Insight Space

cyber insights programme

nccgroup

Business Viewpoint

Think like a threat actor:

Counter common techniques to secure your organisation

Tim Rawlins

The techniques used by criminals to attack IT systems, whether they're criminals or nation-state actors, are often the same. It can mean that it's difficult to tell them apart.

However, it also means that if you harden your systems and educate your staff about commonly-used techniques, you will make your organisation more resilient.

This paper is designed to help you understand the techniques used by the criminals and the common methods to stop, delay, or detect them. This should allow any executive to challenge their IT team, security manager, chief information security officer or IT guru, at any level, on the practical security measures in place to defend their organisation. Finding the optimal level of security to reflect the risk and investment required to defend against it is difficult. But with this knowledge, at least a better-informed conversation can take place.

We use the same methods employed by criminals to test an organisation's ability to stop, or spot and react to, an attack. Our 'Red Team' simulates criminal activity to help identify any weaknesses, so that you can fix them before suffering a real attack.

We know that criminals and hostile states regularly follow the same routes during an attack and so the methods and techniques have been codified into the "Mitre ATT&CK" framework. This framework makes it easier for organisations to examine their defences to see what they have in place to stop or detect an attack at the various different stages.

We've identified issues throughout this paper that have an associated Mitre ATT&CK number, which describes a particular technique, as well as outlining the steps that attackers typically take when trying to break into business systems. To get reassurance that things are under control, ask to see the evidence that each issue and technique has a mitigation in place.

This is where the criminals, known in the cyber security world as "threat actors", look for information about the organisation they are targeting.

Our 'Red Team' simulates criminal activity to help identify any weaknesses, so that you can fix them before suffering a real attack

Reconnaissance

Most organisations and their staff leak information and it is very difficult to control such leaks. But identifying what information is available, most often on the internet, can help the organisation identify where accidental oversharing of internal information is taking place and help address it.

Common places to look for information leaking include:

- Staff job adverts - which may reveal your IT systems, either current or planned
- LinkedIn - where project names, IT systems, security clearances, roles and responsibilities are public, and email and phone numbers are often available
- Staff and organisational social media accounts - particularly where staff passes are included on photos, and people talk about internal issues and projects and identify colleagues
- Council, real estate and office building websites - these often include floorplans with too much detail, such as access control points and IT rooms, and policies for getting into a building
- IT developers' code stores - such as GitHub, BitBucket, GitLab, and SourceForge where internal information including individuals' names, IT details and even passwords are regularly found
- Breach databases - where email addresses and passwords can be found, giving a helping hand to the criminals

Once the threat actors have enough information to target an organisation, they move on to the next stage known as In Phase.

Insight Space
cyber insights programme

What to ask your security team:

- Do we actively look for publicly available information about our organisation? If it is sensitive, what steps can we take to remove or amend it?
- How can we avoid this information being published in the future?

In Phase

In this stage, attackers look to gain an initial foothold on the network and, using the Mitre ATT&CK framework, may seek to **exploit vulnerabilities**, known as ATT&CK T1190.

Trying to remove all the vulnerabilities from an IT system is extremely hard. The usual mantra of 'patch your systems' to ensure that the latest version of software is in use on every machine across an entire network of laptops, routers, switches, servers, printers and firewalls etc. is very difficult. This is particularly true where old, legacy systems and third-party equipment and processes are necessary to deliver business services.

Start by ensuring that systems that can be seen from the internet are as up-to-date as possible. This does mean that an accurate record of everything in the system, no matter how old or unused, will help ensure that nothing is missed. Too often compromises have come via old equipment or websites that have been forgotten about but are still connected internally.

Regular scanning for known vulnerabilities should help identify when something needs to be looked at and prioritised for replacement.

If the system is no longer supported by the manufacturer or supplier, but is business-critical, then additional protection must be put in place to defend it.

You should assume that your IT systems have been attacked and the attacker is on the inside, known as an 'assume breach' mentality. Having this mindset means that you will understand that even internal systems, not visible from the internet, are vulnerable.

To maintain security, you should put in place a regular review to identify updates and new vulnerabilities. This means an internal scanning process should be in place, as well as an external scan.

Another essential way to improve resilience, described as the ability to resist and then adapt to change, is to ensure that any system that can be seen from the internet is hardened. This is to counter the **external authentication exploitation** known as ATT&CK T1078.

