DEF CON 26 SECTF | DerbyCon 8.0 SECTF | www.social-engineer.org

The 2018 Social Engineering Capture the Flag Report

Social-Engineer, LLC

Table of Contents

Executive Summary

Social-Engineer.org (SEORG) hosted two Social Engineering Capture the Flag (SECTF) contests this year.

The first was in August at DEF CON 26 in Las Vegas, NV for the ninth year in a row, with this competition targeting transportation companies. From 137 DEF CON entries and over 34,000 views on 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 reports	2060
Total points scored on calls	3908

Table 1: DEF CON SECTF general summary

The second SECTF was held at DerbyCon 8.0 in Louisville, KY in October 2018 and was the second SECTF to be held there, targeting Fortune 500 companies in the oil and gas industry. From 17 DerbyCon entries and over 4,000 views on the application page, we selected 6, and 5 competed. Below is a table highlighting some basic statistics from this competition:

Target companies	5
Competitors	5
Total points scored on reports	837
Total points scored on calls	924

Table 2: DerbyCon SECTF general summary

As in years past, the overall goals of these contests 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 social engineers. 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 are 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) contests are annual events held within the Social-Engineer Village at both the DEF CON Hacking Conference in Las Vegas, NV and the DerbyCon Information Security conference in Louisville, KY. The SECTF is organized and hosted by Social-Engineer.Org (SEORG), the noncommercial, educational division of Social-Engineer, LLC.

The competitions were formed to demonstrate how serious social engineering threats are to companies and how even novice individuals can use these skills to obtain important information. The contests are divided into two parts, the information-gathering phase that takes place prior to the conferences, followed by the live call phase that occurs at DEF CON and DerbyCon.

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 events, SEORG solicited for individuals who wished to compete via our social media outlets and the 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 that included the 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 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 were given preference in selection, it was not mandatory. From 137 DEF CON applicants, we selected 14 contestants and randomly assigned them to a company. From 17 DerbyCon applicants, we selected 6 contestants, 5 of whom competed, 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 live event date. For DEF CON this year, we selected transportation as the target industry. These organizations operate on a global scale and are instrumental to the constant movement of goods and services in America. A high-profile attack on these companies could be devastating for these businesses as well as the US as a whole. For the SECTF at DerbyCon, we selected energy companies that support the infrastructure of the whole country.

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 IntelTechniques.com, FOCA, Maltego, etc. During this information-gathering phase, contestants attempted to capture as many of the pre-defined flags as possible. The information gathered was to be assembled into a professional 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.

Contestants were then assigned a time slot to perform their live calls on either Friday or Saturday during DEF CON and Friday during DerbyCon.

Great care was taken in the development of the contest to ensure maximum success for the contestants. Since DEF CON calls were conducted from 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 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," 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.

Contestants are then placed inside of a sound proof booth at the live event. Each contestant was free to use their entire allotted 20-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 during DEF CON (including that by the audience), but recording was allowed at DerbyCon as Kentucky is a one-party consent state. Photographs were allowed at both competitions with permission of the contestant.

Scoring was accomplished during each call by two judges at both DEF CON, Chris Hadnagy and Neil Fallon, and DerbyCon, Chris Hadnagy and Ryan MacDougall. Based on very positive feedback from previous years, we again took opportunities after each call for a Q&A and discussion with the contestant and judging panel. 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 the conferences to determine the winners.

It should be noted that all 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 calls, unless they were not present for their time slot.

2018 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 the audience. Some of those guidelines are as follows:

- Contestants were no longer allowed to obtain the same flag multiple times during a single call from a single target
- Contestants were no longer allowed to re-call the same target to obtain the same information previously acquired
- Contestants were allowed to call potential target companies prior to DEF CON, only to ensure telephone numbers were valid, and contestants were prohibited from speaking with any individual that answered the line
- Bribery ("you will be given a gift card for your participation") was explicitly disallowed

Primary changes for 2018:

- The target companies were all transportation companies for DEF CON
- The target companies were energy companies for DerbyCon

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.

As in previous years, we made the call for companies to be willing participants in the SECTF. This year, no companies, either in the target industries or elsewhere, volunteered as participants.

The DEF CON target list (in alphabetical order):

1. Alaska Airline
2. American Airline
3. Budget
4. Delta
5. Enterprise Rent-a-Car
6. Estes
7. Heartland Express
8. Hertz
9. JB Hunt
10. Old Dominion
11. Ryder
12. Southeastern
13. United
14. United Rental

The DerbyCon target list (in alphabetical order):

1. Devon Energy
2. Haliburton
3. Noble Energy
4. Phillips 66
5. Sunoco

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 contestants' personal information is never revealed, and they are only photographed if they provide explicit verbal permission prior to their live call segment. No recording of contestants during their calls at DEF CON is ever permitted due to two-party consent laws in the state of Nevada.

There were 14 competitors selected from an original pool of 137 applicants for DEF CON. At DerbyCon, 6 competitors were selected, 5 of whom competed, from 17 applicants for DerbyCon. 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 remain within the legal bounds as prescribed by state and federal law, based on the advice of our legal counsel, as well as ensuring we adhere to our ethical beliefs as an organization.

Table 3 outlines the list of specific flags, their categories, and point values for 2018.

2018 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		
What is the name of the 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	12
What version?	8	
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
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 a maximum of 50 points.	0-50	N/A

Table 3: Flag list for SECTF

Scoring

Social-Engineer possesses a proprietary application for scoring of both the OSINT and live call portions of the competition. Flags obtained during the OSINT phase of the contest are worth half-points (see Table 3) and could only be obtained once each during OSINT. OSINT reports were scored prior to the live call event.

Scoring for the telephone calls was accomplished during each call by a two-person judging panel at DEF CON and DerbyCon. Flags captured during this portion of the event were awarded full points (see Table 3) and could be obtained once from each distinct target. 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 the SECTF calls made to them. Contestants who used strong communication and interpersonal skills, as well as those that prepared well, obtained better call scores. 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 do 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 do 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. Contestants were only allowed to verify that the telephone numbers collected during OSINT were valid. 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 at http://www.social-engineer.org/ctf/def-con-sectf-rules-registration/ and https://www.social-engineer.org/sevillage-derby-con/sectf-derby-con/.

Results and Analysis

High profile events as a result of malicious social engineering are illustrative of the fact that organizations continue to have vulnerabilities to human based attacks. Unfortunately, this year's SECTF supported this evaluation as our contestants, both experienced and newcomers alike, were able to obtain flags both through OSINT and the live calls. Our findings are detailed in the sections that follow.

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. 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 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	Wigle.net
Spiderfoot	Indeed	IntelTechniques.com
Bgp.he.net	Leakedsource.com	LinkedIn
Haveibeenpwned.com		

Table 4: OSINT tools and websites used by 2018 Contestants

The quality and research dedicated to the reports continues to be impressive. Figure 1 shows total OSINT scores compared to the last 3 years of competition at DEF CON. Figure 2 shows total OSINT numbers for the initial two years of DerbyCon. Note that it is interesting to compare DerbyCon numbers to DEF CON, but they are not directly comparable due to the significantly smaller number of competitors at DerbyCon.

