Social Engineering Capture the Flag Results

Defcon 18

defcon@social-engineer.org

Christopher J. Hadnagy
Mati Aharoni
James O'Gorman

Table of Contents

Executive Summary

The “Defcon 18 Social Engineering CTF - How Strong Is Your Schmooze” will be remembered as one of the most ground breaking events of Defcon's 18 year history.

Social engineering is a real-world threat in Corporate America today, one in which many organizations do not take seriously. Our goal in organizing the Social Engineering CTF contest was to raise awareness of this threat. By organizing a contest that would allow participants to attempt many different pretexts on a wide variety of targets we felt we could demonstrate:

- The risk that is posed to organizations by even unskilled social engineers.
- Identify what approaches are actually effective in real world situations.
- Demonstrate how well organizations are protected against these sorts of attacks.

Attackers seek the same high return on investment goals as Corporate America. As technical defenses rise, the cost of technical attacks go up as well. Targeting people has become the most cost efficient attack vector in many situations, and all indications point to this trend continuing to increase.

Below are some statistics from the event:

Number of Companies Called:	**15**
Possible Flags:	**25**
Number of Companies with Flags Captured:	**14**
Days Contest Was Held:	**2**
Total Phone Calls Made:	**135**
Companies Who Put Up Resistance:	**7**
Employees Who Put Up Resistance:	**11**

This event is the one of the first times that social engineering tactics have been put on display to the public in a real world context against actual companies. For the first time, we can demonstrate what sort of attacks work against Corporate America and the ease in which they can be conducted.

Primary Findings

For awareness training to be truly effective it requires complete coverage of all employees. In many instances contestants would contact call centers, which often do not have as complete of awareness training programs. This translated into information leakage that could have been avoided as well as significant increase of risk to the target organizations. Demonstration of the ineffectiveness of awareness training was apparent by the lack of employee resistance to answering questions.

When employees do not have clear guidelines set in place in response to a given situation, they will default to actions that they perceive as being helpful. This natural response was what was utilized in every instance where contestants obtained high scores.

Companies need to provide direction to employees on social media issues and expectations. Social media remains a low effort vector for information gathering that very few organizations are addressing.

Information perceived as having no value will not be protected. This is the underlying fact that most social engineering efforts rely upon, as value to an attacker is different than value to an organization. Companies need to consider this when evaluating what to protect, considering more than just the importance of value to the delivery of service, product, or intellectual property.

Organizations need to understand that regardless of the protections in place, information such as operating system, browser version and so on will be compromised. Security by obscurity is still not an option, as it oftentimes leads to a breach. Security through education must be the foundation of every solution -- education on the tactics, the methods and thinking of malicious. This education will inform all other actions, providing an increase in effectiveness.

Background and History of CTF Event

The team at Social-Engineer.org was invited to run the Social Engineering Capture the Flag (SE-CTF) event for Defcon 18. The team carefully considered this request before committing as there was extreme concern on how to conduct this event in a manner that was ethical and still providing value to the community.

After committing, initial plans for the event were made by the Social-Engineer.org team, followed by announcements to the public. These announcements stated the rules, called for participants, and certified that sensitive information like passwords, credit card information, or social security numbers, etc. will not be allowed. Also a list of industries that prohibited was listed (i.e. government agencies, educational institutions, financial institutions). These announcements were met with a surprising level of unease in the industry, leading to alerts from various groups about the risk posed by this contest.

This wave of concern lead Social-Engineer.org to be contacted by the FBI. After speaking with the FBI, the team at Social-Engineer.org was able to explain the intent and the plan for the event, and the FBI provided important advice. At all times, a friendly relationship was maintained between the FBI and Social-Engineer.org.

Despite considerable efforts to assure that controls were put in place to ensure sensitive data will not be targeted and companies would not be harmed in this effort, constant concern persisted. This resulted in a number of contestants that were forced to drop out of the event. As such, on the dates the event occurred, only 15 of the original 33 scheduled contestants were able to compete.

Contestants were assigned a target company, with each having two weeks to use passive information-gathering techniques to build a profile. No direct contact between the contestant and the target was allowed during this time. The information was compiled into a dossier that was turned in and graded as part of the contestant's score. During DefCon, contestants were then allowed 25 minutes to call their target and collect as many flags as possible, which made up the remainder of their score.

Flags

Contestants were allowed 25 minutes to contact their assigned targets during the course of the contest. Flags were picked to be non-sensitive information, and each was assigned a point value based on the degree of difficulty in obtaining the information associated with the flag. The contestant's job was to develop a believable pretext along with a real world attack vector that would enable them to obtain as many flags as possible. Then they performed their attack vector live at Defcon during their 25-minute time slot.

In House IT Support?
Trash Handling?
How are Documents Disposed of?
Who Does Offsite Back-Up?
Employee Schedules?
PBX System?
Name of PBX?
Employee Termination Process
New Hire Process?
Open a Fake URL
What OS Used?
What Service Pack?
Mail Client?
Version of Mail client?
Anti-Virus Used?
Is there a Cafeteria?

