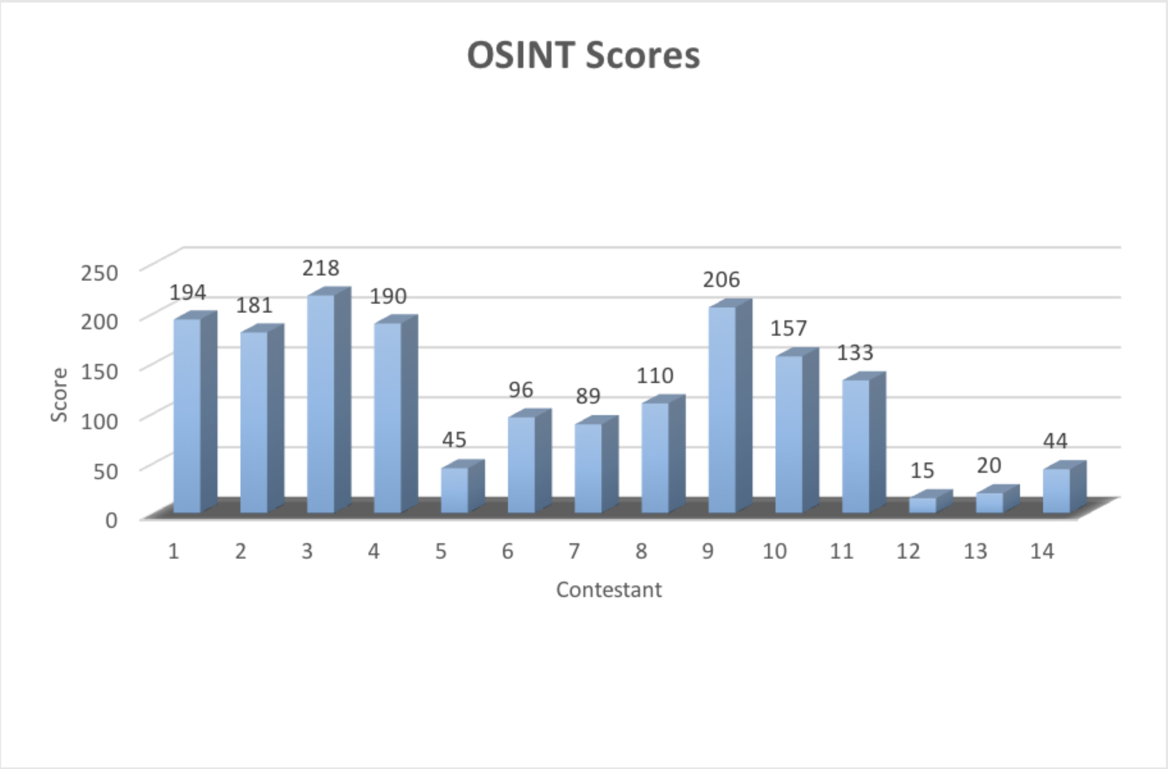

Figure 2: OSINT Scores by Competitor

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

Selecting a proper pretext is a key component to the success of a vishing campaign. This year there were a variety of pretexts used with varying degrees of success. Newcomers predictably struggled the most with both believable pretexts as well as with maintaining the pretext for the duration of the call.

Some contestants attempted to use accents which were not natural to them and found very little success. An important thing to remember when selecting a pretext is to select one which is the most believable. Several of the younger sounding contestants were able to obtain good results using intern/college student pretexts where these would be inappropriate for older sounding contestants. Several newcomers demonstrated an ability to use the inherent nervousness present when competing as part of their pretext.

One of the most important rules for the SECTF is that contestants are not allowed to use negative pretexting. This includes threatening disciplinary action, and/or using extreme fear or anger towards a target. This rule is in place to keep targets from being left in fear for their employment as well as to provide a challenge to the contestants to formulate a pretext that is more creative. This year, one contestant did attempt a pretext which the judging panel felt incited extreme fear in a target. His call was interrupted and he was instructed to recall the target to rectify the situation.