Additionally, DerbyCon 7.0 and 8.0 data are not directly comparable as there were 6 competitors in 2017 at DerbyCon but only 5 in DerbyCon 8.0. That being said, it is interesting that the total OSINT scores were significantly higher for DerbyCon 8.0 compared to DerbyCon 7.0. This could indicate the target companies had more online exposure or that this year's competitors increased the number of flags discovered through OSINT. Given there were fewer competitors along with notably higher total points discovered through OSINT, this may reflect that this year's competitors spent more time and energy on the reporting aspect of the competition allowing more flags to be obtained in the reporting phase. Again, the data noted are strictly for general comparisons only and do not indicate statistically significant differences across years.

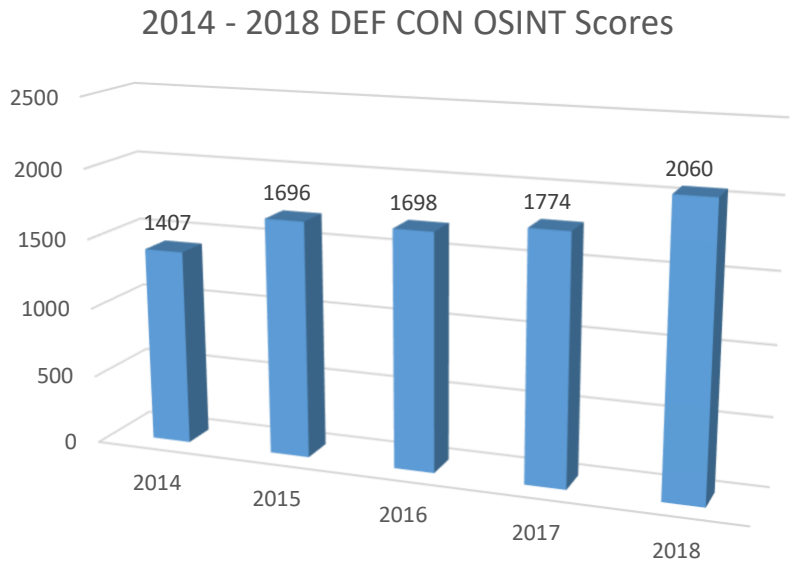

Figure 1: Comparison of DEF CON OSINT total points 2014-2018

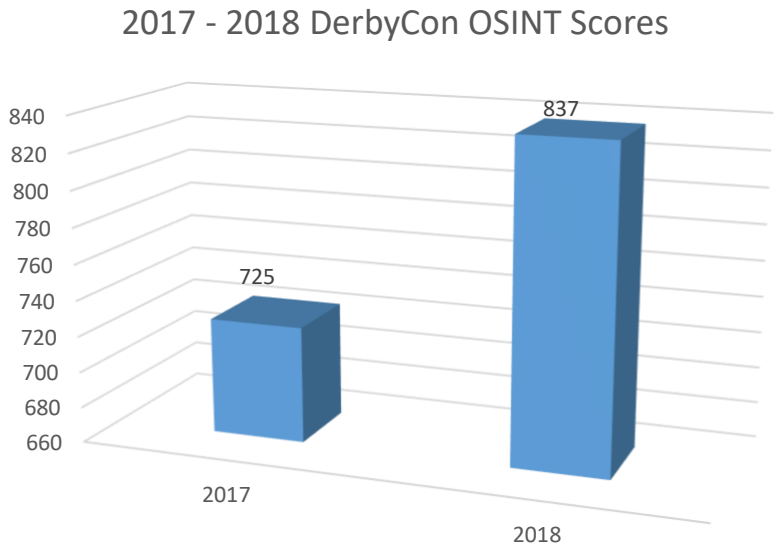

Figure 2: Comparison of DerbyCon OSINT total points 2017-2018

An examination of OSINT mean scores and standard deviations in Figures 3 and 4 indicate that the amount of information located online by contestants has remained relatively stable with a slight increase in 2018 for both competitions. This is particularly notable at DerbyCon this year, as fewer contestants participated, while OSINT scores increased.

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.

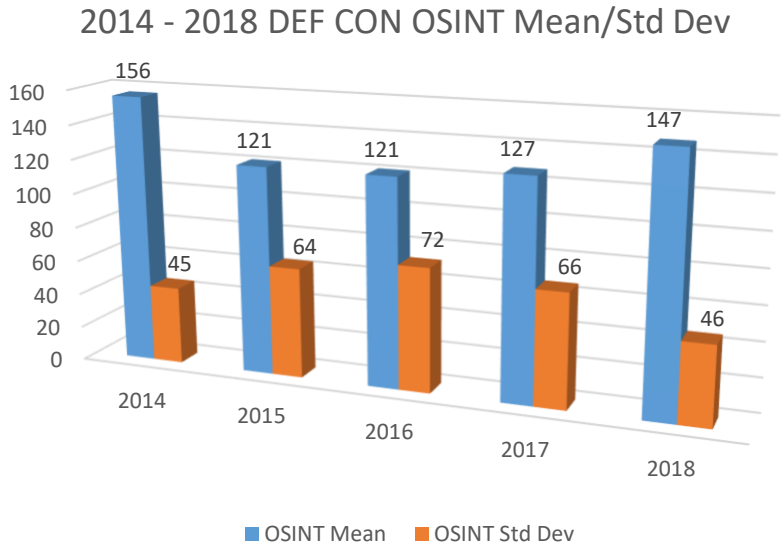

Figure 3: Comparison of OSINT points means and standard deviations from DEF CON from 2014-2018

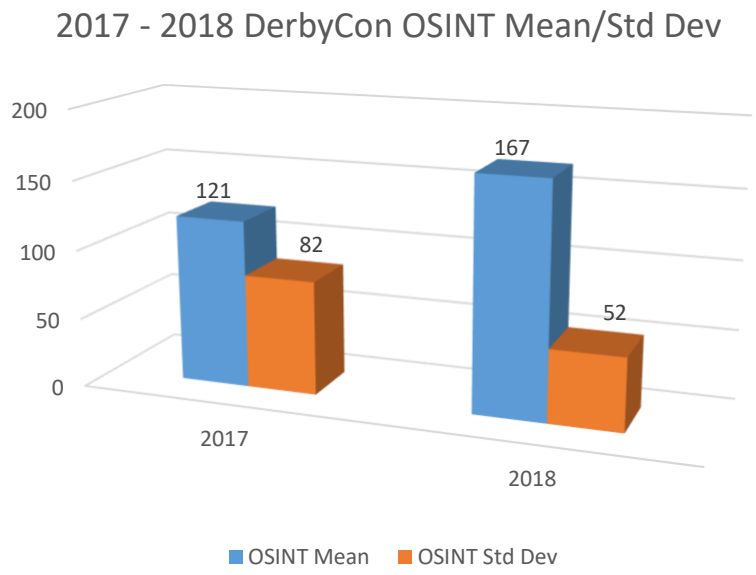

Figure 4: Comparison of OSINT points means and standard deviations at DerbyCon from 2017-2018

The following list of this year's more significant 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. Only the more significant findings are listed.

