The 2019 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 this year.

For the 10th year in a row, the SECTF was conducted in August at DEF CON 27 in Las Vegas, NV. This year, competitors targeted companies within the alcohol, tobacco, and firearms (ATF) industries. From 86 DEF CON entries and more than 34,000 views of the application page, 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
Total points scored on OSINT reports	2,042
Total points scored on live calls	1,268

Table 1: DEF CON SECTF General Summary

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

It is important to note that the Target Company Ranking was a combination of points scored by the assigned contestant in the Open Source Intelligence (OSINT) gathering phase and live calling phase of the SECTF. The ranking within this report does not necessarily indicate that one company is more or less secure than another company. However, it is an indicator of potential vulnerabilities that may exist. These corporate vulnerabilities demonstrate that despite training, warnings, and education, social engineering is a serious and viable threat to enterprises.

Overview of the SECTF

The Social Engineering Capture the Flag (SECTF) contest 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.

This competition was formed to demonstrate the severity social engineering can pose to companies and how even novice social engineers can obtain restricted access and confidential information. The SECTF is a two-part challenge, with an information-gathering phase taking place prior to DEF CON, followed by a live-call phase occurring at DEF CON.

Timeline and Process

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 challenge is to demonstrate how much information can be freely obtained through online sources and/or via telephone elicitation.

Months prior to the SECTF, we announced through our social media channels and our website that we were accepting competitor applications. Along with a short entry form, we asked the potential participants to submit a 90-second video outlining why they should be one of the few chosen to compete.

Our panel made contestant selections based on a number of factors that included the desire to learn, as well as our perception of the contestant's intent. As the SECTF is an educational event, we wanted our participants to hold a strong belief on ultimately helping increase awareness around social engineering threats and improving corporate security, as opposed to the singular goal of "winning" a contest. Although applicants who submitted videos received preference in selection, it was not mandatory to submit a video. From 86 DEF CON applicants, we selected 14 contestants and randomly assigned each contestant with one of the target companies.

All chosen contestants were required to place a $20.00 fully refundable deposit to reserve their spot at the SECTF. All contestants were refunded this deposit immediately after completing their calls, unless they failed to show.

Leading up to the competition, contestants did not know of any competitors or target companies, aside from themselves and their assigned target company. The target companies were not informed of their inclusion in the SECTF, nor was the chosen industry announced prior to the live event date. This year, we selected companies within alcohol, tobacco, and firearm industries as targets. These are all non-governmental entities separate from the US government's Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF). These organizations operate on a global scale and a high-profile attack on these companies could be devastating for these businesses.

Contestants received a time slot to perform their live calls on either Thursday or Friday during DEF CON. Great care was taken in the development of the contest to ensure maximum success for the contestants.

Because the live-call portion at DEF CON occurred from the West Coast, companies whose headquarters are located on the East Coast received earlier time slots.

Contestants had 3 weeks to gather as much information about their target company as possible and generate a formally written report. During this information-gathering phase, contestants attempted to capture as many of the designated flags as possible. Only Open Source Intelligence (OSINT) that could be obtained through search engines or tools such as IntelTechniques.com, FOCA, Maltego, etc. qualified for points. Then, contestants assembled the OSINT and flags into a professional report. A sample report was provided for the contestants' reference. In addition to earning points for submitted flags, points were awarded based on the professionalism and quality of the report.

In preparation for the live calls, contestants submitted a list of target company contact phone numbers they obtained during the information-gathering stage. They also submitted a list of phone numbers they wished us to spoof on their behalf during the live calls. Caller ID spoofing is a method through which one's incoming phone number can be forged, or "spoofed," usually to appear as a non-threatening and/or internal number. This is a tactic commonly used by social engineers to increase their credibility with targets.

On the Social-Engineer Village stage at DEF CON, contestants sat inside a sound-proof booth facing the audience with live-stream projection for in-room viewers. Each contestant received a 20-minute allotment to perform as many or as few calls as they wished. Contestants were permitted to bring with them tools they deemed necessary, such as laptops and papers.

United States federal law only requires one party to be notified in the event of recording a telephone call. However, many states, including Nevada, have additional laws requiring both parties' consent to a recorded call. Since we would not be able to obtain the consent of target companies without jeopardizing the integrity of the contest, no recording of any type was permitted during the SECTF, including that by the audience. However, photographs were allowed with permission of the contestants.

With logistical assistance by the SEORG team in spoofing the calls, projecting the contestants live on-screen, and keeping the audience quiet, the contestants made their calls.

Chris Hadnagy, Robin Dreeke, and Ryan MacDougall judged each live call. Hadnagy is the Founder & CEO of Social-Engineer, LLC as well as the Founder of Social-Engineer.Org. Dreeke is the former Chief of the Federal Bureau of Investigation's Behavioral Analysis Program. MacDougall is a Senior Social Engineer Penetration Tester and open source intelligence (OSINT) trainer for Social-Engineer, LLC.

We took about 10 minutes after each contestant finished their calls for Q&A and a brief discussion. During that time, we analyzed the success of techniques used and answered as many questions (directed to the judging panel and/or contestant) as time allowed. After the live call portion of the SECTF, call scores and comments were reviewed along with the previously submitted OSINT reports to determine the SECTF 1st and 2nd place winners.

2019 Parameters

Overall, we aimed to keep the major parameters of the competition as consistent as possible with previous years:

- Contestants were not allowed to obtain the same flag multiple times during a single call from a single target.
- Contestants were not allowed to re-call the same target to obtain the same information previously acquired.
- Contestants were allowed to call potential target company contacts prior to DEF CON, but only to ensure the telephone numbers were valid. Contestants were prohibited from speaking with any individual that answered the line.
- Bribery, such as, “You will be given a gift card for your participation,” was banned.

However, we did make some changes to ensure that the contest continued to be challenging and educational for both contestants and the audience. Primary changes for 2019 included:

- The target companies were all alcohol, tobacco, or firearm companies.
- The scoring platform was adjusted to allow for more accurate trending purposes going forward. When applied to past competitions, no outcomes or results were seen to have changed.

