Shutterstock: Andrey_Popov

Jul 01, 2019 22:05 BST

Black Team War Stories Part 1 - Which company are you a contractor with?

The Target

The targets were three industrial sites spread over the UK each handling rare and controlled substances. The client's primary physical security concern was whether any of these materials could be taken off site during their production life cycle from an insider threat.

The client's main concern was an insider threat and less about external threat actors. After seeing their physical security, you can understand why.

Reconnaissance

The black team phase of the engagement required a substantial reconnaissance. It was evident that the target organisation had invested heavily in their physical security. They had numerous physical controls including:

- Dual 25ft fences
- Motion detectors
- Prison-style turnstile entrance and exits
- 2FA access control
- Full CCTV coverage
- Security personnel who turned out to be ex-military contractors
- Round the clock perimeter sweeps
- Random security searches.

It was also clear that staff recognised one another, meaning that any member of the Black Team who did manage to breach the site would likely raise suspicion by their presence alone.

Acquire Access

The obvious obstacle for this job was the 2FA on the perimeter. Tail-gating was out of the question due to the turnstiles. We needed legitimate passes and pins. That meant targeting staff leaving for work to clone their passes. We approached them asking for directions on our phones with the brightness turned down so they had to lean in to see, in turn making their pass come into contact with the cloner. The cloned data from the passes was then sent to the Red Team who could look up on the target's system to ascertain the corresponding pin and what level of access the staff member had. This was only possible as the Red Team had already acquired a foothold on the network via phishing and compromised the entire estate including the door control system.

With these pins and our newly created cards we had persistent access to the main site. Not only this, but the Red Team had grabbed design documents of the passes so we had exact visual matches.

Breach

The sites were enormous. Each consisted of multiple buildings with segregated access controls. The engagement was heavily time-limited with very specific objectives from the client and so breaching and searching every building to achieve the assessment goals would have been noisy and time consuming. Fortunately, the Red Team found building documents detailing what each building was and its function. The issue now was gaining access to the required buildings.

Lateral Movement

Each building was at least RFID controlled although the majority required a pin as well. It was also found, through awkward trial and error, that cloned passes didn't have access to the objective buildings. In an attempt to find more ways of breaching, the Black Team searched some offices in buildings they did have access to after staff had left for the night. The goal was to search for new passes that might provide wider access. Safes, drawers, offices and other secure areas were broken into and numerous items of clothing and passes were found. We took the clothing as it was branded with the company logo and helped us blend in at the other sites. Unfortunately any found passes were either deactivated or didn't have the access required. Just before Black Team left the building, security arrived on the scene carrying out their rounds. In a split decision the consultants made a break for the toilets. It's a fifty/fifty chance but one of the consultants ended up trapped in the females... After waiting for the guard to pass, the team made a quick exit leaving the site for the day.

So with no new passes found, the team decided to return to pass cloning. Using a two-man team, one consultant stayed on site and identified people leaving the target building. They sent their description to the second consultant outside the site. The second consultant would then engage those identified in conversation whilst attempting to clone their pass. This was very successful and over ten passes were cloned in half an hour. Considering this site was remote with little around, this was a win. Also one of the passes provided almost limitless access which meant we had our access to the objective building.

The Objective

Now we could access the building, all that was left was taking imagery (the easy bit) and leaving with it (the hard bit). No personal phones are allowed in

the building and searches are carried out on staff members leaving. Kind of like an airport style but more…personal. Now we didn't intend to enter this area yet but accessing an office area through a close by turnstile (which turned out to be one way) turned out to be linked to this area. So the consultant was trapped in there. As the consultant had already taken the imagery there was little else to do but leave performing a "Dynamic Risk Assessment" – wing it.

Busted?

So approaching the exit it turns out the searches are random, so there's some hope for getting out of this scot-free, but of course, the consultant is selected. Whilst this was a major inconvenience to the team, it does mean the client is getting a much more in-depth assessment of their security procedures. The client gains very little from the team "lucking out".

So the consultant is taken into the security room and all the exits locked. There are two guards who are clearly ex-military and the security process is solid. There was an airport-style x-ray scanner, a physical search, close inspection of the pass and a bazillion questions. In short, it would be extremely difficult to secrete anything through this office, and certainly not a mobile phone full of compromising images that the consultant had in his possession at the time. The "personal" mobile is spotted by security immediately and I kid you not, his face lost colour which is when it was obvious that this was pretty serious.

So things are going from bad to worse and the guard informs the consultant that they have to go through the calls, tests, and photos on the phone. Pretty much all of these have seriously incriminating evidence that the consultant shouldn't be there and has broken all the rules in the building. The consultant knows that the moment they see these, the gig is up, however, until they call the police it's still very much game on. "Dynamic risk assessments".