Corporate Information

- Multiple breaches and information leaks have exposed sensitive corporate information
    - Plaintext passwords for corporate accounts (these passwords were not verified to be current and working)
    - Directions on accessing corporate VPN (these directions were not verified to be active)
- Open employee social media use indicated a lack of distinction between personal and professional communications – corporate as well as product information was often located on personal social media accounts
- Pay and shift schedules were located on various employment sites as well as employee handbooks
- Vacation accrual and other benefits were located on various employment sites as well as employee handbooks
- Security awareness training policy was located on social media accounts and online documentation
- Pictures of employee badges were often located on various social media accounts
- Badge types as specific as HID ProxCard II models were also discovered
- Organizational charts and department lists were located on corporate websites
- Expansion plans and additional business ventures have been announced openly
- The standard formatting 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
- Training courses were disclosed via the social media accounts of multiple targets' employees

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
- One target published Instructions for remote guest access to networks
- Use of a webmail client by several targets was discovered
    - Multiple target companies' Outlook Web Access (OWA) portals were discovered.
- Outdated and vulnerable programs were in use by many target companies
- Identity management information was exposed in many instances including password reset instructions for some login portals were available through open web searches
- One target company failed to anonymize their domain registrant information
- 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
- A development website was found to be publicly accessible
- 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
- Routers discovered at specific IP addresses disclosed their models and serial numbers
- Server software versions were exposed.
- Servers with accessible and public directory browsing
- Software suppliers were discovered for almost all target companies

- Specific findings (not all-inclusive):
    - VPN platforms such as Cisco, Citrix, OpenVPN, etc.
    - Computer makes/models identified (e.g., Dell, Lenovo, Mac, Windows tablets)
    - Telephone systems (e.g., Cisco, Polycom, Avaya)
    - Cloud service providers (Amazon, Azure, Google Cloud, etc.)
    - 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, etc.)
    - Office productivity applications (e.g., Microsoft Office Suite, Google Suite, Adobe Suite, Cisco WebEx, Microsoft Lync)
    - Security applications (BitLocker, Cisco AnyConnect VPN, Mac Filevault)
    - Antivirus applications (Norton, Symantec, Okta, McAfee)
    - Other miscellaneous technologies (PowerShell, Slack, Fortinet, Confluence, SharePoint, VMware, etc.)
    - Specific wireless network ESSIDs/SSIDs

Physical Location Information

- Documentation of secure locations such as Network Operations Centers (NOC) 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
- 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 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, 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
- One target company did not provide many of their employees with internet or WIFi access, restricting their abilities to affect the network
- Employees would occasionally properly shut down contestants on calls
- 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 concerned. However, it is important to be aware of information that is freely available in order to mitigate possible exploitation by malicious attackers.

Figures 5 and 6 provide 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.

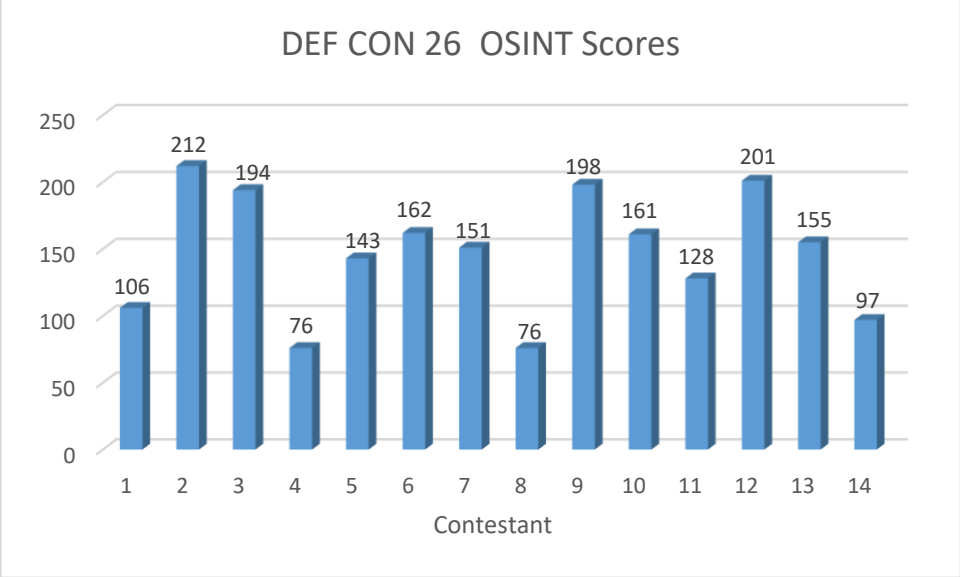

Figure 5: OSINT Scores by DEF CON competitor

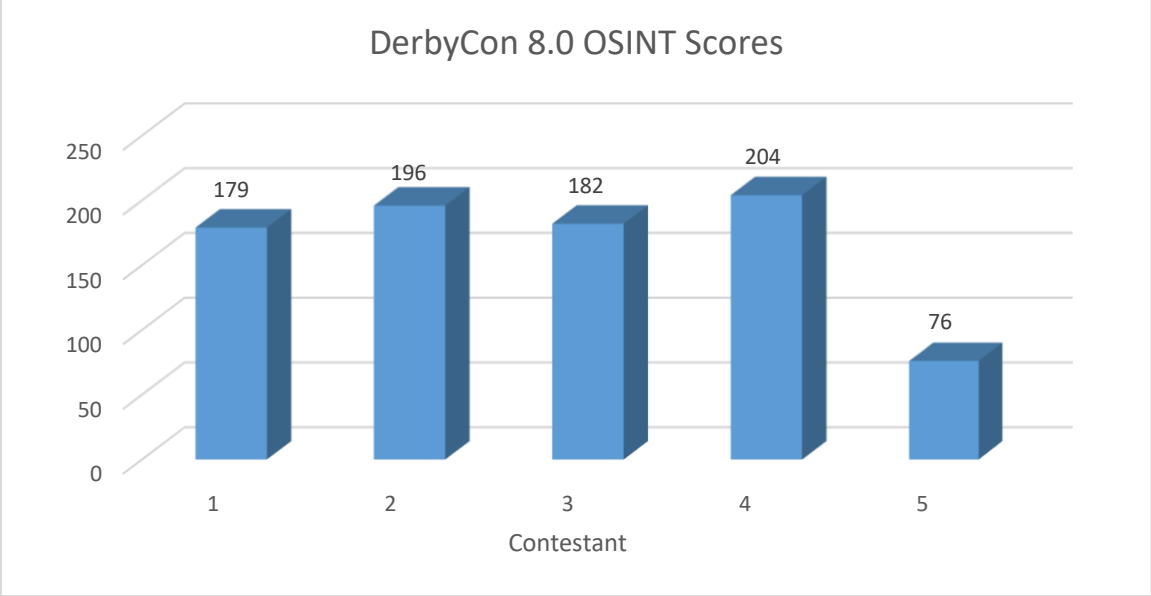

Figure 6: OSINT Scores by DerbyCon competitor

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 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 believable pretexts as well as with 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 at both competitions used a scenario in which they called as an internal IT staffer attempting to troubleshoot/confirm systems.

Other pretexts used included:

- Army Cyber Command
- Student
- Food vendor
- Other Vendors

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 happy 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 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 7 shows total call scores compared to the last 4 years of competition at DEF CON. Figure 8 shows DerbyCon 7.0 compared to DerbyCon 8.0. It should be noted that DerbyCon scores are not comparable to DEF CON totals due to the significantly smaller number of competitors. Additionally, DerbyCon 7.0 and 8.0 data are not directly comparable as there were 6 competitors at DerbyCon 7.0 but only 5 at DerbyCon 8.0. Having one less competitor at DerbyCon 8.0 could account for the lower mean call score at DerbyCon in 2018 compared to 2017. Again, 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 more flags than competitors last year. This may be due to the skill of the caller or to lower security awareness on behalf of the target.

