Exploits in Wetware: How the Defcon 2017 SE CTF experience can help organizations defend against social engineering.

Robert discusses his experience at the Defcon SE CTF and how his efforts clearly show how easy it is to get sensitive info on any organization. The 2017 Verizon report clearly shows the dramatic growth rate of SE attacks and Robert demonstrates how easy it is to get thousands of data points from an organization with OSINT. He then goes into the vishing strategy he implemented to maximize the points he collected in the 20 minute live contest. Without much effort Robert was able to know their VPN, OS, patch level, executive personal cell phone numbers and place of residence.

Robert lifts the curtain of the SE world by showing tricks of the trade such as the "incorrect confirmation" which is one of many methods to loosen the tongues of his marks. Robert then shows the pretexts he designed to attack companies and the emotional response each pretext is designed to trigger. By knowing the patters we can better educate our staff.

With that much information at his fingertips, how long would it take him to convince your executive to make a bank transfer? If your organization lost a few million dollars due to social engineering, who would be to blame? Are you insured for that? Who is getting fired?

Robert wraps up his talk with a series of strategies companies can take to reduce exposure and risk. He goes over current exposure, building defenses, getting on the offense and finally… a culture shift.

Table of Contents:

Introductions

Robert is a Senior IT Manager in the aerospace industry where he spends most of his time managing InfoSec teams. While his teams focus on the traditional blue/red team exercises, lately he has spent an

increasing amount of time building defenses against social engineering. Robert has spoken about the rising SE risk at numerous events and on different security podcasts.

Robert is also a nine year veteran with Search & Rescue in British Columbia, Canada. In his SAR capacity, Robert is a Team Leader, Trainer, Marine Rescue Technician, Swift Water Technician and Tracker. While one may think that SAR has little do to with InfoSec, tracking lost subjects in the bush has many of the same qualities as tracking individuals or organizations online with OSINT.

Robert grew up on a small fishing resort where he would have new friends every two weeks (he claims this had no psychological impact but we are not sure). When he has time, he enjoys super long (all day) runs in the mountains. He does at least one ultra run (50km) trail run per year.

Social Engineering (intro)

Social engineering has been defined by Wikipedia as the manipulation of people to take action or divulge information that would normally not be acceptable. This behavior is likely written in policy and would normally be not considered however the social engineer puts the mark into a position where it is acceptable.

Whereas most of us are familiar with the traditional social engineering scams such as tailgating, shoulder surfing and dumpster diving but the new threats such as phishing, vishing, smishing and pharming are less familiar to most.

Interestingly enough however, social engineering has been around for a long time and one only need to walk onto a used car lot to experience it with the masters. Sales and marketing has perfected social engineering so in many ways we can draw parallels to that.

The trend line of social engineering attacks is so steep if it was a stock we would all be buying it as fast as we could. In fact the 2017 Verizon Report clearly shows this on page 7. While some attack types are rising or even declining, social is looks like a 35% incline. Some companies are quoting 20% which is still alarming. Based on this growth rate, we should expect both an increase in quantity and quality.

Another interesting diagram to look at is the new OSI model with the “user” layer added to it. This new idea has not made it into the CISSP exam study guide yet but in enterprises we all know that our people are a huge consideration when mitigating risk. The “user” layer is a cost effective target for bad guys.

Does everyone agree with Kevin Mitnick that, “the weakest link in security is the human element” or do we need to do a quick demo?

Do demo. Apologize for social engineering them.

Show them the news articles. Easy to see the growth. Just Google it.

Defcon

2016 was my first Defcon and it really changed how I look at conferences and learning in general. People call Defcon a conference but it’s not. How can it be? At Defcon you can spend the night in the desert and

wake up to shoot huge fully auto machine guns with fellow infosec professionals. At Defcon you can party all night and then hack a voting machine. At Defcon I can sit in my hotel room or I can stand in line and meet the most interesting people.

If we have to call Defcon a conference then at least call it a collection of conferences with CTFs, workshops, talks, parties BBQs, villages and spontaneous events that just randomly start.

I always tell people that Defcon is more like Burning Man than it is a conference. If you look at the 10 principles of Burning Man, it is very similar to the spirit you will find at Defcon.

In 2016, I wondered around Defcon like a kid in a candy store. I ended up sitting in the social engineer village and promised myself that I would participate next year. I knew that the candidates were all very talented and that I would have to do something to stand out so I made this super creepy video which was basically me trying to convince someone to click on a link. It was bad. Super bad. But also very very creepy. I decided it might just be exactly what I needed to ensure they would never forget me. It was.

I was accepted. I was so excited. And then I wasn't. I had to do a ton of work to ensure I didn't have total failure in Vegas.