Insight Space

cyber insights programme

Regular scans can also help to identify misconfigured systems that are connected to the internet – often, systems that were thought to be 'internal only' have been a regular way in for both threat actors and our Red Team. Identifying these weak spots and removing any points of access that only require a username and a password from internet-facing websites and systems is essential.

Instead, these systems should require a form of multi-factor authentication. Ideally, this will reply on the users entering a username, a password and a randomly generated number from an app on their phone, although other methods using keys, text messages, and dongles are also available.

Just having multi-factor authentication is not enough. There needs to be some monitoring or logging of attempts to gain access. And then an investigation of unusual attempts such as logging in from unusual locations, at strange times, using odd equipment or from different locations with the same account details in a very short period (known as impossible travel). There are lots of unusual behaviours that the threat actors use to log in, but effective multi-factor authentication will resist many of them. It will also help to limit success of the phishing (email-based) and 'vishing' (voice or social engineering attack) identified as ATT&CK T1192, T1193, T1194, TA0003.

Phishing emails are one of the most common ways that organisations are attacked. The more sophisticated attackers will use the information gained during the reconnaissance phase to send emails targeted at specific individuals. This is known as 'spear phishing' and frequently targets IT administrators with high levels of access, personal assistants with access to their boss' emails, finance departments, and individuals with high levels of authorisation to internal systems – including the executives such as you.

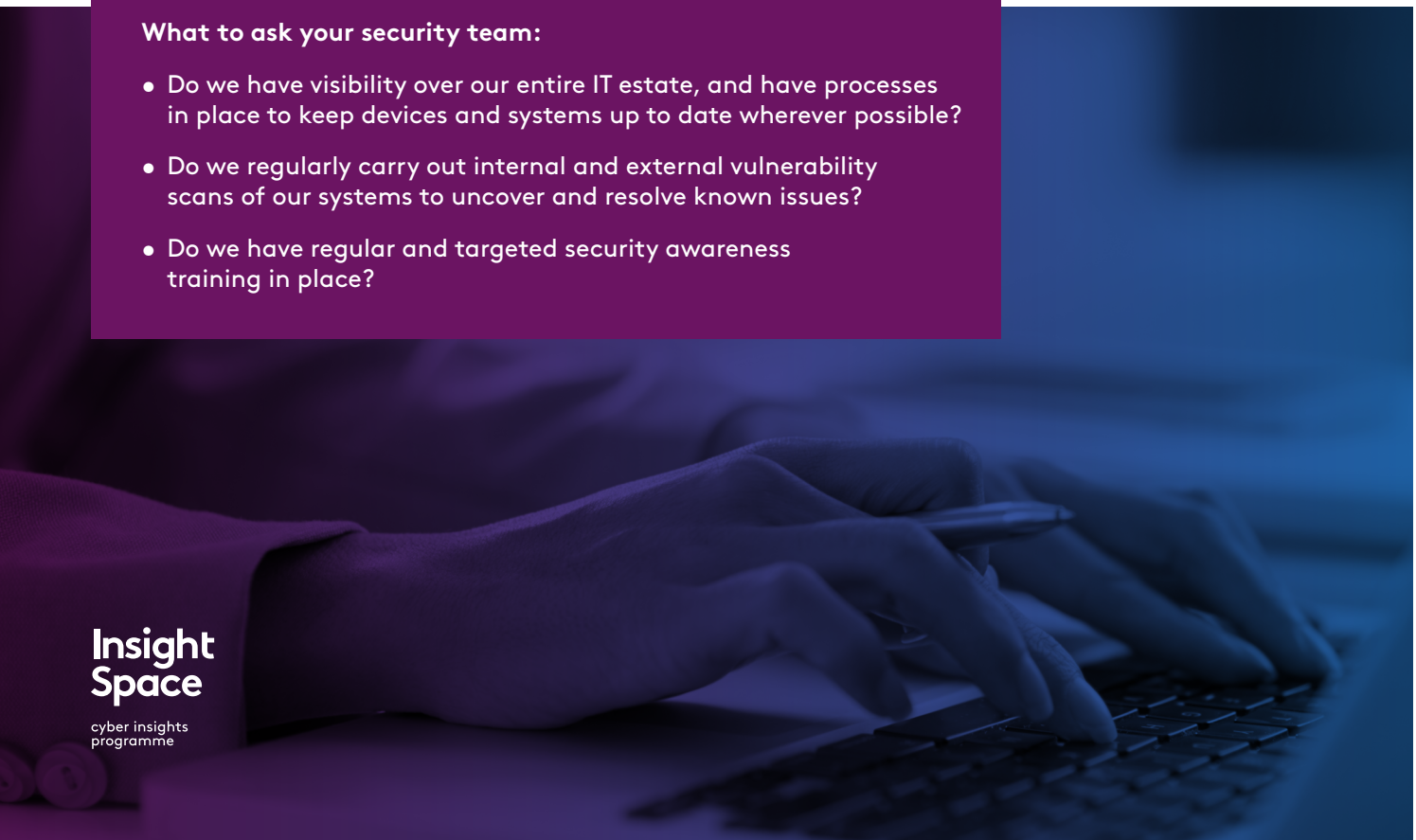
Phishing emails usually seek to get a response, such as opening a document or clicking on a link, although it may be the precursor to a telephone call or vishing from an individual claiming to be from an IT department, a client changing account details or a head hunter wanting to get information on your availability for a new job.