Target Companies

The SEORG staff accomplished target selection through an open nomination and voting process. We made every attempt to ensure that no bias was introduced through attitudes or preconceived notions regarding any particular company. As in previous years, we made a call for companies to be willing participants in the SECTF. This year, no companies, either in the target industries or elsewhere, volunteered. This year's SECTF target company list included (in alphabetical order):

1. Brown Forman
2. Busch Beer
3. Campari America
4. Constellation Brand HQ
5. E&J Gallo Winery
6. Glock
7. Marlboro
8. Molson Coors Brewing
9. Remington
10. Republic National Distributing
11. RJ Reynolds Tobacco
12. Ruger Firearms
13. Skoal
14. Smith & Wesson

Competitors

As in all previous years, one of our core rules is that ***no one*** be victimized. This includes contestants, target company employees who are called, and the target companies themselves. Our contestants' contact information is never revealed, and they are only photographed if they provide explicit verbal permission prior to their live call segment.

14 competitors made the cut from an original pool of 86 applicants. Not all contestants were experienced or professional 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, and some were from other fields not related to social engineering or information security.

Flags

A "flag" is a specific piece of information that contestants attempted to obtain in both the OSINT and live-call portions of the SECTF. Every year, we send an overview of flags, rules, targets companies and other pertinent information to our legal counsel to ensure we remain within the legal boundaries as prescribed by state and federal law. This information is also internally scrutinized to ensure the SECTF adheres to our ethical beliefs and mantras as a leading organization within information security and social engineering.

Table 2 outlines the list of specific flags, categories, and point values for the 2019 SECTF.

2019 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 they have a cafeteria?	4	8
Who does the food service?	4	8
Other Technology		
What is the name of the company VPN?	4	8
Do they block websites?	2	4
If website block = yes, which ones? (Facebook, eBay, etc.)	3	6
Is wireless in use onsite? (yes/no)	2	4
If yes, what's the 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 their 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 security guard company or is it in-house?	5	10
What types of badges do they use for company access? (RFID, HID, None)	8	16
Company-Wide Technology		
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	12

What version?	8	
What mail client is used?	5	10
Do they 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 Information		
How long has the call recipient worked for the company?	3	6
What days of the month does the call recipient get paid?	3	6
Employee's 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 the call recipient had awareness training?	5	10
10 points each for every 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.	0-50	N/A
Format, structure, grammar, layout, general quality of the report, to a maximum of 50 points.	0-50	N/A

Table 2: Flag List For SECTF

Scoring

SEORG possesses a proprietary application for scoring the OSINT and live-call portions of the SECTF. Flags obtained during the OSINT phase of the contest are worth half-points (see Table 2) and could only be obtained once each during OSINT. OSINT reports were scored prior to the live call event.

The three-person judging panel scored each live telephone call. Flags captured during this portion of the event were awarded full points (see Table 2) and could be obtained once from each call recipient. Every attempt was made to ensure consistency in scoring for all contestants, regardless of the judge. Our scoring process does provide some subjectivity through the ability to include notes and comments by each judge for each contestant. At the conclusion of the competition, the application totaled scores to determine the winning scores.

In addition to determining the SECTF winner based on points totals, we conducted an analysis of how the target companies fared in response the SECTF calls made to them. Contestants with strong communication and interpersonal skills, as well as those that prepared thoroughly, obtained better call scores. Even the less-successful contestants still posed as a threat to the target companies. Enterprises simply cannot, and should not, base their sense of corporate security on the hope that a malicious social engineer will be inexperienced, unskilled, or unprepared.

Rules of Engagement

Contestants abided by strict rules to ensure the protection of target companies and its 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. The only permitted method of information gathering was through Open Source Intelligence (OSINT). 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 company before the live calls.

We specifically avoided sensitive industries such as government, education, healthcare, and finance.

We stressed the most important rule of absolutely no victimization of any individuals or target companies to all contestants. For more specific information on the rules of engagement, please see our rules and regulations at https://www.social-engineer.org/sevillage-def-con/the-sectf/.

Results and Analysis

High-profile incidents as a result of malicious social engineering illustrate the fact that organizations continue to be vulnerable to human-based attacks. Unfortunately, this year's SECTF supported this evaluation as our contestants, both experienced and unexperienced, were able to obtain flags through OSINT and live calls. The following sections detail our findings.

NOTE: Any comparisons to previous years' performance are for subjective trend analysis only and no statistical significance can be assumed due to differences in sample sizes, populations, and scoring conditions.

Open Source Intelligence

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

The following table is a partial list of tools and websites used by our contestants during the OSINT phase of the SECTF:

Google	Pyfoca	Pastebin
Maltego	WhoIs	YouTube
FOCA	Vimeo	ThreatCrowd
Twitter	Tineye	FindSubdomains.com
Pipl	WaybackMachine	theHarvester
Facebook	LinkedIn	Google Images
Hunter.io	Monster	Datasploit
Google Maps	GlassDoor	DuckDuckGo
Google Earth	Yelp!	Recon-NG
Shodan	Instagram	Hunchly
Wikileaks	Wikipedia	DNS Dumpster
Robtex.net	Wigle.net	pentest-tools.com
Slideshare.com	Scans.io	IntelTechniques.com
Spiderfoot	Indeed	
Bgp.he.net	Leakedsource.com	
Haveibeenpwned.com		

Table 3: OSINT Tools and Websites Used By 2019 Contestants

The quality and research dedicated to the reports continues to impress. Figure 1 shows total OSINT scores compared to the last four years of competition at DEF CON. The past two years show a notable improvement in OSINT scores over previous years. Keep in mind, the data noted are strictly for general comparisons only and do not indicate statistically significant differences across years.