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 3 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 some contestants found difficulty reaching companies towards the end of the business day while others were ill prepared with very few phone numbers discovered during the OSINT portion of the competition.

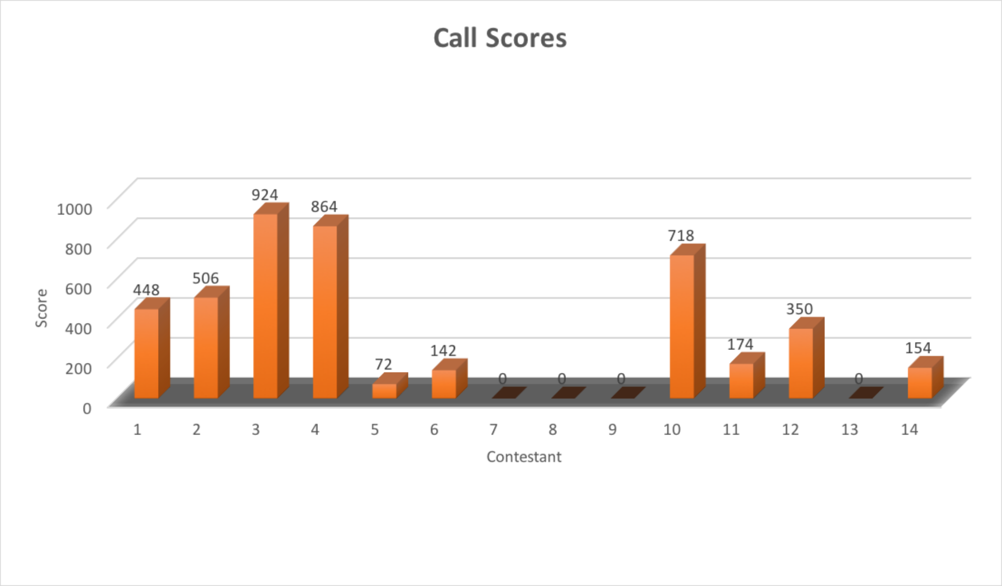

Figure 3: Live Call Scores by Competitor

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, processes, and in one notable case, very recent corporate news.
  - Developed good rapport with the target. In one case, the contestant established a pretext which allowed him to 'assist' a target with figuring out why a fake link wasn't working which led to achieving a high number of flags.
  - 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.
  - Carefully planned the order of their questions. The most experienced contestants tended to start with non-threatening questions and gradually pressed the targets into disclosing more sensitive information.
  - Were persistent. In one case, a competitor was unable to reach his targets and walked his telephone numbers called up by one digit in an attempt to reach people. In a number of cases, competitors recalled individuals when unable to reach other targets.

- Competitors who had the most difficulty:

  - Were not able to make their pretexts immediately clear to their targets. Without being able to establish who, what, and why immediately, these competitors often rambled and were unable to develop proper rapport.
  - Were quick to abandon a call if they met even the slightest resistance.
  - Did not properly research the company before the live calling phase.

- Techniques:
  - A number of successful competitors escalated their requests from small to large.
  - One competitor added an incentive to his pretext by offering a gift card for completing a survey. Upon completion of a brief survey the competitor was able to obtain several more flags by assisting the target with receiving the gift card.
  - A number of successful competitors phrased their elicitations as confirmation of information they already knew (collected in the OSINT phase).
  - Successful competitors also used deliberate false statements to have the target correct them with the correct flag.
  - A number of competitors used a "rapid fire" style of questioning, essentially overwhelming their targets. Depending on the amount of rapport established, this was a successful technique.

- Additional Observations:
  - One competitor noticed that there was a dumpster next to the smoking area for a company during the OSINT phase and used this to obtain the trash pickup company flag during the calls.
  - Two of our competitors were unable to obtain flags due to personnel not answering calls. This mirrors actual social engineering engagements and demonstrates the lack of predictability and control inherent in vishing calls.
  - In more than one case, a company's corporate directory provided the full names of individuals, providing multiple target opportunities with a single call.