Acting as innocent and scared (latter not so hard) and trying to appeal to the guards' empathy by suggesting the consultant is new and younger than they actually are the search went down a completely different path than it should have done. The consultant no longer looked like a potential culprit, just a new employee who has "screwed up on his first week". This assumption also helped the consultant to remain in control of the mobile during the search –

a key factor in this scenario.

To prevent the guard noticing the incriminating imagery a number of “tactics” were used:

1. Turning the screen brightness all the way down

2. Scrolling quickly up and down

3. Drawing attention to the plethora of innocent information on the phone and subsequently away from the incriminating evidence

These simple methods made it difficult to identify any imagery on the device and the phone search ended without the security guard becoming aware of the considerable contraband images. At this point the consultant isn’t acting at all, and the obvious relief is very real.

All the things that should have got the consultant caught, the “Get Out Of Jail” letter being taken out and placed on the scanner and a vigorous inspection of the pass, which was a cloned fake, all should also have given the game away. However, thanks to a number of factors from both the Black and Red team the consultant finished the objective without being burnt.

That was the shakiest walk back to the van.

Site Two

With one site down, the second site was targeted. New passes were needed because the current ones didn’t have access to the site but there was nowhere to intercept staff near the site. Instead a couple of staff were followed over a mile back into town and close to home before a clone was made.

So using the branded clothing from the previous site and the newly cloned passes the site is breached. Without phones. Instead a couple of camera pens are taken in and when the imagery is captured the SD cards are removed and the pens hidden onsite. On the way back the changing rooms are found and hard hats/boots and other kit are taken making the team look even more like

staff.

To get the SD card through the airport scanner, instead of using a Rubik's cube, the SD card was attached to the back of a credit card on the reverse side parallel to the card chip. The wallet concealing the SSD card was then loaded with as many cards as possible to obscure the image when it went through the scanner. The idea was that the SD card and credit card chip would look very similar. If we could engage the security guard in conversation whilst the loaded wallet went through the scanner the SD card would hopefully go unnoticed.

Other items were also taken onto site to fill the tray for the scanner as much as possible - security through obscurity... This was an absolute success. However, one of the items brought in to fill the tray was a packet of cigarettes which turned out to be a contraband item. This triggered a series of questions about the consultant. As these questions became more detailed the guard was left to make his own assumptions. Better this than the consultant readily offering answers that would likely dig the hole deeper. The idea was that the guard would likely offer the answers he was looking for and the consultant could then just agree. One of these questions was, "Which company are you a contractor with?" The consultant happened to be wearing a fleece by a popular outdoor clothing brand, and before they consultant could respond, the guard read the brand name out loud, to which the consultant happily agreed. The outdoor clothing company then became the assumed contracting company...clothing had nothing to do with this site or the business in general and was certainly not a contracting company. Lesson learned? It is a lot easier to let people answer their own questions no matter how crazy the answer may seem, just get out before they realise.

Sprint for the finish

With two sites down, site three was the final target. By this point we had cloned so many passes that the Red Team were reverse engineering the data on the cards without access to the security door system. The result is they were able provide us with the data we needed to write our own cards with access to any site we wanted. We started with an initial breach with no incriminating or contraband items so there would be no issues at security. However, as expected, no search was required on our first trip. Frustrating, but we had identified a number of safe zones, such as toilets and canteens that we could take refuge in if needed.

Fortunately, on our second visit, this time with the camera pen, we were unchallenged on the way out of the area and so there was no security search. Regardless, we had primed the micro SD card on the credit card just in case.

Conclusion

This job required almost every trick in the book. NCC Group used multiple resources to gain access to what otherwise looked to be a site that could not be breached without detection. The key factors that allowed the team to remain undetected and breach successfully were:

- Working in parallel with the Red Team, which provided resources such as detailed passes, door codes and accurate locations of targets
- The extensive experience of the Black Team. This is difficult to plan for and requires expert, on the spot decision making, something the NCC Black Team excel at
- Pass cloning technology, although utilised in certain areas tail-gating was very limited at all of the sites.

The client received a detailed assessment of their physical security from both an outsider and insider perspective. Due to the security search, a detailed assessment was performed on the processes in place to prevent the insider threat from leaving with contraband items. On paper this process looked to be more than sufficient, only from the Black Team assessment was this process proved to be flawed. With the recommendations to the issues raised it would be exceptionally difficult to perform the same assessment without detection again.

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and

manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970

NCC Group - Financial Media Enquiries
Press Contact
Maitland AMO
Financial Results Media Enquiries
+44 (0)20 7379 5151

Regional Press Office - North America
Press Contact
NCCGroup@cdc.agency
+1 408 776 1400
+1 408 893 8750