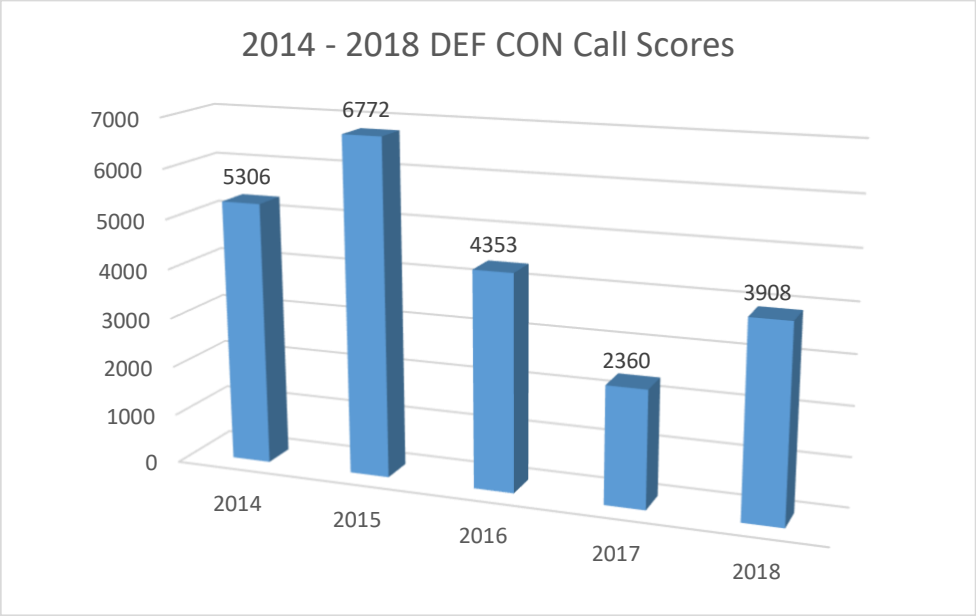

Figure 7: Comparison of call total points 2014-2018

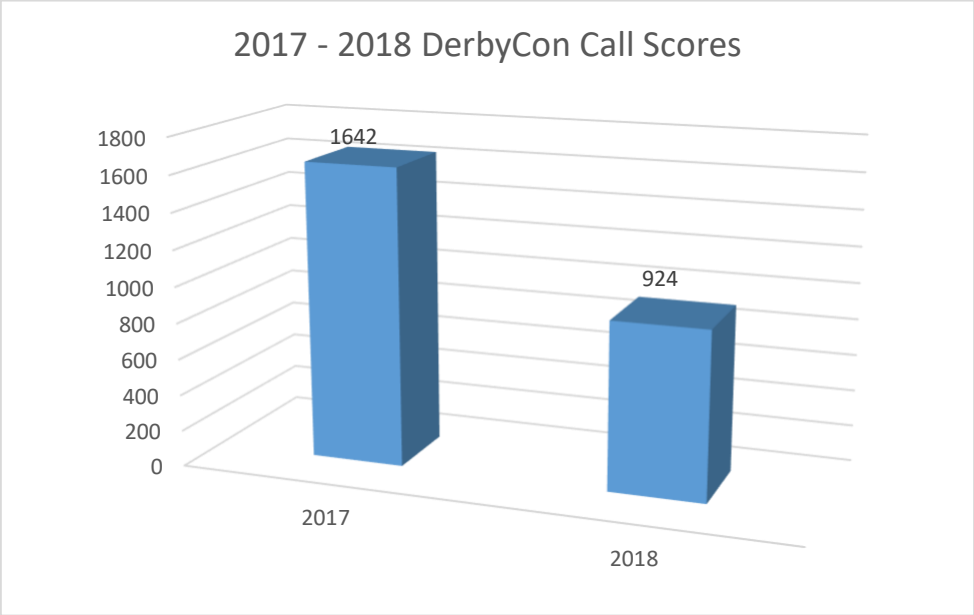

Figure 8: Comparison of call total points 2014-2018

An examination of call mean scores and standard deviations in Figures 9 and 10 supports that contestants were, on average, more successful in obtaining flags over the telephone than in previous years, although variability was very high.

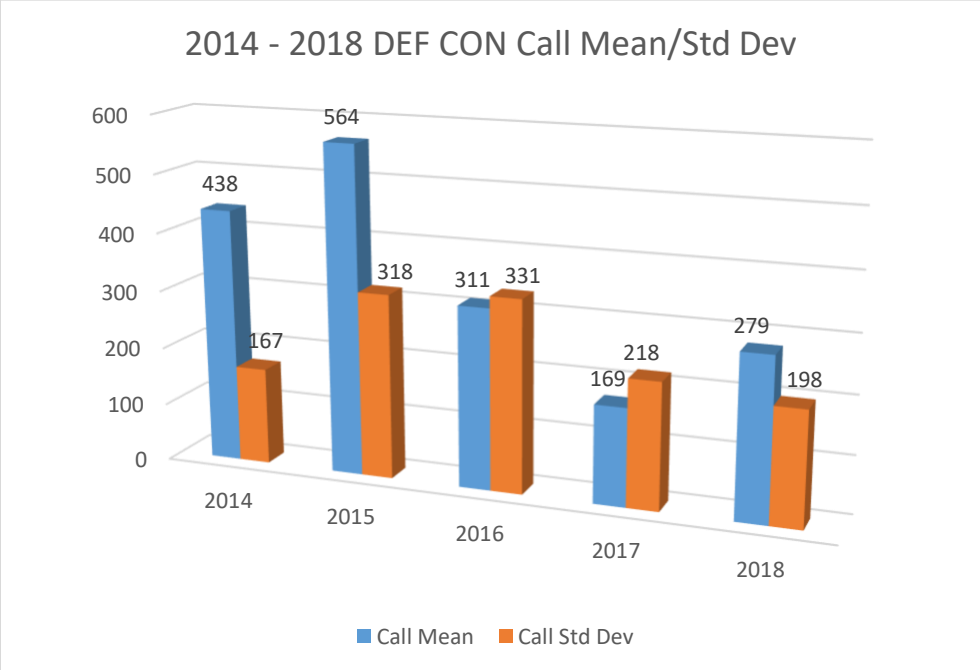

Figure 9: Comparison of call points means and standard deviations DEF CON 2014-2018