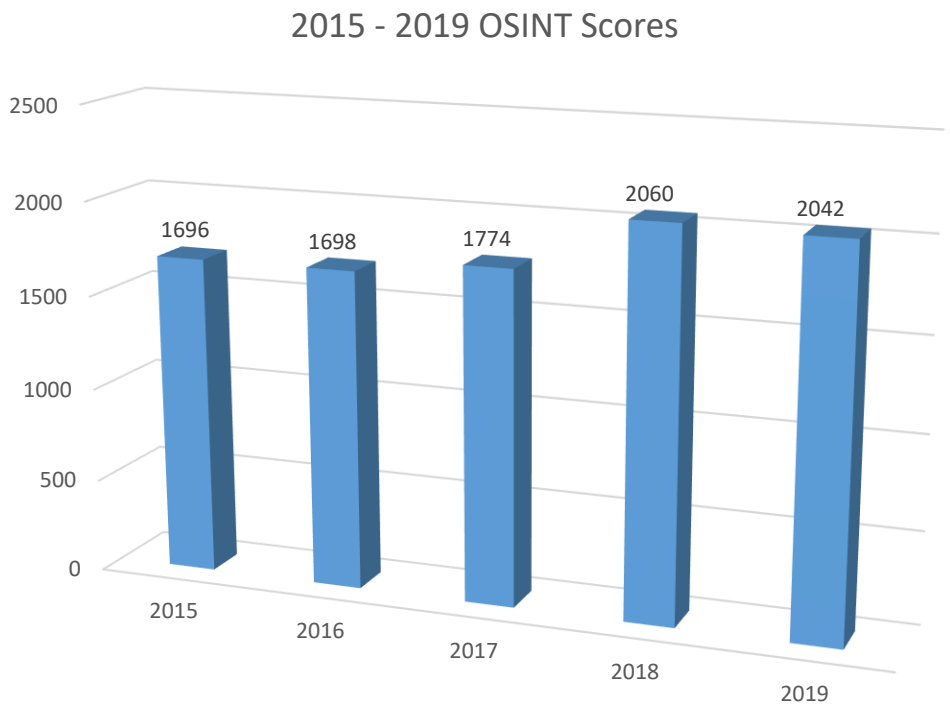

Figure 1: Comparison of OSINT Total Points 2015-2019

An examination of OSINT mean scores and standard deviations in Figure 2 indicates that the amount of information located online by contestants remained relatively stable, including this year.

The mean score is simply the mathematical average of the groups. The standard deviation is an indicator of how much the scores varied from the mathematical average; in other words, it is an indicator of score dispersion. A larger standard deviation indicates the scores are not as clustered around the average, and therefore show greater variability.

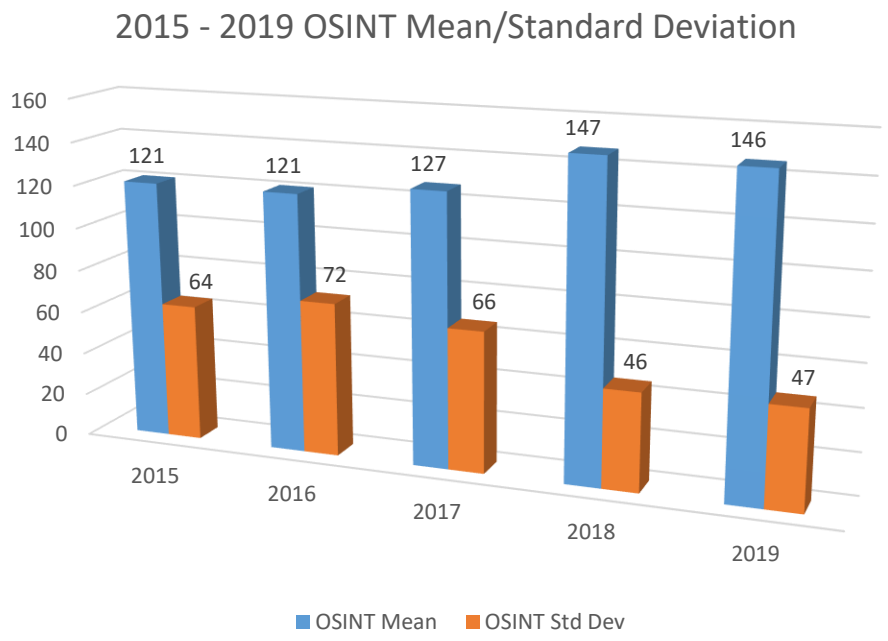

Figure 2: Comparison of OSINT Points Means and Standard Deviations 2015-2019

The following list of this year's more significant findings demonstrates the extremely prevalent danger posed by socially-engineered information gathering. Any of the following pieces of information could be used by a malicious attacker to further develop vishing, phishing, or onsite impersonation attacks. Only the most significant findings are listed.

Corporate Information

- Data from multiple breaches and information leaks exposed sensitive corporate information.
    - Plaintext passwords for corporate accounts (these passwords were not verified to be current and working).
- Open employee social media use indicated a lack of distinction between personal and professional communications. Personal social media accounts often contained corporate and product information.
- Various employment sites and employee handbooks housed pay and shift schedules.
- Various employment sites and employee handbooks contained vacation accrual and other benefits.
- Social media accounts and online documentation included security awareness training policies.

- Often, various social media accounts contained pictures of employee badges.
- Badge types, as specific as HID ProxCard II models, were discoverable.
- Corporate websites included organizational charts and department lists.
- Expansion plans and additional business ventures were openly announced.
- The standard format for email addresses was discovered for numerous companies.
- Direct telephone extensions were located on numerous occasions.
- The full employee directory was available via telephone for a number of companies.
- A public-facing website listed detailed information to include employee programs, benefits, training networks, and social media accounts.
- Websites provided internal jargon that could be used by a social engineer to build rapport and gain validity.
- Camera's and camera locations found online using posted pictures.

Employee Information

- Open corporate culture and social media use at both corporate and employee levels facilitated locating and connecting employees' professional and social networks as well as identifying key personnel.
- Corporate and employee social media often disclosed significant amounts of employee information to include education, background, length of time with the company, hiring/departures from the company, employee ID numbers, etc.
- Employee resumes were located; many listed PII to include home addresses and personal cell phone numbers.
- Multiple breaches and information leaks have exposed the personal and professional information of many employees.
- It was discovered that some posts on Glassdoor geotag individual employees reducing the anonymity of the site, increasing employee exposure risk, and providing social engineers additional information.