Competitor Summary

This year we had our typical range of novice social engineers to professional penetration testers. Average OSINT performance for this year remained identical compared to last year as demonstrated in Figure 4. 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. Call score appears to have fallen this year which may be attributed to the difficulty some competitors had in reaching employees at the target companies. 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.

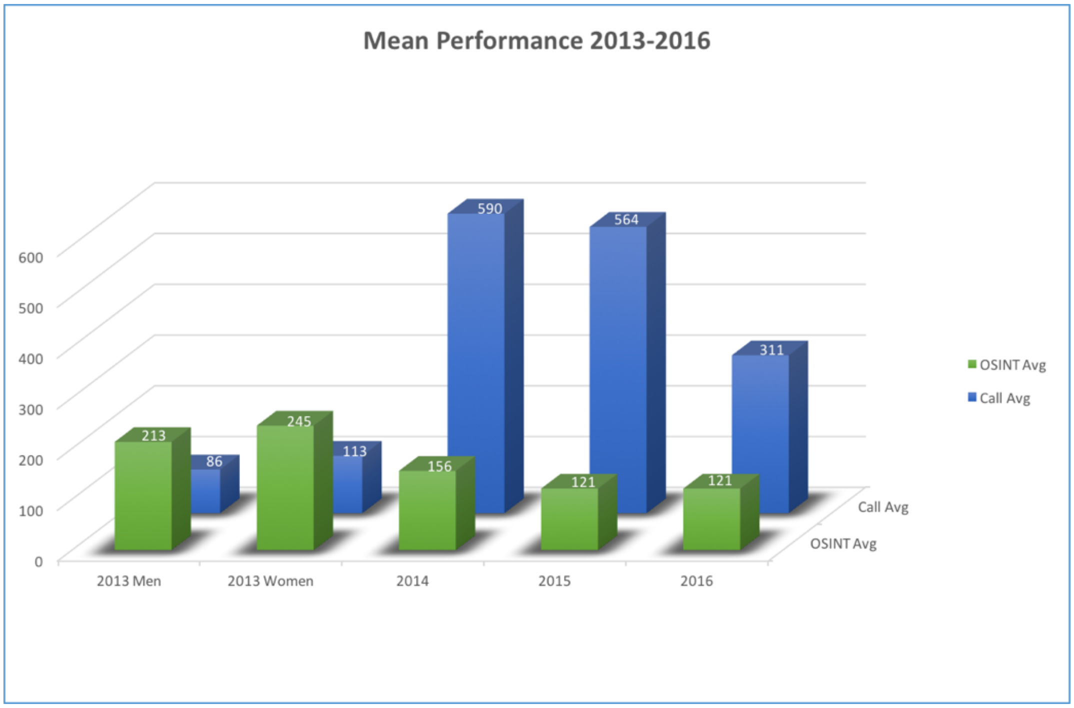

Figure 4: Mean Performance for SECTF 2013-2016

Final Contest Results

At the conclusion of the live call portion of the contest, the judging panel met and reviewed all scores. Figure 5 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.