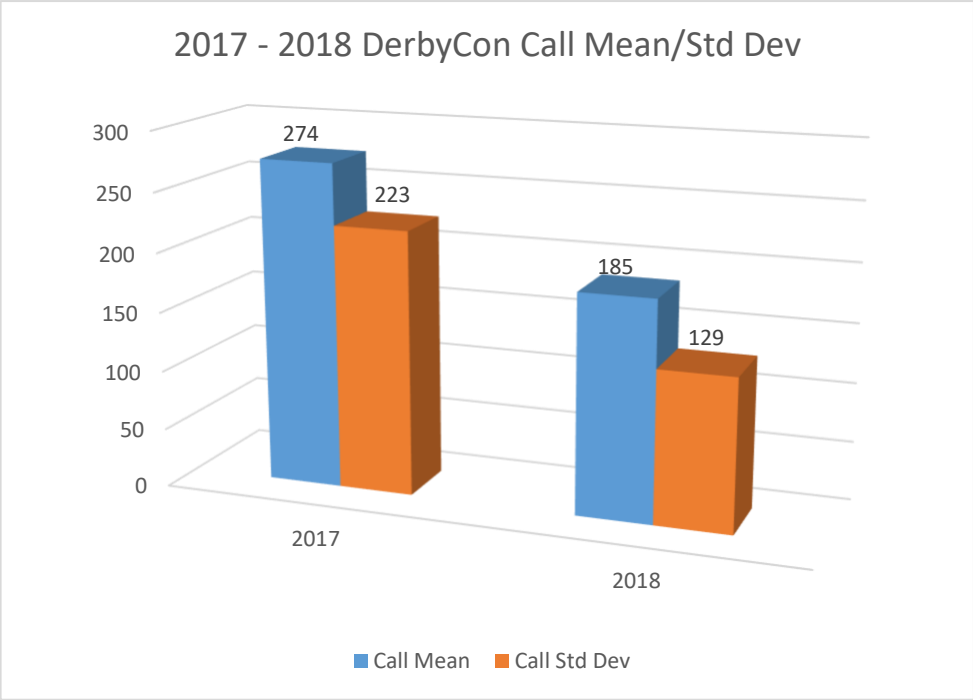

Figure 10: Comparison of call points means and standard deviations DerbyCon 2017-2018

Figures 11 and 12 quantify 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.

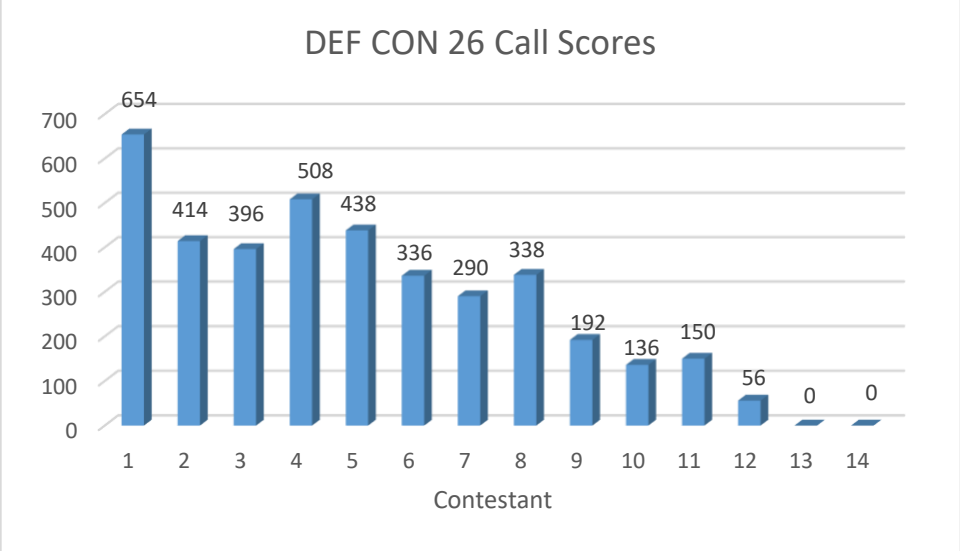

Figure 11: Live call scores by DEF CON competitor

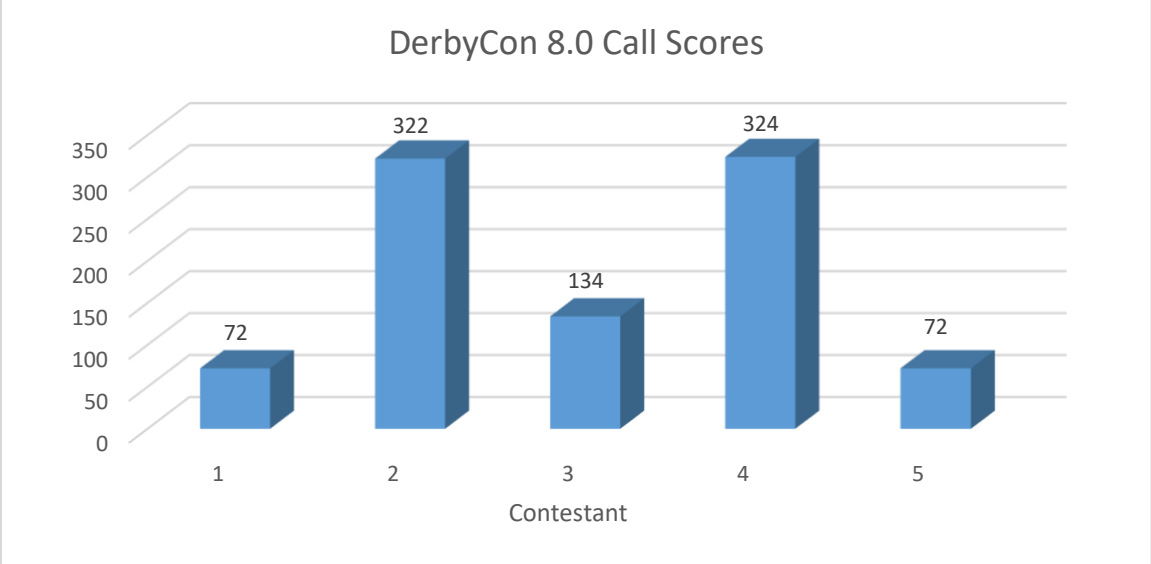

Figure 12: Live call scores by DerbyCon competitor

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 (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.

Figures 13 is a summary of the mean scores of both OSINT and calls for the past 5 years at DEF CON and Figure 14 is a summary of the mean scores of OSNT and calls for DerbyCon contestants in 2017 and 2018. The mathematical average of scores is impacted by outliers (either very high or very low), so is relatively limited in the information it conveys. One *can* surmise that competitor performance on OSINT 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. Contestants may be aiming to obtain higher point flags in larger quantities, therefore increasing the overall call scores this year.