Computer Make and Model
Wireless On-Site?
ESSID Name?
Days of Months Paid?
Duration of Employment?
Shipping Supplier?
Time Deliveries Are Made?
Browser?
Version of Browser?
PDF Reader?
Version of PDF Reader?
Websites Blocked?
VPN In Use?
VPN Software?
Badges for Bldg Access?
Who Supplies Food?

Results and Analysis

Dossiers

Each contestant was given two weeks to do passive information-gathering on a target organization that was assigned to him or her. The intent was for them to create quality dossiers in the same manner that is completed by professional social engineers when on a customer engagement.

Information Sources

The contestants used many different sources for gathering data on the assigned targets. However, a few information sources were used by almost every contestant: Google, LinkedIn and Facebook.

Much attention has been given to social media and its ramifications to information leakage in the last couple years. However, much of that attention has been toward consumer facing issues, not business-related issues. As such, the attention has focused on Facebook and Twitter as the two most popular services. In the course of information gathering, very few contestants made use of Twitter. Facebook, however, was used extensively as the number of public accounts make it quite useful.

LinkedIn is a service that has not received as much popular attention, but in the context of the CTF event was far more useful than any other single information source. Some contestants were able to build very complete organizational charts simply by mapping relationships of employees within their target organization. Further, by tracking what groups employees in key positions were members of, additional data such as technology used in the company or associations employees were members of became simple to document.

This use of public social media resources to attack organizational assets is a common issue in real world attacks, a fact that was reflected in this event. This is a difficult challenge for many organizations, as there are not clear boundaries between work and personal life in social media information management. It is important that organizations make clear choices regarding the manner in which they would like employees to behave regarding social media and then model that behavior with social media accounts that are pointed out to employees. With social media being such a new and immature industry, there are very few role models to use as examples.

Google was another avenue that was used by every contestant. Not only searching for the standard information using corporate websites and simple searches, but also utilizing more advanced Google Dorks, a list of queries on Google that can be used to reveal some surprising results. In many cases this led to some surprising results.

The other aspect of this that is easy to overlook is that a truly malicious social engineer will not only attack a target at their place of business, but through their personal life as well. If a target appears to be well protected, compromising a spouse or child that may not be as well defended might be the simplest path to a target.

Interesting Approaches

Through the information-gathering phase, much of the information returned in the dossiers was fairly standard. However, there were a few examples with unique approaches that are worth mentioning.

An interesting surprise was the use of Google Street View as an information-gathering tool. One dossier that was returned included complete pictures of the target organization's corporate headquarters, including identification of information directly associated with target flags, such as the name of the waste management company the target used and the off-site tape back-up company. Beyond that, possible entrances were identified, along with estimations of closed circuit camera coverage of the location.

Another contestant utilized searches like *Paper shredding "target company", +"target company" +pbx* and finally *+encryption +"target company".* These searches lead the contestant to gather quite a few PDFs that answered each of these inquires in full detail.

All of this demonstrated the fact that even non-skilled social engineers using standard search methods are able to gather enough information to develop detailed profiles of a company and its employees.

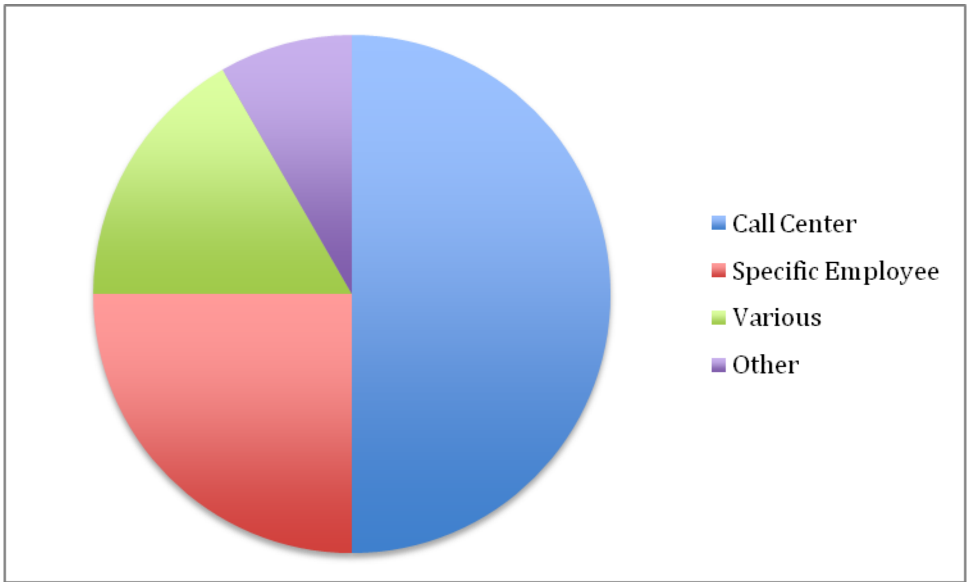
Calls

Successfully Targeted Employees

After a social engineer develops a detailed profile on the whole company, it is not uncommon to pick out one employee or group as the target for the attack. The logic behind this is that a stronger pretext can be built by identifying an employee or group and conducting a more in-depth information-gathering against this target, creating a scenario that is custom designed for the situation.