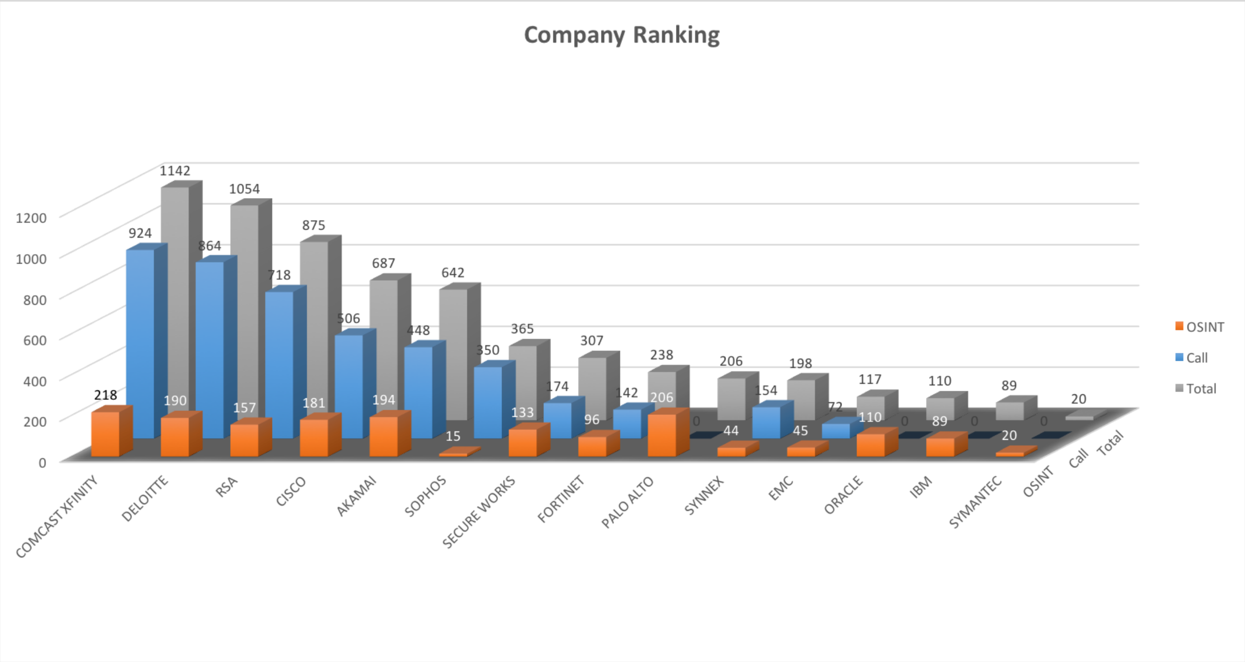

Figure 5: Company Ranking

Keeping with the trend from last year, contestants relied heavily on the call portion for their score. Unfortunately, it should also be noted that there were several targets this year completely untested during the call portion due to personnel simply not answering telephone calls at all. Finally, every target company disclosed at least some information (either discovered during OSINT or during live calls) which could be used as a possible attack vector for malicious actors.

The ranking of companies from best performance (lowest score) to worst performance (highest score) is as follows:

1. Symantec
2. IBM
3. Oracle
4. EMC
5. SYNNEX
6. Palo Alto
7. Fortinet
8. Secure Works
9. Sophos
10. Akamai
11. CISCO
12. RSA
13. Deloitte

14. Comcast Xfinity

We do not release information on 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 attempted to verify the contestant and refused to disclose any information when the contestant could not be located in the employee directory.
- The target looked up the domain and company from the contestant's pretext and refused to have further conversation when these turned out to be fake.
- The target politely shut down the contestant insisting that any requests for a survey should go to the target's manager.
- A target company sent a bulletin company-wide that the firm was under attack from DEF CON.

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 6 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 the amount of time the target had worked for the company, followed by whether or not there was an onsite cafeteria, then employee schedule. The first flag could be used by a malicious attacker in determining how difficult it might be to escalate an attack using this individual as well as the value of the information they may hold. A newcomer to an organization may be an easier target, but may also provide less valuable information, depending on their job function. The other flags could be used to perpetrate believable attacks 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.