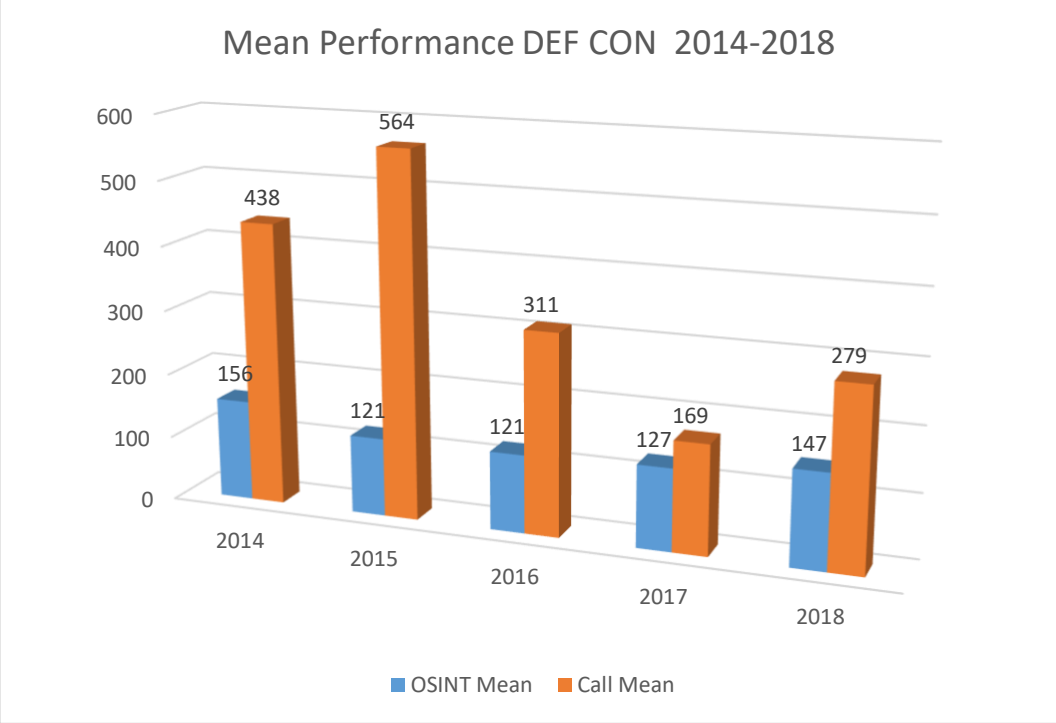

Figure 13: Mean performance for SECTF DEF CON 2014-2018

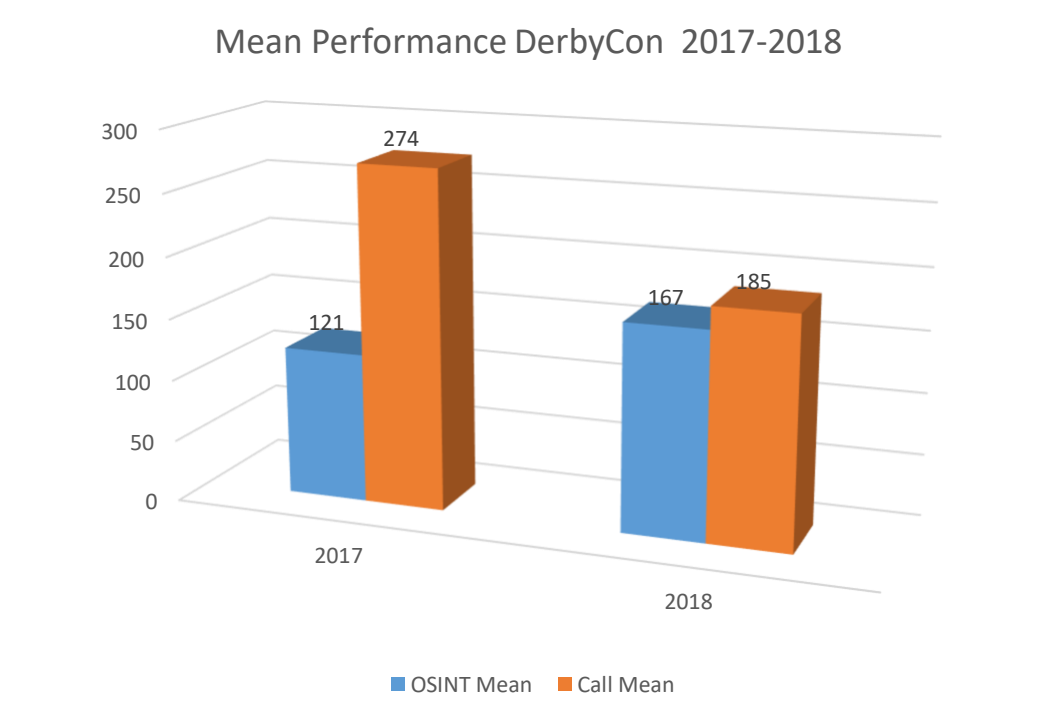

Figure 14: Mean performance for SECTF DerbyCon 2017-2018

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 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.
        - One target referenced a “big event” in progress that our competitor failed to pursue.
    - 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 every target’s name. For example, a target would answer and say, “Hello,

my name is Joe," and the competitor would respond, "Joe! No way?! That's my dad's name."
  - Successful competitors made use of dead time on calls. One returning competitor, while waiting for his pretext's "database" to load, would ask seemingly innocuous questions of the target that would elicit flags, such as, "So, how long have you been with the company?
  - One effective competitor was able to compromise a target and then have that target forward the competitor to another individual who was then also compromised.
  - 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 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:
  - The competitor targeting Alaska Airlines had to contend with the recent news that one of the company's planes had been hijacked. Despite this, the competitor was still able to elicit flags.
  - One contestant got the target on the phone and was notified there was no internet at any of their terminals. Therefore, the contestant had to think quickly to choose a pretext that would still elicit flags.
  - One first-time contestant who had a very low report score was able to receive the second highest call score
  - 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.
  - A contestant who competed at DEF CON and had a lesser report returned to compete at DerbyCon and wrote one of the highest scoring reports we received. It is evident that this contestant learned from their previous experience and grew, which is a necessary skill for strong social engineers.
  - All of our highest-ranking contestants in 2018 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.
  - In more than one case, a company's corporate directory provided the full names of individuals, providing multiple target opportunities with a single call.

Final Contest Results

At the conclusion of the live call portion of the contest, the judging panel met and reviewed all scores. Figure 15 and 16 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. Average OSINT scores remained stable for both DEF CON and DerbyCon, but call scores appear to have risen this year, which differs from the historical pattern of call scores decreasing.