Indeed, this is what was initially planned for in the majority of the submitted dossiers. However, when the calls were attempted, not all of the calls were not successful. There were various reasons for this, but the most obvious one was due to the fact that there was limited time for the calls to take place (25 minutes per contestant). When a targeted employee was unavailable to answer the line, the contestant simply had to move on.

In the course of the contest, most successful calls were directed toward call centers. This allowed for ease of contacting a potential target, letting the focus of the contestant's time to be directed toward the collection of flags.



While this may be an anomaly due to the constraints of the contest, it raises an interesting, and often overlooked, point as to the very real possibility that all employees retain the capacity to leak important and sensitive corporate data. Very often, call center employees are overlooked in various employee awareness programs. However, this weak link, at least in the context of this contest, led to the vast majority of the captured flags.

Proper mitigation of this is quite an undertaking for most companies, as it requires proper and effective awareness training for all employees including call center and other similar employees. Only with complete coverage for all employees can an organization ensure that consistent controls are in place.

Pretexts Used

Pretexting is when a social engineer develops a storyline that he or she are able to portray to the target. It is more than just a line or a lie; it is a whole act that may include clothing, names, identities, email addresses, websites and much more to make the story believable. It provides the justification for the questions being asked. In the course of the contest, there were surprisingly few pretexts attempted. Many contestants independently converged upon three primary pretexts: A Customer, A Company Employee, or a Survey that is being conducted.

The pretext of a survey is an obvious one that justifies the contestant making a great number of questions without alarm being raised. Simple to conduct, this pretext is an obvious choice in many situations. However, it is a rather simple pretext to defend against by simply instructing all employees that authorized surveys will never be conducted other than through official channels.

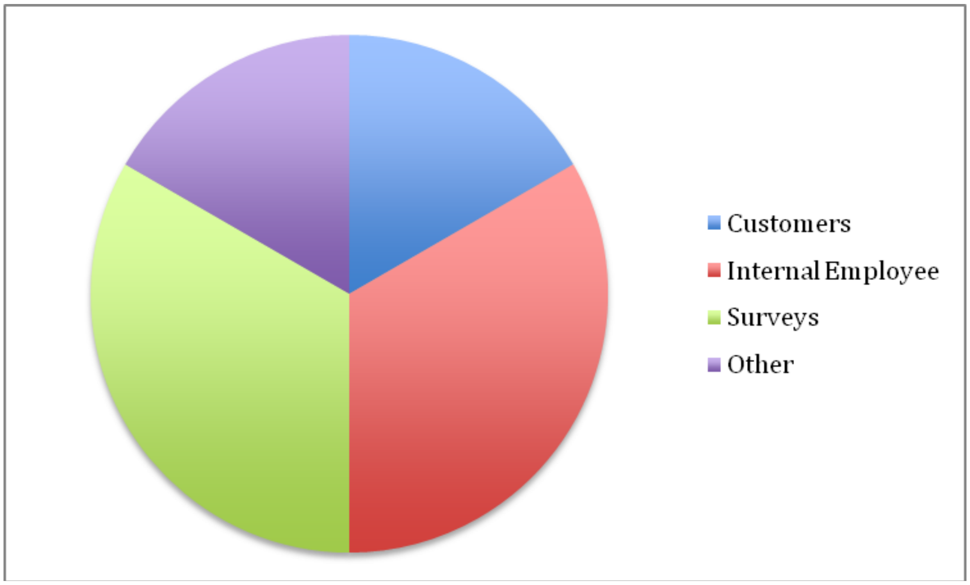
The pretext of internal employees, however, is a more complex pretext to successfully accomplish. Proper execution of this approach requires a greater degree of information gathering in order to ensure that suspicion is not raised by the caller not having information that an employee would be expected to have.

In fact, on more than one occasion, this pretext collapsed on contestants due to standard requests such as employee ID number. In some instances where contestants had not completed professional information gathering, they would often seize up and end the call. This is in part due to the relative inexperience of most contestants, as some of the more experienced contestants would find ways to ad-lib their way around or, in some cases, just ignore these requests altogether.

The final common pretext used was pretending to be a customer. This allowed for a justification of ignorance when information would be requested of the caller but increased the difficulty of flag collection due to a lack of justification of being allowed some information. Information gathering requirements for this pretext are rather minimal, allowing ease for the inexperienced contestant.

Other pretexts attempted worth mentioning include corporate security tests, reporters collecting information for a story, and job recruiters. The corporate security was a rather complex pretext to successfully accomplish; however, the contestant was able to pull it off with accomplished ease due to his experience.