Technologies

- Location of IT services was discovered, either being in house or external providers.
- Single Sign On (SSO) portals were found, in some cases, to be publicly facing.
- Use of a webmail client by several targets was discovered.
    - Multiple target companies' Outlook Web Access (OWA) portals were discovered.
- Identity management information was exposed in many instances including password reset instructions for some login portals were available through open web searches.
- Intranet links were located on public facing websites.
- Trouble ticket submissions by customers at one target company allow the inclusion of links, attachments, and files.
- Knowledge of multi-factor authentication tools, or lack thereof, used at target companies was discovered.
- Production servers were determined to be in default configuration.
- A webmail subdomain was easily guessed and exposed multiple pieces of information to include technologies in use.
- Social media and job postings often revealed technologies used within companies to include specific infrastructure, telephone and badging systems, and applications.
- Server software versions were exposed.

- Servers with accessible and public directory browsing were found.
- Software suppliers were discovered for almost all target companies.
- Specific findings (not all-inclusive):
    - VPN platforms (e.g., Cisco, Citrix, OpenVPN)
    - Computer makes/models identified (e.g., Dell, Lenovo, Mac, Windows tablets)
    - Telephone systems (e.g., Cisco, Polycom, Avaya)
    - Cloud service providers (e.g., Amazon, Azure, Google Cloud)
    - Badge type and vendors identified
    - Operating systems (e.g., Linux, Mac, Windows, Linux)
    - Access point technologies (e.g., Cisco)
    - Email applications (e.g., Microsoft Exchange/Outlook, Gmail, Lotus notes)
    - Office productivity applications (e.g., Microsoft Office Suite, Google Suite, Adobe Suite, Cisco WebEx, Microsoft Lync)
    - Security applications (e.g., BitLocker, Cisco AnyConnect VPN, Mac Filevault)
    - Antivirus applications (e.g., Norton, Symantec, Okta, McAfee)
    - Other miscellaneous technologies (e.g., PowerShell, Slack, Fortinet, Confluence, SharePoint, VMware)
    - Specific wireless network ESSIDs/SSIDs

Physical Location Information

- Documentation of secure locations such as Network Operations Centers (NOCs) was discovered.
- The availability of tours of the facility was located online.
- Work locations, such as whether employees work from home and where headquarters are located were found.
- Pictures and videos on personal and corporate media revealed many details about the physical location:
    - The type and location of badge sensors
    - Location of surveillance cameras
    - Interiors of offices
    - Cafeterias
    - Fitness centers
    - Complete layout of the facility to include ingress/egress points

Contractor/Vendor/Other Companies

- Corporate websites and corporate/employee social media often disclosed vendors such as shipping companies, waste disposal, and food service.
- Media such as news outlets and vendor websites, disclosed employee benefits to include cafeterias, health subsidies, etc.
- Vendors were found to post target company information on their own websites.
- Specific contractors/vendors/other companies located include:
    - Shipping (e.g., UPS, FedEx, USPS, DHL)
    - Food service (e.g., Coca Cola, Starbucks, Freshly, Sodexo, Aramark)
    - Waste/janitorial (in-house solutions, e.g., Waste Management)
    - Security (e.g., ADT Security Systems, Allied Barton)
    - Real estate management (e.g., Allied REIT, PMI Properties)
    - ISP/content/technology providers (e.g., AT&T, Comcast Xfinity, Rackspace)

- Corporate lodging and shuttle transportation were determined

Positive Findings

- Some companies had low technical exposure online.
- Employees would occasionally properly shut down contestants on calls.
- Shut downs were at an all-time high this year.
- Evidence of security awareness programs exist.
- Internal communication and reporting policies were in place at some target locations for how to properly handle security threats.
- Some companies did not have direct telephone lines to employees.

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

Figure 3 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 228 points. The X-axis represents the competitors, and the Y-axis the point values for total points awarded for this phase of the competition.

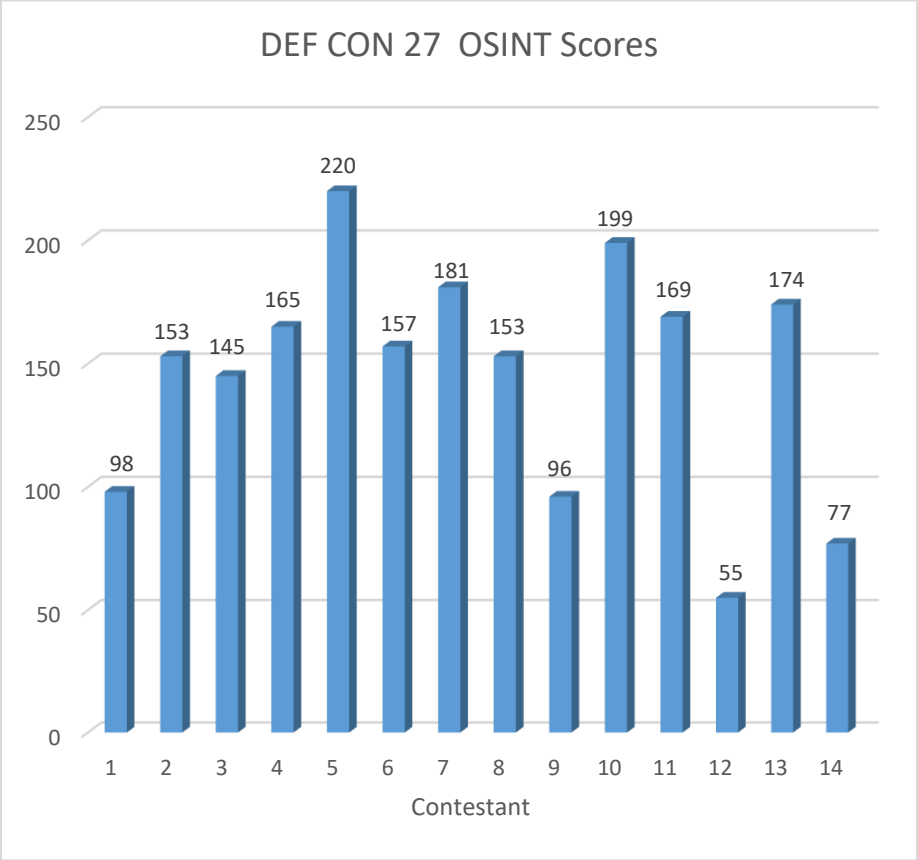

Figure 3: OSINT Scores by DEF CON Competitor

The OSINT portion of our competition stresses a few key points. First, it 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 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-gathering 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 many pretexts used with varying degrees of success. Newcomers predictably struggled the most with both relaying believable pretexts and maintaining the pretext for the duration of the call.