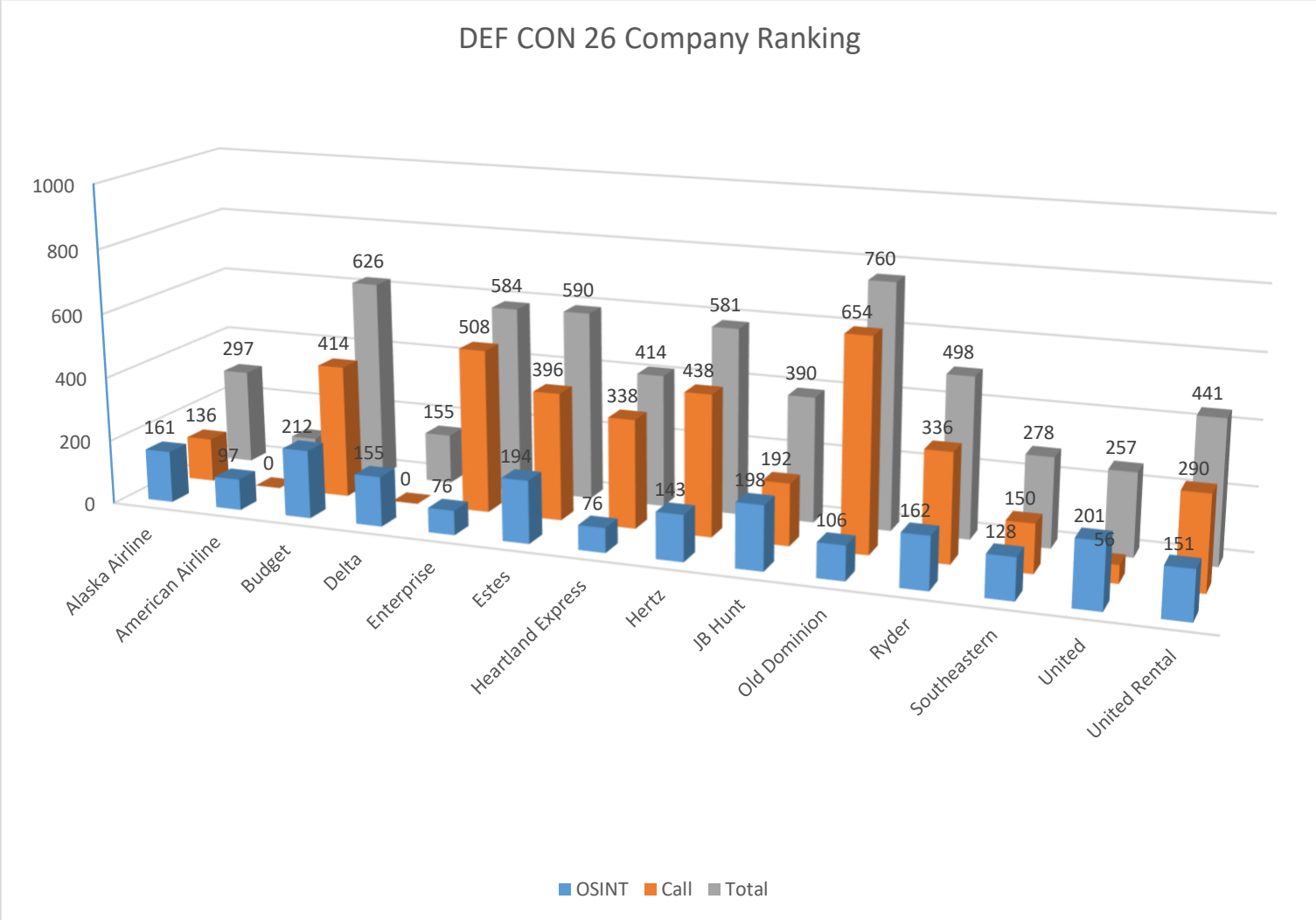

Figure 15: DEF CON 26 company ranking

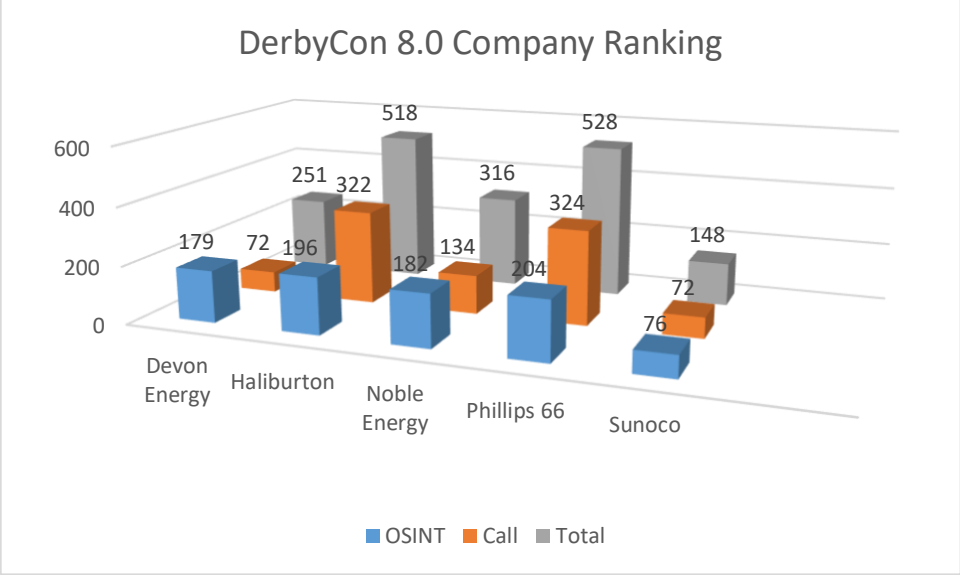

Figure 16: DerbyCon 8.0 company ranking

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 2018 is as follows:

1. American Airline
2. Delta
3. United
4. Southeastern
5. Alaska Airline
6. JB Hunt
7. Heartland Express
8. United Rental
9. Ryder
10. Hertz
11. Enterprise
12. Estes
13. Budget
14. Old Dominion

The ranking of companies from best performance (lowest score) to worst performance (highest score) for DerbyCon 8.0 is as follows:

1. Sunoco
2. Devon Energy
3. Noble Energy
4. Haliburton
5. Phillips 66

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. 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 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.

Figures 17 and 18 illustrate 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.