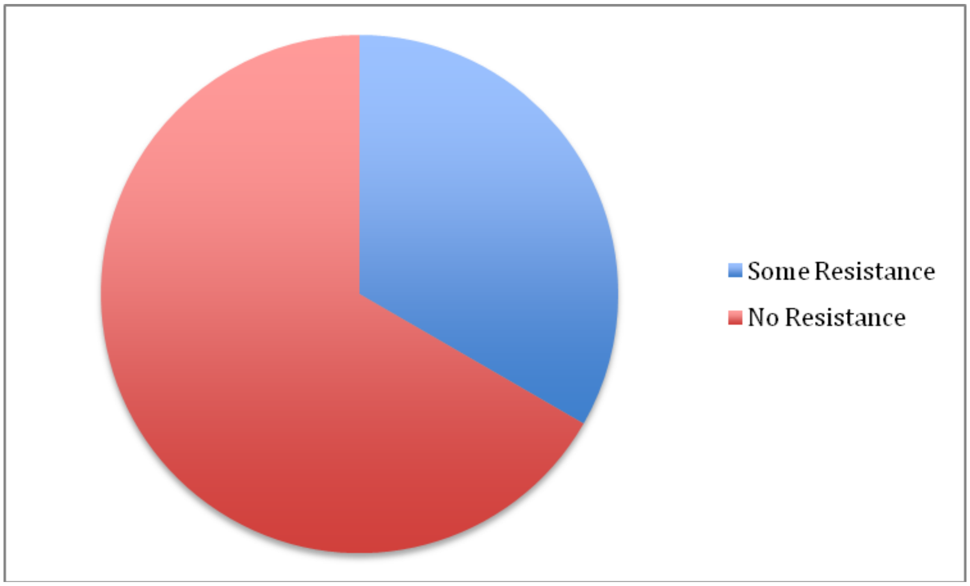
The instance of the job recruiter is another interesting point, as potential job seekers are in a state of mind to give information away in an attempt to impress. Collection of information in this case is also easy due to public resume posting boards. Mitigation against this one is particularly problematic as it draws to attention that even ex-employees could be targeted for information leakage.



Employee Resistance

The concept of employee push-back or resistance to information gathering based elicitation is a direct indication of how well the existing awareness programs are working within organizations. These challenges to questions the callers are making force the social engineer to justify why they should be allowed answers.

Unfortunately throughout the course of the contest, the number of times contestants encountered any degree of resistance was rather minimal. In tallying these results we took a very liberal approach on classification of resistance. According to our analysis, the results show that in the calls that were made, awareness training was not effective within the targeted organizations.



As disturbing as these results are, the full picture is even worse. For instance when some degree of resistance would be encountered, bypassing this was in every case simply a matter of calling back and reaching a different employee. In only one organization there were multiple instances of resistance in consecutive calls. However, after three calls the next employee encountered was willing and able to provide the flags the caller was requesting.

Indeed, more so than resistance to questions, the biggest obstacle once a contestant had an employee on the phone was simple ignorance of the answers to questions. It was far more likely for an employee to want to answer a question but simply not have the information that was being requested. At one point when calling a target and asking about browser type and Adobe software in use, the employee was so willing to help she said, "Let me just go to the manager's computer and give you the answers to this question." To some extent, this does speak to segregation of information as being a more effective defense than most organizations' security awareness programs.

In the instances that resistance was encountered, it was often driven not by suspicion on the part of the employee but rather by impatience at the time being taken out of the employee's day by having to answer these questions. In part, this was driven by the prevalence of the survey pretext, due to the fact that as a society people do not have much tolerance for what they see as "annoyance calls". The other primary driver was the employee having other, more pressing, duties in which to attend to.

In the cases that resistance was attributable to awareness, the calls were ended very fast by the target. They would simply state, "These questions sound fishy. Have a good day." Then hang up. In one instance, the target questioned the contestant about his pretext, then even went as far as to question him about his calling number and became very combative. This was encouraging to us as it showed a glimmer of hope that some employees are taking these matters seriously.