Security awareness training is the only way of preparing staff to manage and resist vishing attempts. It needs to be bite-sized, frequent, targeted to particular internal audiences and focused on the organisation.

The impact of phishing emails can be reduced with technical measures and should be the focus of a regular conversation with your security team to ensure that these measures are cost-effective and up to date.

What to ask your security team:

- Do we have visibility over our entire IT estate, and have processes in place to keep devices and systems up to date wherever possible?
- Do we regularly carry out internal and external vulnerability scans of our systems to uncover and resolve known issues?
- Do we have regular and targeted security awareness training in place?



Through Phase

If the measures to keep the threat actor out of your systems have failed, they will seek to move across the network. This is because the initial point of the compromise is rarely the place with the information or access that they want.

Often, they will seek to use **internal information repositories** ATT&CK T1213, T1039, T1081 to further their attack.

These internal repositories might be something as simple as a list of passwords stored in a Word document on a desktop, password reset processes and systems, or an internal site or HR database. This information could give the attacker essential access to other parts of the network, known as lateral movement, or to higher levels of authorisation, known as privilege escalation.

To defend against the harvesting of such information internally, a regular review of where sensitive information is stored, and who has access to it, should be carried out. The logging of wide-scale internal searches, and alerts for specific keyword searches, such as "password", can also warn that an attack is taking place.

You could also ask about the use of 'canaries', not the birds but a small snippet of code that is disguised as something interesting such as a file, document, photo or even an entire fictional computer that sends an alert when looked at.

The threat actor might be able to **use the access already secured** ATT&CK T1078 to obtain the information they are looking for. One simple measure is to ensure that staff with high privileges use separate accounts, or even separate machines, to do technical administration and not the same one they use for email and surfing the internet. This restricts access and reduces vulnerability.

The threat actor will probably want to ensure that, having gained access to the system on one machine, they can continue to do so even if it is turned off or rebooted. This may require them to **maintain access through movement** ATT&CK T1075, T1076, T1028 which essentially involves moving to a better place on the network.

In many modern systems the servers are not regularly turned off so the attacker may look to sit there as it gives them access to different users and often a path out to the internet.

The separation of internal networks with additional control, limiting access to the internet, and ensuring that endpoint detection and response software is installed on servers as well as laptops or computers used by staff (endpoints, in IT terms), will all help limit the criminals' activity.