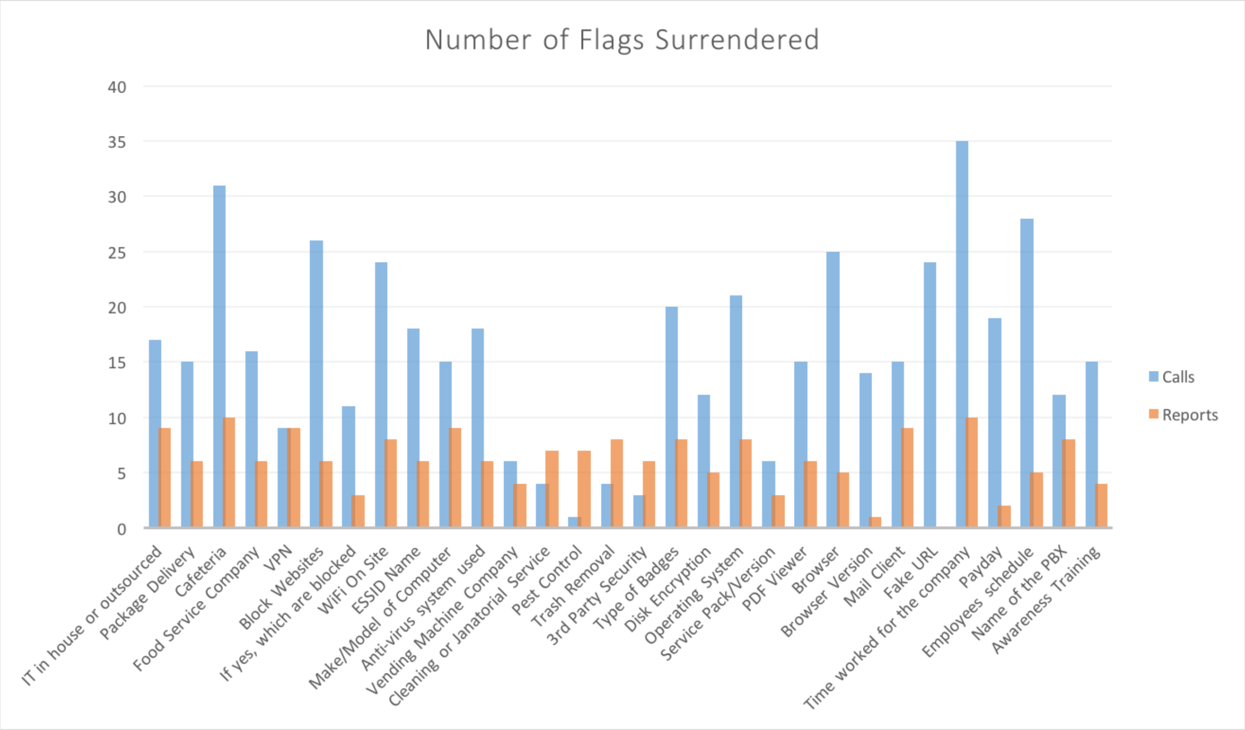

Figure 6: Frequency of Flags

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 was our seventh 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 were experienced information security professionals; however, all were able to obtain flags. 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. Clear communication with, and accessibility of information by, clients and partners 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 information security 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 appears 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 regular 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.

About the Social-Engineer Village

DEF CON 24 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 reboot of last year's "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 2017 and will once again host the Human Track at DEF CON 25. We will be releasing a Call for Papers along with our call for 2017 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 fantastic year for the SECTF. There were many first time contestants as well as some returning from past years. With some of the novice competitors outperforming experienced security professionals the competition continues to demonstrate that social engineering can be a powerful skill for people at any level. Unfortunately, as in years past, our limited findings show that companies are still vulnerable to social engineering attacks. 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 premier consulting and training company specializing in the art and science of social engineering (SE). Social tactics are an established and quickly growing trend in information security in the forms of phishing, phone elicitation (vishing), and impersonation.

With more than three decades of combined experience, Social-Engineer, LLC assists organizations in government, law enforcement, and the private sector in detection and mitigation of the devastating effects of both physical and information breaches. Social-Engineer, LLC focuses on the abilities of a hostile attacker to exploit the human element of businesses to gain access to corporate assets. Through assessment, education, and training, Social-Engineer, LLC helps organizations protect themselves and their trade secrets. To learn more about professional social engineering, services please visit: http://www.social-engineer.com/social-engineering-services/.

Sponsors

The 2016 Social Engineering Capture the Flag contest and the Social-Engineering Village would not have been possible without the generous support of the following organizations:

SOCIAL-ENGINEER

www.social-engineer.com

TRUSTEDSEC
INFORMATION SECURITY MADE SIMPLE

www.trustedsec.com

PhishLine®
Measured Security Awareness

http://www.phishline.com/

pindrop™
security

www.pindropsecurity.com

Asgent
One Step Ahead of The Game
アズジェント

http://www.asgent.com