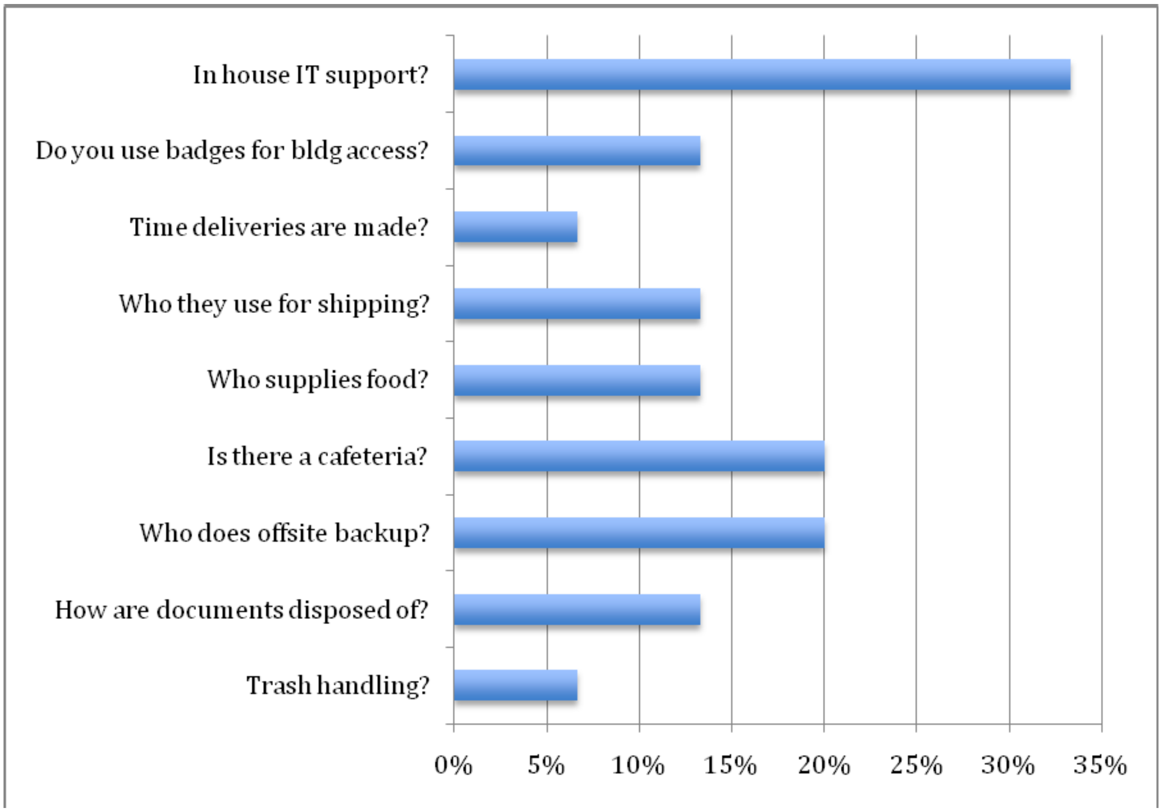
Information Returned

In the analysis of the data from the CTF event, we have separated out the various captured flags into categories of data that support similar attacks. The idea behind this is some information would be used to support a physical onsite attack, while other information would be most useful for technical attacks. Please note, that not every organization had every flag targeted, and as such, results are a combination of contestants that requested the information and organizations that had an employee which knew the answer as well as being willing to provide the flag to the caller.

Flags that were targeted in the course of this contest were information that is typically classified as non-sensitive. In many cases, the flags were data that could be found in public information sources or through information such as web server logs or e-mail headers. Information such as social security numbers, passwords, credit card numbers or other financial information was not targeted. Finally, the names of the individual employees contacted were never recorded and the phone calls themselves were not recorded.

Company Logistics

This category consists of information from internal company processes. This information can be used most obviously for physical attacks against an organization but also for tailored attacks using knowledge of the company processes against the organization.

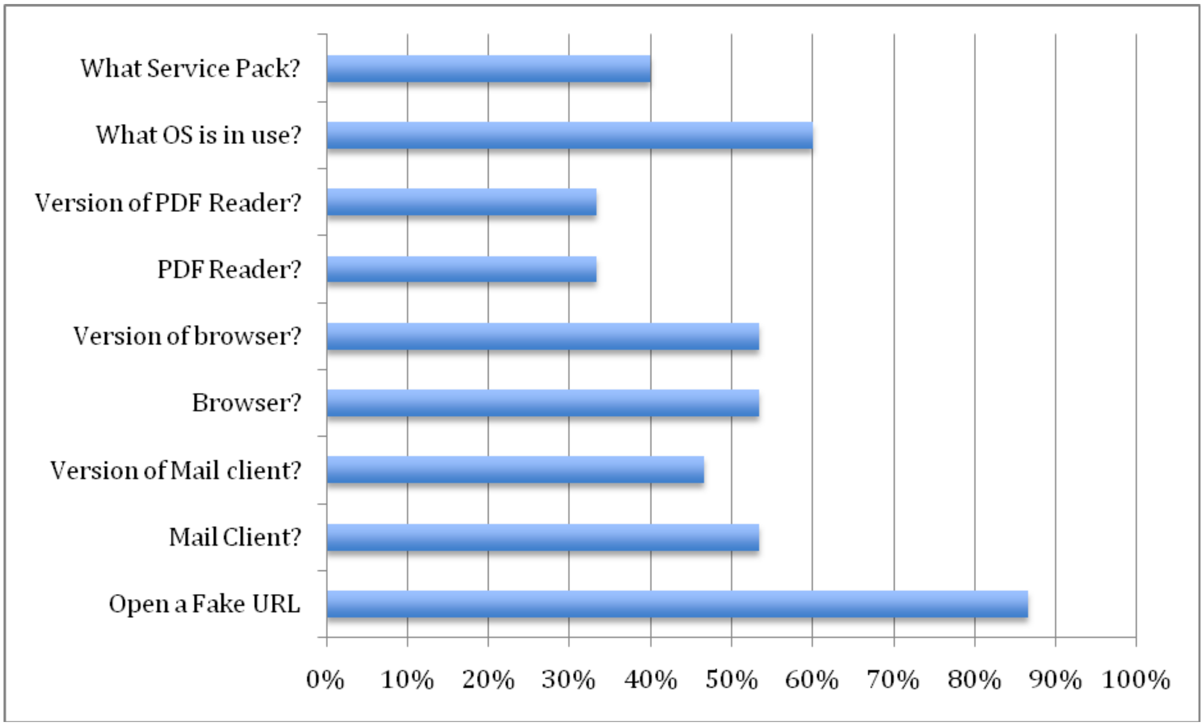


One example of this is identifying if the organization uses a third party company to stock their cafeteria food supplies. With this information the social engineer can create a solid pretext of faking a delivery of food supplies. This sort of information can be difficult for organizations to protect simply because it appears to be non-sensitive to many.