OSINT

Once you are accepted to compete the contest, they give you a target company which is part of a target industry for that year. For example, in 2017 the target industry was gaming. Therefore my target company was a gaming company.

There are two stages to the contest:

1. Three weeks to perform the initial OSINT which is a collection of 29 flags.
2. The 20 minutes of live vishing which takes place in Vegas in front of hundreds of people.

As soon as I started doing my OSINT I became addicted which is good because I ended up investing over 100 hours into my first stage which was the OSINT.

I started with LinkedIn which is a great tool for getting intelligence on corporations. To bypass the limitations of the free version and to avoid costly membership fees you can use tools like LinkedIn XRay which allow you to see a lot more.

LinkedIn allows you to start your OSINT base as it gives you many of the things you need such as organizational structure, titles, locations, tenure, industry connections and even connections to their other social media channels. For an organization, it is a target rich environment.

The flags are all very benign and relatively harmless yet something that the target company probably wouldn't advertise. This includes information such as type of computer and if they have a cafeteria. Some of this could be used by an attacker doing physical penetration testing.

As in most things, doing the OSINT resulted in the 80/20 rule. 20% of the staff gave me 80% of my flags. In fact, there were just a handful of people which were the social butterflies. These people gave up the farm.

Ironically, in LinkedIn when you look at people's profiles the often get excited and want to see who you are. I am sure we have all done this. Noticed someone looked at our profile and so we get curious and check out theirs. I didn't really think about covering my tracks and hiding until I was too far into it. If I was to do this professionally I would definitely want to be more covert to avoid detection. Don't wear orange when you go hunting humans…

My pretext development was interesting as I started off with huge and complex pretexts. I thought the more exotic the better. However when practicing with people at the bar I soon found out that these just didn't work. Working with real receptionists I quickly found what they would consider legit and what they would be guarded against. Acting with polite authority and being concise was the best mix.

Vishing

After handing in my report I had to prepare for Vegas. Defcon has one rule everyone tries to follow and it is called the 3,2,1 rule. Get at least 3 hours of sleep. Eat at least twice and shower at least once. People who stink with "con funk" are not popular.

I bought some comfortable shoes as I knew I would be logging at least 10,000 steps even though I would camp in the SE village. Everything in Vegas is big and routes you through the casino. Just going from your room to the conference could easily be a few thousand steps.

Now my marks, who were the individuals I targeted within the company were carefully selected. From several hundred people I knew I would only have a chance to talk to a couple people. So who would that be? I had several groups to choose from. I had the InfoSec people who gave me lots of info. I even knew what gyms they went to. I had the HR group who I had their personal cell phone numbers for. But at the end of the day I turned to the interns. These were the people with the least industry knowledge, the least company familiarity and likely the least amount of awareness training. I set out to violate the interns.

Unfortunately, the only people I ended up getting was the receptionists who were actually quite good.

The 20 minutes goes by fast. For the first 10 minutes all I got was voicemail. I fell back to anyone who would pick up the phone. This was reception. I got most of my flags in the last few minutes. Rapid fire.

I had 9 main pretexts. Everything from the FedEx courier to the University Intern Coordinator.

I also had a bunch of tricks I would. Some of my favorites were giving compliments and doing a false confirmation which I knew the mark would correct.

SE CTF Results

The results of my effort was a third place overall. I actually got third in OSINT and then third again in Vishing so at least I was consistent. The first place winner did extremely well on the vishing part and was a pleasure to watch.

A Reflective Moment

While the Defcon SE CTF is a lot of fun, it also points out some serious issues with organizations security. Right now we put so much emphasis on patch management and incident response. While these things are important, the rise of social engineering must be considered when developing a security program.

Some questions to consider:

- How bad would it be if your organization was a victim to social engineering?
- Who would get fired? If you don't know, it is likely you.
- Do your employees know how to protect themselves?
- Would they report a social engineering incident to you? Do they know how?
- Are you insured against one of your executives doing a large bank transfer to a bad guy?

Recommendations

Understand your Exposure

- OSINT yourself
- OSINT your company
- Find the 80/20s
- Understand what's at risk

Build up Defenses

- Make a phishing program. Vish your executive.
- More communication channels
- Create choke points – Invest in your receptionist
- Get rid of dial by name on your PBX
- Stop answering the phone

Get on the Offensive

- Culture of Security
- Gamify your training
- Recognize that policy is not keeping you safe

Culture Change

- Create a culture of heroes
- Celebrate success.
- Proud protectionism
-

Resources

- Michael Bazzell is a great resource. His website has a lot of good tools. He also has online training and an excellent book.
- Cybrary is good free training resource
- Pluralsight is a good paid training resource for corporate teams.
- Social-engineer.org is another good resource.