The most successful pretexts used this year were variations of a fellow employee. Our first and second place winners used a scenario in which they called as an internal IT staffer attempting to troubleshoot/confirm systems.

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. We are pleased to report that all contestants stayed within the boundaries of non-manipulative pretexts this year.

Live Call Performance

The live-call portion of the SECTF is an interesting trial for the contestants. 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-gathering phase are not applicable. For this reason, we congratulate all of our contestants in completing this phase of the competition.

Figure 4 shows total call scores compared to the last four years of competition at DEF CON. The data noted are strictly for general comparisons only and do not indicate statistically significant differences across years, but a cursory examination of DEF CON data suggests that callers obtained less flags than competitors in previous years. This may be due to the skill of the callers or to higher security awareness on behalf of the targets.

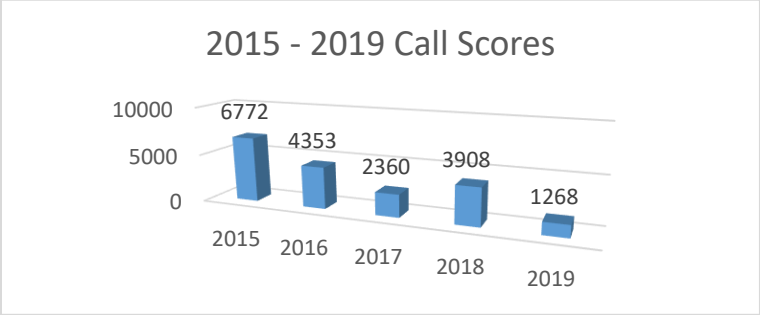

Figure 4: Comparison of Call Total Points 2015-2019

An examination of call mean scores and standard deviations in Figure 5 supports that contestants were, on average, less successful in obtaining flags over the telephone than in previous years.

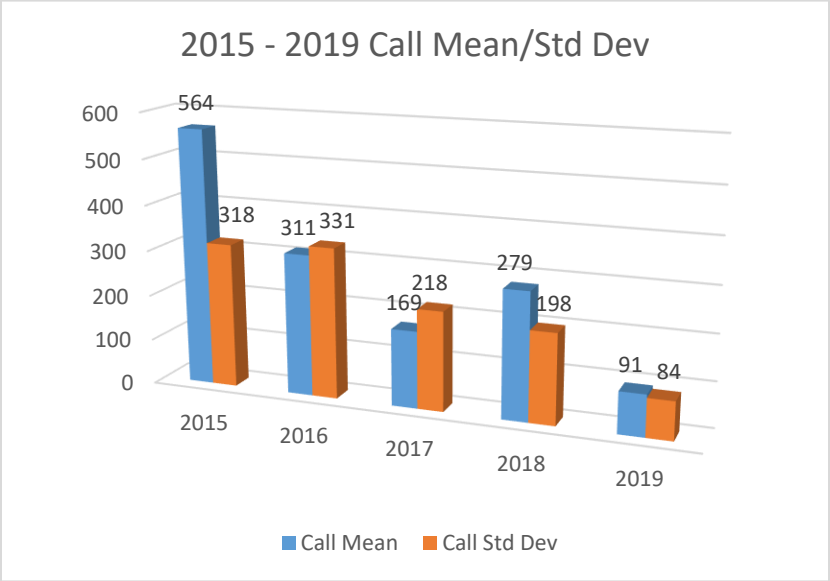

Figure 5: Comparison of Call Points Means and Standard Deviations 2015-2019

Figure 6 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 shows the point values awarded.

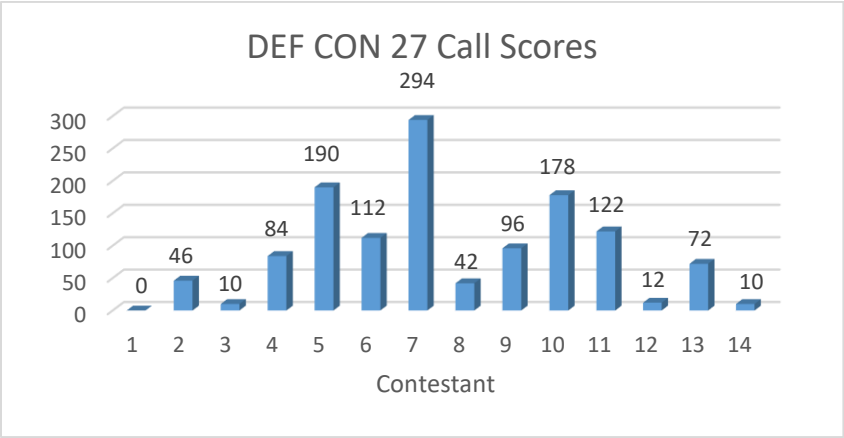

Figure 6: Live Call Scores by DEF CON Competitor

Even a cursory examination indicates extremely high variability amongst contestants. Some of this is attributable to chance, with success based on the frequency with which targets were reached. However, we feel that the vast majority of performance difference is due to preparation on the part of the contestant.

Competitor Summary

This year, we had our typical range of novice social engineers to professional penetration testers. However, since we make changes to the conditions, target industries, number of competitors, and scoring each year, these averages are only valuable in terms of identifying large trends, such as the data reversal we saw in 2019.

Figures 7 is a summary of the mean scores of both OSINT-gathering and calls for the past five years at DEF CON. The mathematical average of scores is impacted by outliers (either very high or very low), so it is relatively limited in the information it conveys. One *can* surmise that competitor performance on OSINT-gathering has remained relatively consistent, while there has been much greater variability with respect to call success. This may be in part due to contestants or target industry.