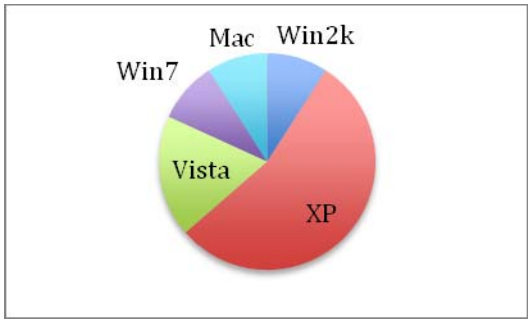
When information is perceived to have no value, no effort will be placed into its protection. This is what malicious social engineers rely upon, and make use of when conducting attacks against organizations.

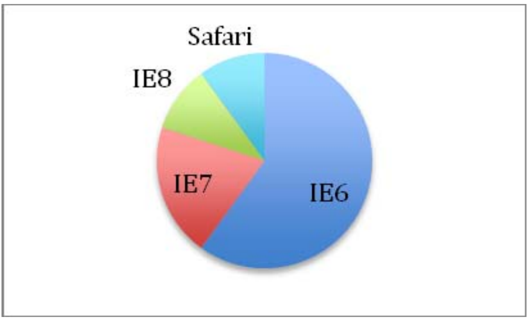
Popular Technical Information

This section defines flags that are associated with commonly executed technical attacks. The information associated with these flags is often associated with common remote attacks. For instance, in the last year the number of Adobe acrobat vulnerabilities that are exploitable had a drastic increase. Knowledge of what particular version is key information for a remote attacker when constructing a plan of attack.



As an example of the sort of information that was extracted, for the purposes of this analysis, we have compiled specific stats on common version information that was collected during the course of the CTF event. These numbers are obviously not a statistical sample of Corporate America due to the limited population of targeted organizations. However, if this had been an attack against these organizations, the value of the collected information becomes immediately obvious.



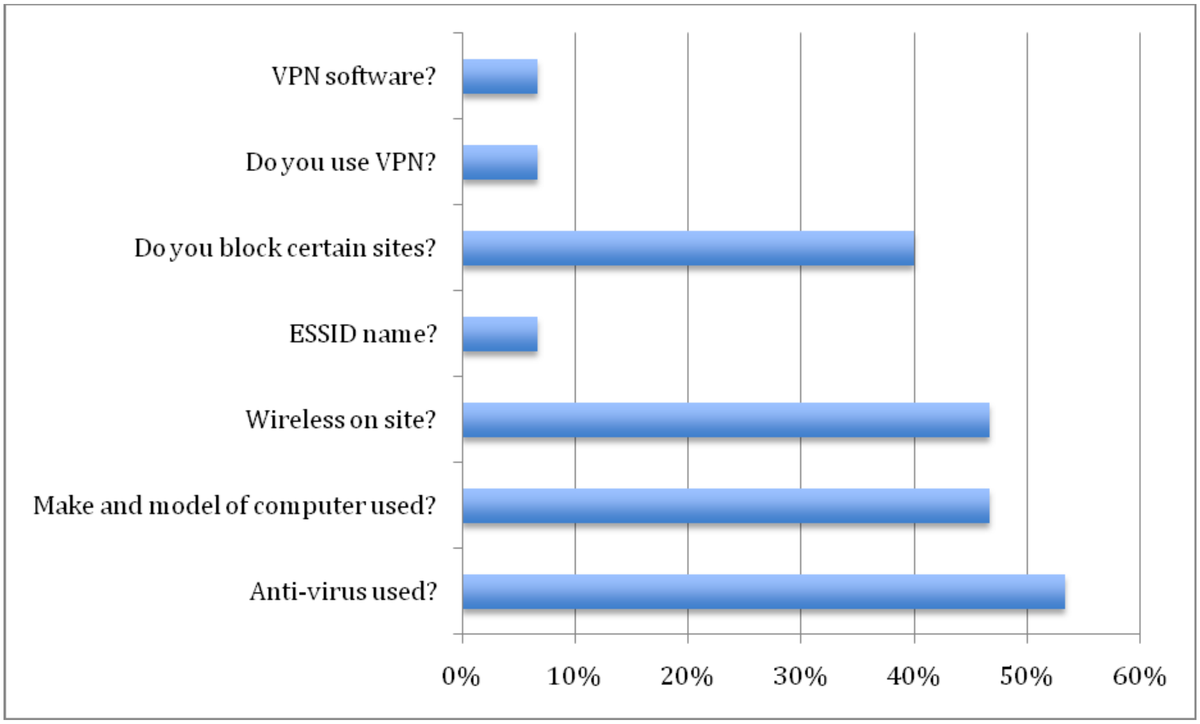


The combination of older operating systems and browsers deployed within the targeted organization becomes very troubling due to the quantity of public exploits targeting these systems. Combined with the statistic that 87% of the targeted organizations opened URLs in which contestants provided to them, it is even more troubling. Since the URL flag was the highest scoring flag on the list, it was the most attractive target to the contestants.