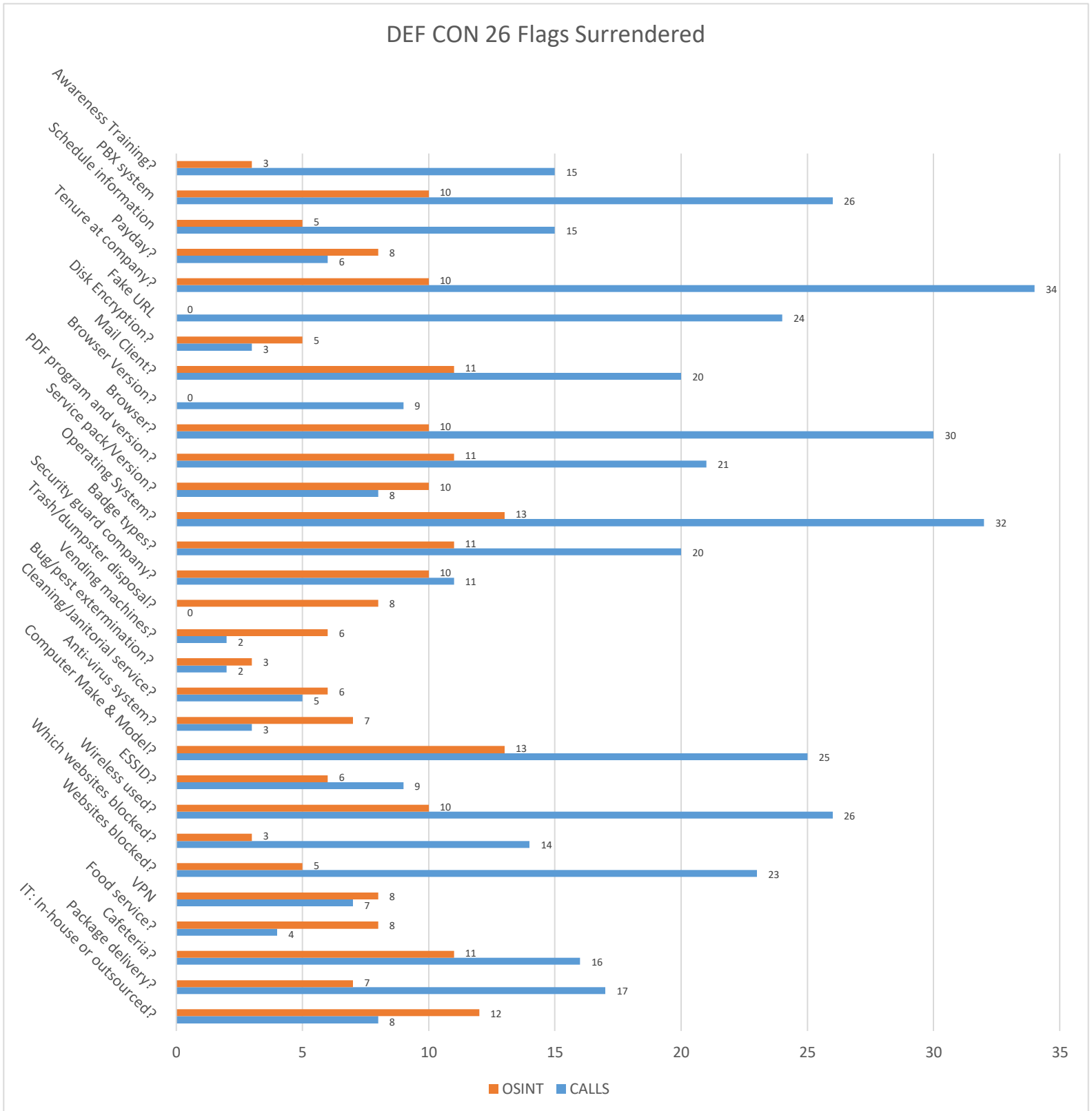

Figure 17: DEF CON 26 flag frequency distribution

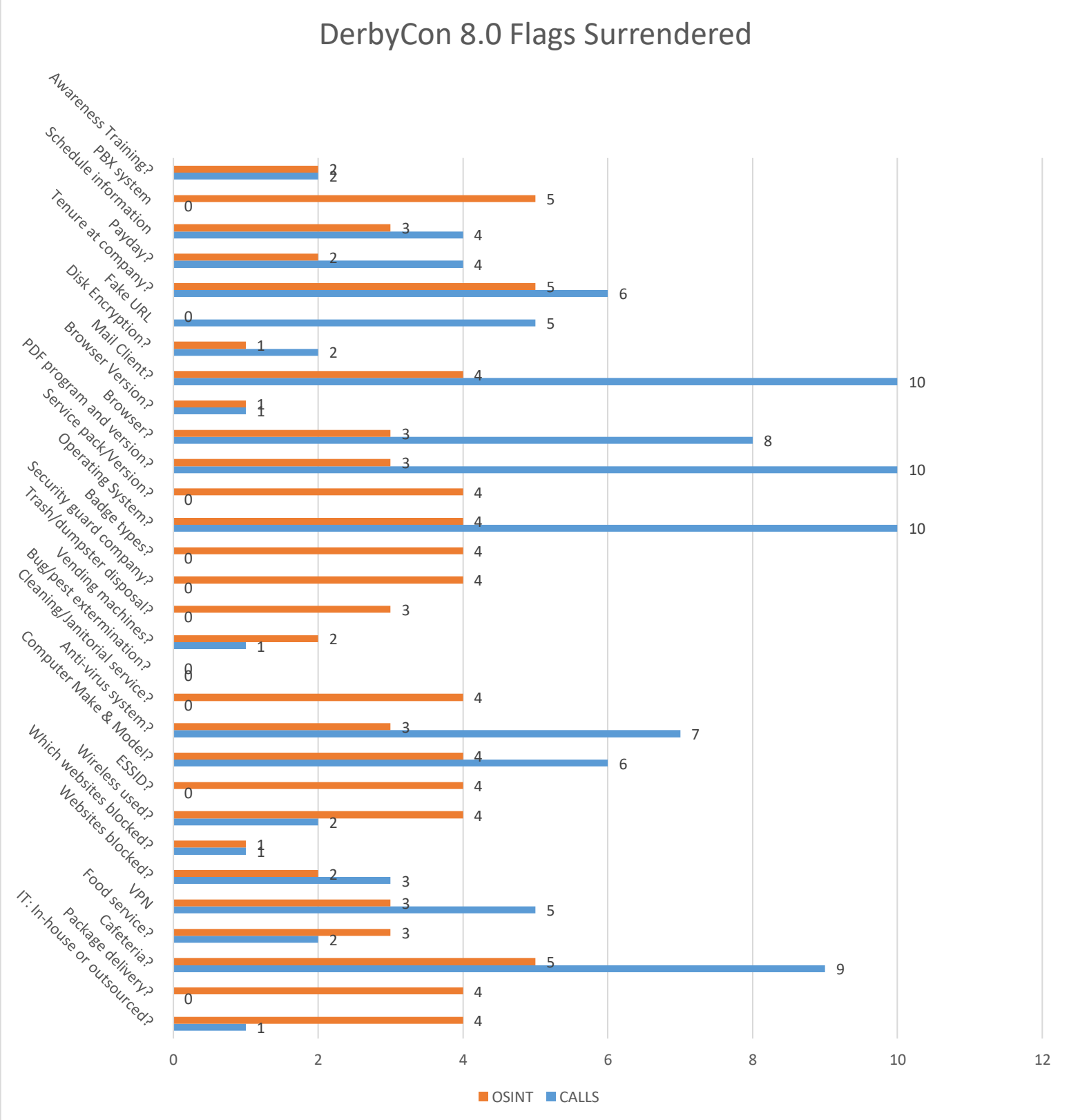

Figure 18: DerbyCon 8.0 flag frequency distribution

Inspection will reveal that the most commonly obtained flag this year at DEF CON was the amount of time the target had worked for the company, followed closely by what operating system was in use by the target. While the most common flag is identical to last year's top flag, historically the 2nd most obtained flag at DEF CON was, "do you have a cafeteria?" 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 flag could be used to perpetrate believable attacks via malicious executables that could affect the target's host machine.

There was a three-way tie for the most commonly obtained flag at DerbyCon. Those flags were:

1) what types of badges are used for physical access,
2) what service pack/version of operating system was in use, and
3) what version of browser was the target running.

The first flag could be used to help replicate the company's badges and facilitate access in an impersonation attack. The latter two flags are both very valuable when building and executing phishing attacks to facilitate network access at the targeted company. This information could be used in planning a phishing attack using a malicious link, particularly if it was determined that the target company had weak policies or controls in place to monitor unauthorized internet access.

The take-away 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.

In a departure from past years, there was one flag that was not obtained in either SECTF. That flag was, "who does your trash/dumpster removal?"

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 ninth 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 again this year 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 they are certainly 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 over sharing 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 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 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 hacker’s job that much 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 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.

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 that 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 businesses making 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

One large mistake that many organizations make is assuming a deficit model of decision making, which states that if individuals are provided with more information, they will make better decisions. There is a significant amount of research that indicates this is untrue. 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, SEORG has 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 SECTF, the "Mission SE Impossible," and "Can you Fool the Polygraph" challenge, and we also hosted a very successful panel on ethics in social engineering.

Based on an overwhelmingly positive response, the Social-Engineer Village is planning to return in 2019 to both DEF CON and DerbyCon. We will be releasing a Call for Papers along with our call for 2019 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

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 2018 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

KnowBe4
Human error. Conquered.

https://www.knowbe4.com

pindrop
security

www.pindropsecurity.com

Hillbilly Hit Squad

http://hillbillyhitsquad.com

RED SKY
A Presidio Company

https://www.goredsky.com/