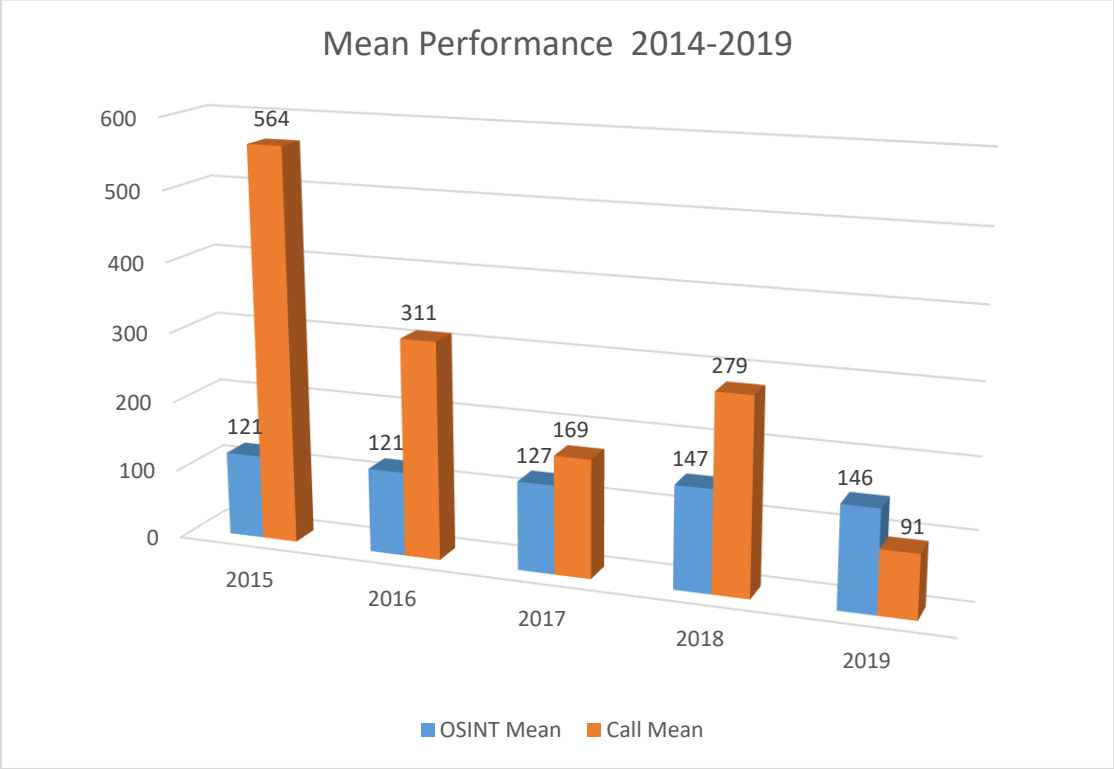

Figure 7: Mean Performance for SECTF DEF CON 2015-2019

The following are observations made during calls.

- Competitors who were the most successful:
    - Were very well prepared. They had conducted thorough OSINT-gathering and possessed more than enough possible targets/phone numbers to call and relevant, detailed pretexts;
    - Developed strong rapport with the target;
    - Used strong pretexts that would yield answers to higher-earning flags;
    - Used internal pretexts that would lead to a more natural request for flags;
    - Were happy, positive, and welcoming in their vocal tones on the calls;
    - 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;
    - Made masterful use of questions and obtained flags without directly asking – a key in good elicitation;
    - Had excellent time management – with an eye on the clock, this allowed the contestant to decide when to abandon an unproductive call and move on to the next target;
    - Dealt with resistance and rejection in a calm fashion; and
    - Had professional and well-written reports.

- 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;
    - Failed to recognize opportunities that could either continue an ongoing call or lead to more informed follow-on calls:
        - Several competitors ended calls when the intended target was not reached, even when the person on the phone indicated willingness to assist.
    - Used weak pretexts such as those impersonating external vendors, unaffiliated organizations, or student;
    - Wrote reports that were unprofessional or filled with errors;
    - Spent more time talking than listening;
    - Used closed-ended questions that often cut off the opportunity to continue the conversation; and
    - Made assumptions about certain departments (e.g., HR would be less forthcoming) and lost opportunities.

- Techniques:
    - A successful, returning competitor employed a rapport building strategy of relating personally to a target on paternity leave after they themselves recently had a baby.
    - A number of successful competitors escalated their requests from small to large.

  - Several competitors had discovered the names of target company employees and referenced them in calls.
  - A number of successful competitors phrased their elicitations as confirmation of information they already knew (collected in the OSINT phase).
  - Successful competitors also used deliberately false statements to have the target correct them with the proper flag.
  - A number of competitors attempted to use an external site to gather numerous flags about the target's technology. Depending on the amount of rapport established, this was a successful technique.

- Additional Observations:
  - One first-time contestant who had called the same office multiple times with the same pretext was called out by an employee after speaking with another targeted employee.
  - Making and completing more calls did not necessarily mean earning more points. Many high call scores came from very few calls. One contestant was able to get most of the points while only completing two calls. One winner only made 3 total calls.
  - All of our highest-ranking contestants in 2019 used an IT-based pretext.
  - One of our competitors was 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.

Final Contest Results

At the conclusion of the live-call portion of the contest, the judging panel met and reviewed all scores. Figure 8 are tallies of OSINT scores, call scores, and grand total by company. The higher score denotes that a higher number or value of flags were disclosed and is indicative of poorer performance on the part of the company.