With it being proven to be a simple task to have a target organization open a specific URL and the widespread usage of Internet Explorer 6, a malicious social engineer has an easy path to a foothold into an organization.

Technical Information

This section consists of other technical flags that may not normally be associated with common attacks but can nonetheless still be devastating to some organizations. For instance, if a remote attacker is able to identify a VPN is in use at a target organization it opens an additional possible venue of attack.



In many cases, information within this category seemed harder to justifiably request in the course of a telephone call, and it is reflected in the lower rates for items such as ESSID names of wireless networks on site (additionally, the company would have to have wireless deployed on site for this question to even be asked, further lowering the pool of opportunity to make this request). In most cases that this request was made, it was normally in a give/take situation such as:

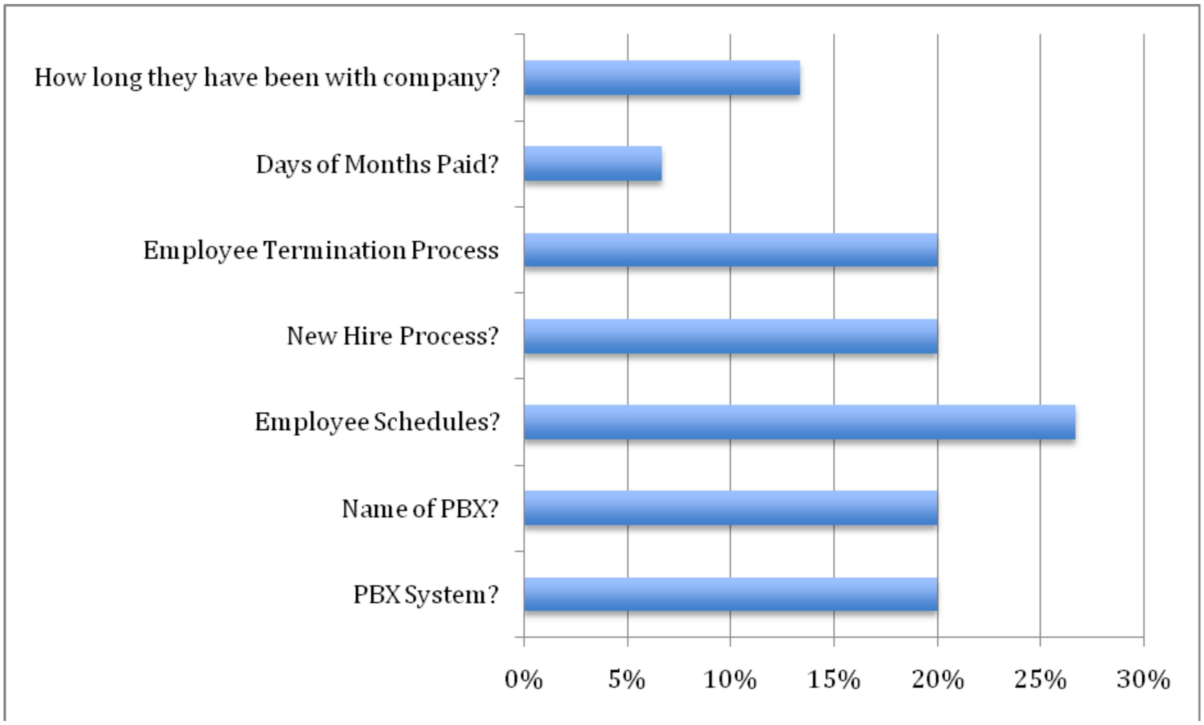
Caller: “Oh, so you run wireless on site? You know, I always find it interesting what companies decide to name their wireless networks, as they are often something silly. Like at work, we call ours “NoMansLand”. What is yours called? Is it something funny?”
Company: “No, we keep ours pretty simple, it's “XYZCorp”. I guess we don’t have a sense of humor around here.”

This sort of information being provided across the phone is shocking not due to the sensitivity level, but rather due to why would a caller legitimately need to know what brand of computer was in use at the facility? Again, we find information that is perceived to not carry any value will not be protected.

Additionally, employees need to be provided with simple and easy justification for denying callers with requested information. When a caller makes a request, regardless of how absurd, employees are in a situation where they feel obligated to help. Unless employees have been coached in a clear manner as to how to respond to uncommon requests, the default behavior will be to act as helpful as possible.

Employee

This final section is made up of flags that relate to information associated with employee information. All the flags in this grouping are relatively low return, which is a reflection of the number of attempts that occurred during the CTF event. This was not a surprise, as many of the pretexts did not easily lend themselves to allowing a justifiable request for information such as what days of the month employees are paid or details about the employee termination process.



In the cases where this information was obtained, it was directly related to rapport that was established toward the beginning of the calls. Once this bond was established, contestants would inquire about this information during small talk.

