Shutterstock: steved_np3

Jul 22, 2019 22:43 BST

Black Team War Stories Part 4 (final): Textbook

The Target

NCC Group was approached by a multinational R&D company which returns a profit of billions per year. Their primary concern was unauthorised access to their laboratories and the reputational damage that could potentially be caused if members of the public broke in.

The site was located on an enormous, shared business park. There were numerous buildings, canteens and an impressively intimidating security gate. NCC Group consultants were to perform a Full Spectrum Attack Simulation (FSAS) to try and gain access to the network, laboratories and any other areas where reputational damage could be done.

The Objectives

- Breach the company headquarters
- Gain access to the network
- Compromise the domain
- Identify weakness in the internal security
- Identify issues that may cause reputational damage
- Remain undetected during the engagement.

Recon

The OSINT for this job revealed a wealth of information. By combining the corporate videos with social media imagery the consultants were able to piece together a walkthrough of the target's main building. This included external and internal access controls and safe zones. Unfortunately no pass imagery was ascertained from corporate released media. The client had clearly gone through all their imagery to ensure that pass designs could not be acquired. However, towards the end of the OSINT phase a charity that visits large corporations was referenced on the client's social media page. Upon visiting the charity's own social media page numerous images were found with employees having their photo taken with the charity mascot. In these photos staff had their passes on display allowing the consultants to replicate them using design software. This highlighted the issue that although the client was aware of the dangers of uncensored staff imagery they had failed to realise that this threat goes beyond the imagery under their control.

The on-site recon was critical to this engagement. All the OSINT had suggested that the site would be exceptionally difficult to breach. There was a large number of security guards, a huge, intimidating gate house and each car was being checked upon entry. However, when the consultants arrived on site and performed an initial perimeter sweep they found that despite the sites fenced perimeter and guard house, there was an open entrance for dog walkers at the rear of the site. All this security and dog walkers were entering on foot all day. Site access – check.

The OSINT suggested that the back entrance to the garden area where staff were seen to have lunch would be a prime location to breach – join the staff for lunch, and then tailgate in as if you are from the building. However, when consultants arrived on site motion detectors at the entrance of this breakout area that were not shown in the OSINT were caught at the last second. Pulling back just before triggering the sensors the consultants targeted the main entrance instead.

Breach

So the site breach was simple. The area appeared to be open to the public, if on foot. The second stage of the breach was the target building. Consultants went with the front entrance tailgate during the start of the working day, which immediately led to unsecured meeting rooms and a canteen. NCC Group's strategy when breaching is a slow persistence attack

rather than a “smash and grab” methodology. When breaching, consultants will attempt to integrate with the business and staff. The goal is to convince staff that the consultants work there. This presents a very dangerous situation for businesses should attackers succeed in doing so. As with cyber attacks, the potential impact to the business can be far more severe when you are unaware of the attackers’ persistent presence. This is not something that can be demonstrated in one or two days but every business should be concerned about.

To the business' credit there were multiple layers of security before the laboratories could be reached. Now that consultants had breached the first two sets of security controls resulting in access to the canteen area, there were two more sets before the labs.

The consultants spent the next two days going in and out of the building. They played a few games of pool, interacted with staff members, occupied meeting rooms (and bugged them, obviously), put up fake advertisement posters (directing staff to a NCC controlled login page) in toilets and other communal areas. Consultants even helped members of staff with directions to other areas of the business (thanks to such a successful OSINT phase). These actions may seem cocky, however they are just a demonstration of detailed OSINT and planning stages of the engagement. By taking their time the consultants had integrated as members of staff.

The next step was to gain access to the office area. It was agreed that the best way to accomplish this was to tailgate people who were leaving through a secure door at the end of the day so the office space would be empty. Consultants could then impersonate IT staff doing checks if there were any staff members left to challenge them. This plan was further supported now that staff were comfortable with the consultant’s presence and would be less likely to challenge them. The only issue with this was that the main entrance to the building was access-controlled when leaving as well as entering. This meant that if the consultants stayed too late there would be no-one to tailgate out of the building and they would be trapped for the night.

Looting

So the team are in the office area and immediately individual offices are identified and accessed. The benefit of these types of offices over communal office space are that staff members cannot easily observe what you are doing. They also often belong to senior members of staff with more sensitive documents as well as, on occasions, keys and RFID tokens to more secure areas.

It was here that the Black Team were able to get a foothold on the network for the Red Team. To do this the Black Team worked in a pair, one keeping a look out for staff members whilst the second ran malware on a corporate machine to call out to the command and control server. The team were able

to log in to this host using credentials captured by the phishing campaign executed earlier in the engagement. It took two attempts to run the code on the machine as the Black Team had to quickly hide when the office was entered by a member of staff. However, after the successful second attempt the Red Team then spent the night acquiring persistent access so that the Black Team would not be required to enter the site each time they needed to access the network if the host was turned off. Textbook.

Know Your Limits

One of the final goals in this engagement was to see if access to the lab environment could be gained. This is an understandable requirement from the client and one seen regularly from clients with such environments. However, this is a simulated attack and these areas are often extremely dangerous and delicate. It is important to know your limits as security consultants. Just by entering an environment such as this the Black Team could inadvertently cause damage to production, materials or the lab. At worst, serious harm could come to consultants and/or others. Often these environments have materials that are not available to the public for good reason and consultants are not trained to handle or deal with such materials. In these situations it is evidenced that access controls to these areas could be bypassed and left at that. It had already been demonstrated that it was possible to move around the building undetected. This, combined with being able to get past access controls to sensitive areas, should be sufficient to demonstrate to a client that the objective has been achieved. Any further desires/requirements should be discussed prior to the engagement with the client.

Lessons Learnt

Both the client and NCC Group consultants gained a lot from this engagement despite it being a “textbook job”. The client was concerned that members of the public would be able to access their laboratories or access any other sensitive information. Consultants were able to demonstrate the sensitivity of areas that the client was not aware of by bugging meeting rooms that were outside the most secure areas of the building. The laboratories were shown to be accessible if attackers were willing to take their time, integrate with the staff and gain their trust. This raised the client’s awareness of persistent attacks – something they were not aware of before the assessment yet were at great risk of. The result was complete and persistence physical and cyber compromise. NCC Group also demonstrated new avenues of attack in areas where the client believed they were strong. By targeting third parties in the OSINT, critical findings that led to the physical breach were identified.

After identifying these weaknesses NCC Group were able to illustrate key changes that would likely prevent attackers from gaining such a foothold, and demonstrate how to detect attackers if they were successful, in order to

avoid persistent access.

Although hardly a dramatic job, NCC Group took the opportunity of an early, simplistic breach to develop new ways of identifying issues for clients while on site. These resulted in further credentials being harvested in ways that can be used on future engagements when conventional methods are unsuccessful. The key here is in developing skills and continuously staying ahead of malicious attackers to provide a continual service to repeat clients that they benefit from, and so avoid becoming a “one trick pony”.

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 15,000 clients worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company’s knowledge, experience and global footprint, it is best placed to help businesses identify, assess, mitigate and respond to the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With over 1,800 colleagues in 12 countries, NCC Group has a significant market presence in North America, continental Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia 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