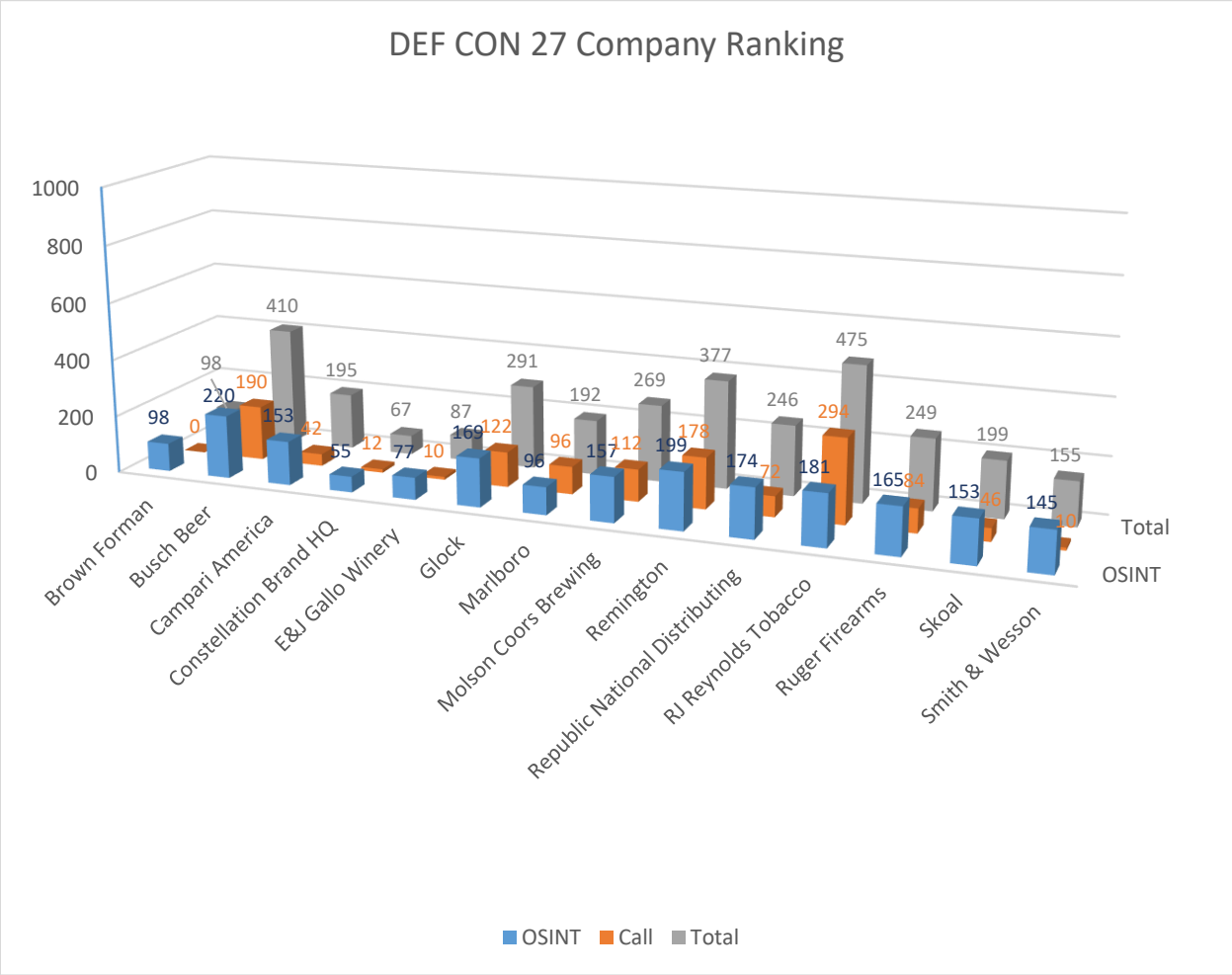

Figure 8: DEF CON 27 Company Ranking

Keeping with the trend from past years, contestants tended to rely heavily on the call portion for their score. It is worth noting that 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) for DEF CON 2019 is as follows:

1. Constellation Brand HQ
2. E&J Gallo Winery
3. Brown Forman
4. Smith & Wesson
5. Marlboro
6. Campari America
7. Skoal
8. Republic National Distributing
9. Ruger Firearms
10. Molson Coors Brewing
11. Glock
12. Remington
13. Busch Beer
14. RJ Reynolds Tobacco

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. Any involved company can reach out to us at* sectf@social-engineer.org *for information on how to obtain this data.*

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

This year, we had several calls during which the targets stated they were prohibited, through company policy, from disclosing information to unverified callers.

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 9 illustrates the number of times each flag was obtained during both OSINT-gathering 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.