Importance of Being Busy

In some instances, companies managed to evade giving out information on specific calls simply by being too busy to deal with the call. This was often related to the pretext that was being utilized, specifically surveys. This built-in "busy" defense appeared to be the most effective defense most companies were operating under when it came to this attack.

The only instance that no flags were compromised from a company, it was directly related to the fact that the only employees the contestant could get on the phone were too tasked to respond to any questions when contacted. This was in part due to the unique nature of the company's business, due to which there was very few call center style locations to contact. Due to the constraints of the contest, follow up contact with the employees that were contacted was not possible.

Small Talk Leads to Big Data Leaks

One repeated lesson throughout the event was the fact that there was no substitute to simply being able to relate well with others. Consistently, all high-ranking contenders were quick to establish a person connection with the target and use that connection as the basis of building rapport.

With the call center locations being targeted as often as they were, pulling the employee off script quickly was a vital piece of the puzzle. Rapport became the basis of this, which had some interesting effects. For instance, if a request was made of the employee to the contestant, the contestant was able to deflect the question by stating they were obtaining that information somehow, and it would be there momentarily. During the time that information was being "accessed", small talk would lead to multiple flag captures.

Many contestants repeatedly utilized this sort of redirection. In related situations, contestants would simply ignore requests that were made of them as if they were not heard. Employees would very rarely repeat the request. This happened in multiple cases in regards to requests for employee ID numbers and even internal extensions as well as other identifying information.

One contestant in particular demonstrated a novel approach by capturing multiple flags without asking any questions. This was done through the use of assumptive statements that employees felt compelled to correct. Surprisingly enough, using this technique, they were able to obtain a sizable score without once putting employees in the mindset that anything was ever requested of them at all.

Called Number Plays a Role

In some instances, calls were made to public numbers instead of internal numbers. This should have been a red flag in all instances, but only a few occasions were the contestants challenged about this. Certain information the caller should have had if they really were internal to the organization was a related issue, but again was often overcome by simply pleading ignorance.

In only one instance was the caller ID information drawn into question. This is too bad, as it is an easy source of information for employees to use to question the caller. It is recommended that caller ID information play more of a role in standard awareness training. Although with the ease of spoofing the caller id numbers, (a technique we did not use for the CTF) it can make this even more difficult.

Conclusion and Recommendations

One of the primary factors in the success or failure of the contestant in the Capture the Flag event had to do with the planning of the overall attack. The most interesting aspect of this has to do with how quickly and easily information could be obtained from all companies in a relatively short period of time, even with the caller under pressure.

An important aspect of what was revealed by this event was that companies are only as secure as their weakest employee. In instances where one employee did not feel comfortable giving out information, a simple call to another employee and the information was compromised. This drives home the importance of awareness training for all employees, including the lowest level of employees within the organization.

Proper information gathering was obvious in its importance. In some instances, simple challenges such as a request for a zip code or e-mail address shut the calls down. With proper information gathering these challenges can be turned into an opportunity to demonstrate legitimacy to the employee and possibly obtain a greater level of trust. These stops would most likely not have been an issue in a professional or malicious social engineering venture, as preparation would not have been limited to 1-2 weeks.

Former employees leave the company with a large degree of company logistics in their head. This is important to consider, especially in relation to downsizing within organizations. Is it more expensive to deal with possible information leakage from a disgruntled employee or to take greater care in employee separation issues to ensure that former employees do not carry ill will toward the organization? Even if there is no ill will from the former employee, one contestant showed how easy it is to obtain information by asking questions like, "When you worked for TARGET what operating systems did you commonly use?" This information was given over to the contestant because his pretext was that of a job recruiter.

For internal company issues, it was proven that it is extremely important to have a stable and straightforward method to verify employee status before providing any information to callers. However, this raises the question of how often this sort of information is printed on employee ID cards and how often they are on public display in locations such as restaurants, etc.

Overall, what does all of this point to? Social engineering is a very real and dangerous attack vector in Corporate America. Security Awareness programs are falling short and not really getting through to the employees how serious this is. There needs to be a complete revamping of the methods and thinking that surrounds security in businesses today.

Social engineering threats will continue to increase if this year’s results are any indication of the level of training in large-scale companies. As software is built better and it is more difficult to gain access to data that way, hackers will turn to the easiest path into companies - The Human Vulnerability.

About Social-Engineer.org

Social-Engineer.org was developed to be the authority on the topic of social engineering.

Malicious parties have always been interested in obtaining real return on investment on attacks. With the advent of stronger and more universal protection systems in various networked systems, this has caused an increase in the cost required to successfully execute an attack against modern systems. This has caused many attackers to move to a lower cost avenue of attack, namely targeting people.

Social-Engineer.org has documented the manner in which these tests are conducted to increase awareness of this increasingly active attack vector. Only by understanding how these attacks are conducted can we build proper and effective defense.

Security through education.

Sponsors

The Social-Engineer.org CTF event was made possible through the support of the following organizations: Offensive Security, Continuum Worldwide, and the Electronic Frontier Foundation.