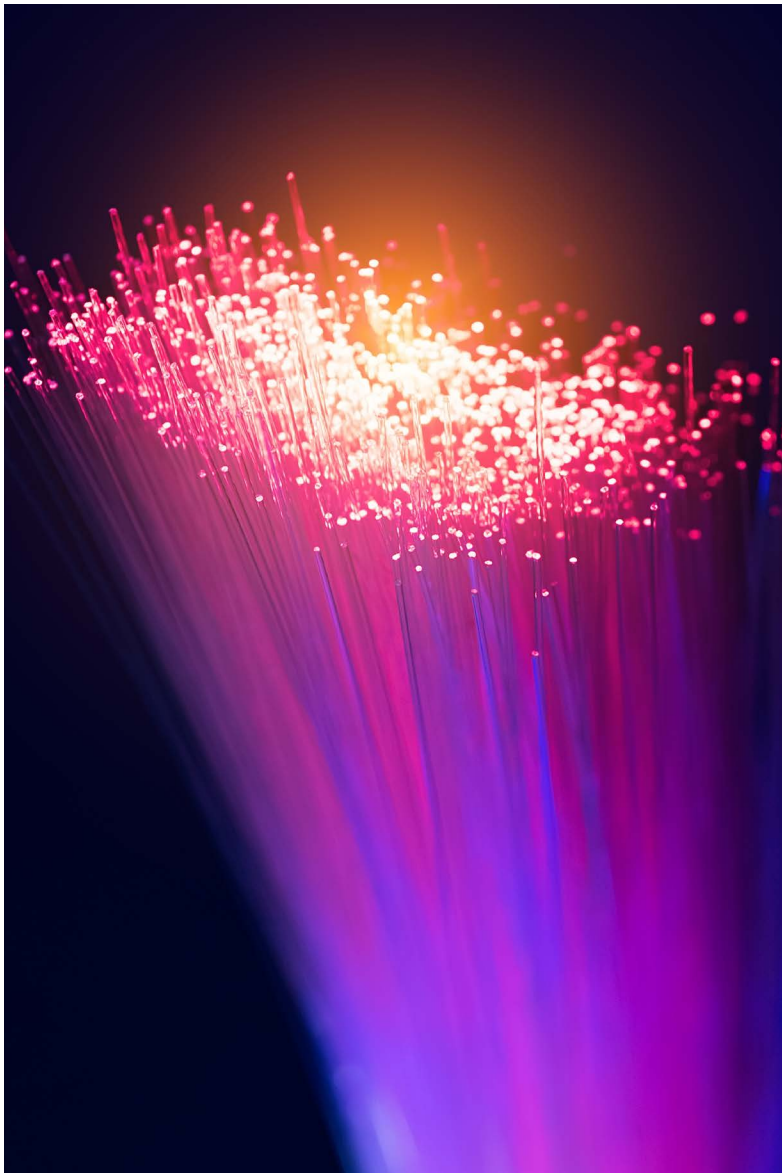
Regularly targeted servers or systems often control identity and access management, such as the Windows Active Directory. So, an attempt to **exploit centralized identity and access management** ATT&CK T1078 is common among criminals and hostile states.

Unfortunately, these are often seen as internal systems and are usually not as well protected as they should be. However, when they are compromised, they regularly provide high level or privileged access to critical systems. Although the resetting of passwords is a frequent occurrence in many organisations, a good process, such as having a manager approve it or requiring a telephone call to the member of staff requesting it, can be an additional hurdle that an attacker may find difficult to overcome.

Having gained access and the ability to move across the network the attacker will begin to look to move to the phase where they can see their objective – known as the Out Phase.

What to ask your security team:

- Do we know where sensitive information is stored, and who has access to this? If not, can we regulate this?
- Can we put stronger password reset processes in place?