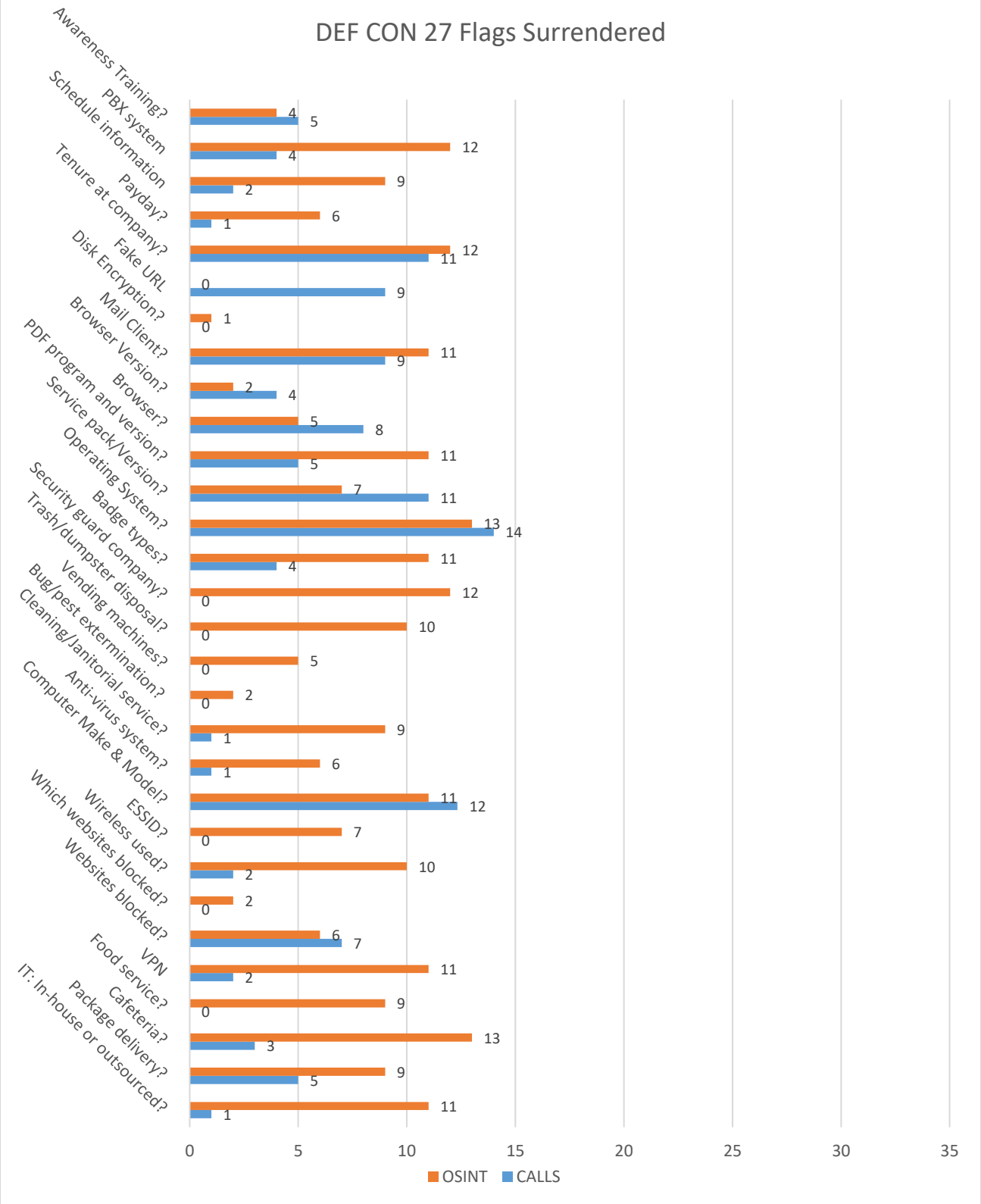

Figure 9: DEF CON 27 Flag Frequency Distribution

Inspection will reveal that the most commonly obtained flag this year at DEF CON was the operating system in use by the target, followed closely by the target's presence or lack of a cafeteria. While this year's most-common flag is identical to last year's second most-common flag, historically, the second most-obtained flag at DEF CON was, "do you have a cafeteria?" The first flag could be used to perpetrate believable attacks via malicious executables that could affect the target's host machine. The second flag could be used as part of an impersonation attack versus the target company.

The takeaway here is that social engineering 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.

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 10th consecutive year hosting this event at DEF CON; in that time, and despite numerous high-profile security breaches that have occurred, 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 this year again support our belief that overall, companies still have ample room for improvement in their security posture against social engineering threats. Not all of our competitors were experienced information security professionals; however, all were able to obtain flags. It does not appear that employees are consistently 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 a 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. Unfortunately, companies need to make a conscience decision regarding what information they are comfortable releasing online based on known risks. 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 social media and other postings of current and past employees. Our competitors clearly found valuable information through these sources, and these posts can certainly be used by

malicious attackers 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 oversharing information. We sincerely hope our findings are useful in making all organizations safer and more secure places 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 purpose 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 being a significant threat to organizations. Mitigation must be a combination of technical controls, policy, and training in order to defeat malicious attackers. Below are a few areas for potential mitigation of this threat.

1. Defensive actions

Good technology must be the foundation of corporate information security. At a bare minimum, organizations must possess basic technical controls that include appropriate hardware, software, and adequate system administration. Technical exploitation continues to be a perimeter test of unpatched systems and outdated technology. Don't make a criminal's job easier by not investing in secure technologies.

In addition, help your employees make safe decisions. Most make decisions that will affect corporate security on a daily basis. If your policy is unclear, or puts the employee in a position to make an unsafe choice, you are not giving them the tools they need to help keep the company secure.

The OSINT-gathering 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 communication with their employees and the world.

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. Security awareness education

One of the areas that appears to be lacking across the board is high-quality and 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 the company discloses. 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 who do not. Many times, the difficulty lies in getting businesses to make training and education a priority to the extent that appropriate resources are allocated to ensure quality and relevance. Security education 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.

3. Realistic testing

The key to helping a population make safer decisions is through realistic testing. Only placing an individual in the position of actually making a decision in a safe setting can assure the organization that their employees will make the right choice at the critical time.

Two of the most necessary aspects of security are 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.

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.

Conclusion

This was another fantastic year for the SECTF. This year, we saw many first-time contestants elicit flags, again proving that anyone with a telephone and courage can obtain valuable information. 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 the Social-Engineer Village

The Social-Engineer Village is now a popular staple at both DEF CON and DerbyCon. In addition to hosting the SECTF within the village, SEORG created a series of events to entertain and educate attendees on all things social engineering. We hosted a number of presentations by well-known social engineers to provide our audience with their unique perspectives in the field and our own live SEORG podcast at DEF CON, alongside our competitions. The competitions seen at DEF CON, in addition to the SECTF, were the Social Engineering CTF for Kids, the Social Engineering CTF for Teens, and, as in previous years, the "Mission SE Impossible" challenge which simulates an office break-in and emphasizes the critical-thinking skills necessary to perpetrate successful corporate espionage. At DerbyCon, our competitions were the OSINTCTF, the "Mission SE Impossible," and we hosted two very successful panels on "Real world vs Competition Vishing" and "Security Awareness: What Works and What Doesn't".

Based on an overwhelmingly positive response, the Social-Engineer Village is planning to return in 2020 to DEF CON. We will release a Call for Papers along with our call for 2020 SECTF contestants in coordination with conference 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.

About Social-Engineer, LLC

Founded in 2008, Social-Engineer, LLC pioneered the recognition, comprehension, and progression of social engineering as a professional practice. With more than 75 years of combined expertise in security and program management, they've worked alongside the world's leading behaviorists and psychologists to develop, deliver, and manage scientifically grounded frameworks, methodologies, processes, and principles for the success of their clients.

Complex international enterprises with more than 280,000 employees trust Social-Engineer, LLC to help them meet their security goals. With clients among the Fortune 500 to the Fortune 10 lists, Social-Engineer, LLC has worked in countless capacities with both private and government entities across the globe.

Our portfolio includes extensive, varied, and multi-faceted consulting and engagements in:

- Risk Assessments & Executive Services
- PhaaS® our trademarked and patented Phishing as a Service
- VaaS ® our trademarked Vishing as a Service
- SMiShing
- Impersonation
- Training

Social-Engineer, LLC's unparalleled understanding of social engineering risks, the mindset of end users, and how to identify, resist, and defeat modern threats distinguishes them and the quality of work they deliver.

For more information and to contact Social-Engineer, LLC please visit https://www.social-engineer.com/.

Sponsors

The 2019 Social Engineering Capture the Flag contest and the Social-Engineer Village would not have been possible without the generous support of the following organizations:

SOCIAL-ENGINEER

www.social-engineer.com

KnowBe4
Human error. Conquered.

https://www.knowbe4.com

CG Silvers
CONSULTING

https://www.cgsilvers.com/