Jun 25, 2021 10:46 BST

A Whole New World

Mark Frost, Managing Security Consultant at NCC Group

It is no secret that the physical security world has taken a back seat during the pandemic. Despite this, the dominant question that kept getting asked was “are restricted environments more or less at risk during lockdown?”

There are many views on this topic, but as organisations return to the workplace, secure environments face a new challenge.

How has the physical security threat landscape changed?

There are many ways to compromise an environment's physical security. But acquiring persistent access whilst remaining undetected is commonly achieved by following the building's legitimate processes and policies as closely as possible. For example, attackers posing as visitors have a high success rate because this process involves letting individuals into an environment that they should not normally have access to. This is ripe for attackers to exploit to gain persistent access.

Now, with staff returning after such a long time away from the office, the number of new scenarios and issues that can be exploited (like the "visitor scenario") is yet to be seen. This could include expired access cards, welcoming employees that have never been to the office, changes in required access, entirely new offices and so on.

Each of these scenarios will put security processes to the test against covert threat actors for years to come. In this short article, we will look at a couple of the more successful scenarios used in previous years, and how they might be applied post-lockdown to get you thinking about how the threat landscape might have changed for your business.

Impersonating staff members

Large organisations are vulnerable to attackers claiming to be staff visiting from another site. With a little information about a staff member (staff ID, line manager, etc) and a vague visual resemblance, threat actors can gain a legitimate form of access to the building. This might be a temporary pass the attack can clone, or just access for the week – more than enough time to leverage further persistence.

Post lockdown

The aforementioned scenario requires specific factors to be successful. But with the large recruitment drive now businesses start to recover, how many new staff members will be returning to the office for the first time? Additionally, how many will not be registered on the lease building's security system?

What is the policy to stop staff and security acclimatising to unknown individuals requesting access? Will security staff just start opening the gates

for “another new starter that has not yet received their access card”?

“Spot Check”

Showing up to “check the fire extinguishers” or “service the printers” has seen a decline in its success rate. From the silver bullet of physical scenarios, it has moved in to the “oh yeah, are you now...” skepticism. But in their time, these scenarios set the foundation for a whole world of “spot check audits”.

Post lockdown

Covid inspections are a necessary part of returning to work on behalf of the government. And with the seriousness of Covid, will people follow the proper checks before admitting individuals? Keep an eye out for our next blog, where we explore this example in further detail.

Cleaners

Going in posed as the cleaners can be a great way of getting into a workplace after hours without much attention from staff. It can require as little as a polo top and some combat trousers. Where this scenario can fall short is when staff are familiar with the cleaners.

Post lockdown

You can think of the return to work as “a clean slate”. Many staff changes will occur across roles, and whilst staff may have previously been familiar with cleaners or maintenance, they will be less likely to question a whole new roster of individuals in these roles. For the next couple of months, attackers might find that they are able to use this guise at most targets without raising suspicion.

Changing the Environment

Any good physical consultant, thief or person trying to maintain a level of stealth knows to leave no evidence. This starts with ensuring any environment that you enter is left the way you found it. Its no good deploying key loggers, drop boxes, listening bugs, cameras and other devices that need

retrieving another day, if the staff and security team notice someone has disturbed the environment during the night. And you can be sure that once they discover one device, the whole site will be on the hunt for the next trophy.

This raises an issue when removing IT devices. Remove a piece of equipment that someone has been working on for the last three weeks, and they are going to notice. And now they don't have their device to work on, they are likely going to spend the day hunting down what happened to it, meaning that when you return the device, its going to look suspicious.

Post lockdown

Office familiarity is a strong defense against persistent attack. But how familiar will staff be having been working from home and not the office? Will staff just assume that the IT laptop must be at home or the head office?

Furthermore, companies sent huge amounts of IT equipment out to remote workers. How sure are businesses that the equipment being sent back (and subsequently connected to their network) actually belongs to them? How sure are they that these are not compromised devices designed to provide a network foothold for the Red Team?

Expired Access Card

One of the first objectives when on site during a physical gig is to create visually accurate staff passes. This will satisfy most challenges for staff members when inside a compromised secure area. However, sometimes its use can go one step further. Threat actors can claim that the card has stopped working to request a temporary pass. Attempts from the security staff to verify the pass can quickly cause this scenario to fail, and being caught with a forged staff pass is an awkward situation for even the best social engineers to talk their way out of.

Post lockdown

There are going to be an enormous amount of expired access cards as people return to the office. The opportunity for threat actors to exploit the fact that access cards haven't been used in a prolonged period will be endless. Even if

a forged card doesn't read when checked by the security team (as an expired card should), or the individual does not appear on the access card system, 12 months of inactivity will be enough to excuse any anomalies with the presented card.

And this leads us on to what the real issue is. During lockdown, we saw a relaxing of security controls in favor of health and safety. Now we will see what malicious actions that bypass security policies are excused as a result of Covid, instead of being correctly identified security incidents.

Are your security policies up to date? Do they take into account the return to work of staff? Are your security controls resilient to attack, having not been used in 12 months? Now is the time to start asking these questions and reviewing your security controls.

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