Insight Space

cyber insights programme

Out Phase

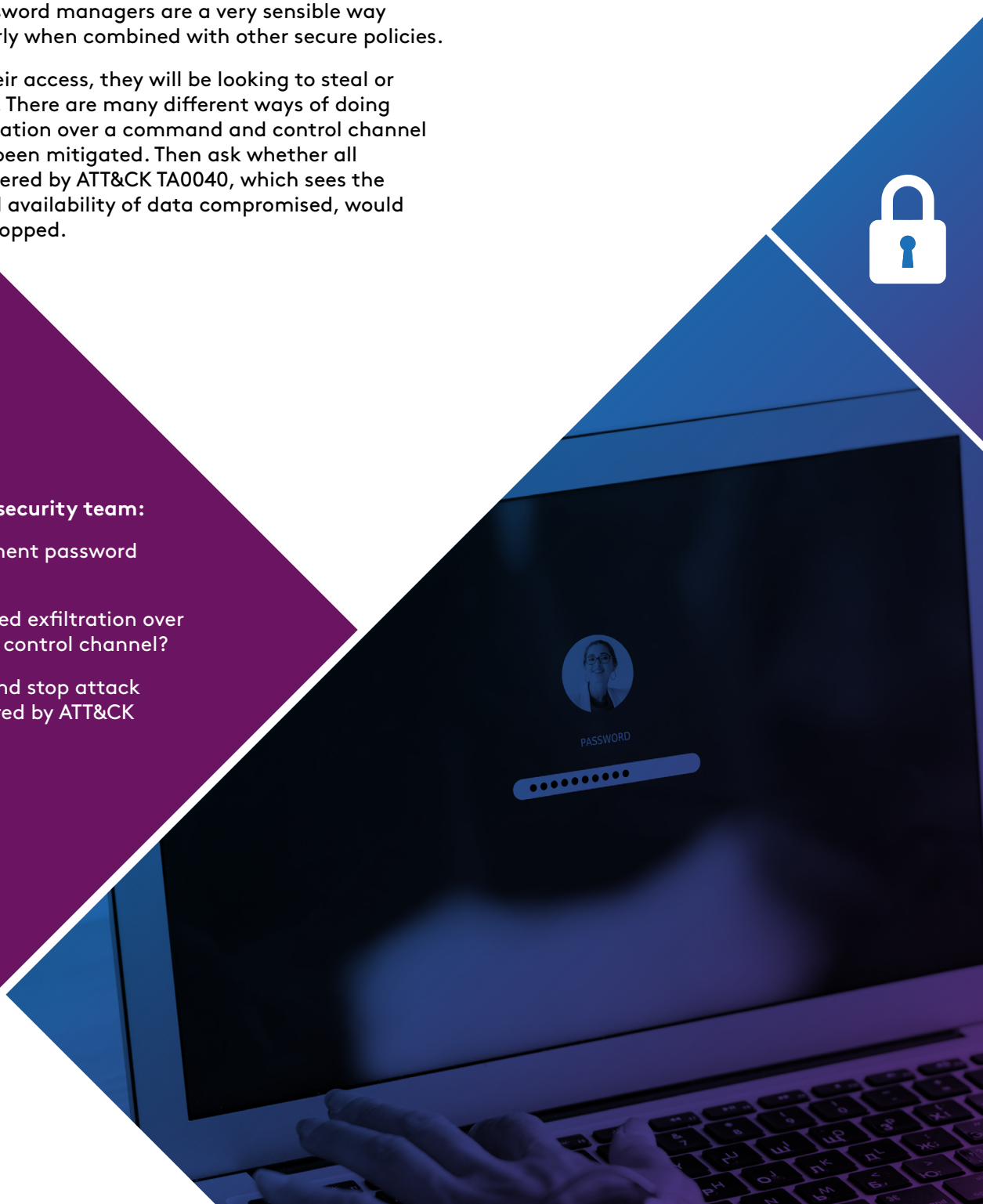
The attacker will need to be confident of **securing the required access** ATT&CK T1078, which will probably involve using the right password.

Our Red Team frequently see passwords based on a single word with a number and changed regularly with a predictable pattern. January2020, February2020, March2020 is very likely to be followed by April2020 if the system requires a new password every 30 days. Password managers are a very sensible way forward, particularly when combined with other secure policies.

Having secured their access, they will be looking to steal or exfiltrate the data. There are many different ways of doing this so ask if exfiltration over a command and control channel ATT&CK T1041 has been mitigated. Then ask whether all the techniques covered by ATT&CK TA0040, which sees the confidentiality and availability of data compromised, would be detected and stopped.

What to ask your security team:

- Could we implement password managers?
- Have we mitigated exfiltration over a command and control channel?
- Can we detect and stop attack techniques covered by ATT&CK TA0040?



Insight Space

cyber insights programme

Conclusion

Securing your data from all the different methods and techniques the opposition use is undoubtedly difficult.

However, if you can challenge your security team to use the Mitre ATT&CK framework to identify the way that they operate, you stand a better chance than many.

Red Team attacks are a great way of checking that these mitigations are in place, but if you are starting out and want to give your security team a bit less of a challenge you might look at Purple Teaming. This is where our Red Team sit with your security, known as the Blue Team.

The two teams then work together to test the methods and techniques described above to test the security of your organisation and make your Blue Team even stronger.

Whatever you do, make the opposition work harder by ensuring the Blue Team:

- Know their threat model and the external information available to an attacker
- Know their external attack surface and actively manage and monitor it
- Know what is in their estate, manage it, have effectively segregated it by its function, criticality status and business owner and are able to monitor it in near-real-time
- Have the right visibility and controls across their estate with an understanding of what is normal
- Have an ability to detect, contain and respond to the anomalous
- Have strong identity and access management system, and have provided staff with tooling to complement it and manage their own passwords effectively, including mandatory multi-factor authentication
- Ensure information repositories and internal file stores have appropriate access controls and do not contain credentials

To make your organisation more resilient, challenge your security team today and start more regular conversations with them. And remember, you can call your NCC Group Senior Adviser to support and guide you as you make your organisation more secure.

Insight Space

cyber insights programme

Insight Space

cyber insights programme

nccgroup

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.

www.nccgroup.com