CYBER DEFENCE 2017: DETER, DETECT & DEFEND

Denis Onuoha

Arqiva LTD, United Kingdom

ABSTRACT

This paper will detail the working methodology of the attackers and define a sample strategy that can be used to deter, detect and successfully defend against this kind of attack.

The concept of the cyber kill chain will be discussed and mapped to the relevant stages of the broadcast chain. Any device that has an IP management interface is susceptible to command and control by an unauthorised user.

Following the recent hacks of US radio stations in the Republican heartland that successfully aired a song against Donald Trump, the hacking of Channel 2 in Israel for politically motivated reasons, the TV5 attack; broadcasters need to pay more attention to the cyber security of the broadcast network.

Attacks come from far and wide, however when the methodology used in attacks is analysed, it is very similar to that used in other industries from which we can learn lesson to prevent any negative impact on our operations.

INTRODUCTION

Organisations operate in a complex environment with adversaries coming from far and wide all over the internet. Previously the attack surface was much smaller, it was limited to physical security and systems operated using one way traffic. In this modern day and age, the threats posed include those from Criminal Gangs, Nation States, and Hacktivists amongst others.

One only needs to look back to the Mirai botnet and Wannacry worm to see the impact these have had on a global scale. These attacks are known as Computer Network Attacks (CNA), with the aim of taking the systems offline and potentially making the system inoperable.

Attackers used a well-planned attack method called the Cyber Kill Chain. This model is based on the military attack structure. In order to defend against this type of attack, the kill chain must be disrupted at several stages.

To disrupt this attack path, the defenders need to assume the mind-set of an attacker. With the broadcast landscape now embracing IP Networks, Personalisation, Cloud

Virtualisation and embracing more disruptive technology, this makes it an attractive target for an attacker.

The recent attacks in the industry have resulted in services going off-air, stolen intellectual property and accessed confidential information. They have also been attacks on the integrity of the chain as attackers have replaced legitimate streams with streams of their choice.

CYBER KILL CHAIN

Figure one below depicts the cyber kill chain. There are seven stages in this chain and these are followed systematically in most disruptive attacks. These stages are described below:

Reconnaissance: This is the stage at which the attackers research their targets and select the target. It is here that social media profiles of the employees are reviewed, browsing behavior pattern, discovery of systems that are exposed on the internet, 3rd party links, email addresses are harvested, amongst other relevant information. The adversary gathers as much information as possible so as to increase the success rate of the entire attack. It can take a few hours to months for this information to be gathered, this timeframe is determined by the cyber maturity of the target. During the Wannacry Ransomware investigations it was discovered that the attackers scanned the internet for computers that had the SMB port open over the internet a few weeks before the attack actually took place.

Weaponisation: This phase commences after the attacker has completed the reconnaissance and is ready to proceed. During the reconnaissance the attacker may have seen that the target is operating a legacy operating system which is not protected, or may have guessed with a high probability of accuracy due to seeing a current staff member's resume online. With this information a known exploit is then weaponised and made ready to be sent via the relevant means such as email, direct remote connection or another weakness such as website injection. A recent example of this can be seen from the Wannacry malware which weaponised the worm to be transmitted via a weakness that existed in the Microsoft operating system family. The time taken for this process to occur can range again from a few hours to months as it is dependent on the cyber security maturity of the target.

Delivery: Once the exploit has been weaponised it is then sent to the target via the relevant attack vector. The majority of the breaches which have been invested recently point to an email being received with a malicious link or file in it being the cause. It is very important to note that this is not the only delivery mechanism; these exploits can also be delivered to the system directly via the internet without the target having to do anything to receive it. Such was the case in Wannacry and also in the Mirai Virus. This process takes seconds to execute. However, the more mature the target is, the less likely it is that this delivery will be successful.

Exploitation: The execution of the exploit occurs at this stage. This enables the adversary to compromise the system and gain a foothold to progress the attack. Not all attacks make use of exploits as some attacks can actually crack a password and get access or even worse - socially engineer the users. It also takes seconds to execute this phase.

Installation: Once entry is achieved the next goal of the attacker is to attain persistence on the system. Access should still be available post reboot of the machine and the attacker should be able to come and go as they wish. They may also move across the network to discover which system is best for them to gain persistence on. The installation is a rapid one time activity. Modern attackers build modular software that they can upgrade remotely should they wish to have newer functionality.

Command & Control: Once installation is complete the attacker will now have command and control of the target's system. This can be an encoder or mux. An example of this kind of command and control will have been seen when the explicit radio broadcast was carried out in the US or the insertion of a different stream in the attack on a channel in Israel.

Action on Objective: The last stage of the kill chain involves the attacker carrying out the final objective. This objective may be data theft in a Computer Network Exploitation Attack (CNE), modifying the data being transmitted, or taking the system offline. Examples of all three attacks types have been seen in the recent months and are occurring regularly.

The seven steps above are heavily geared towards cyber perimeter security, however our world now have a wide perimeter. Services that are based in the cloud are beyond our perimeter so are home uses and freelancers. The key point here is to focus on the "**action on objective**" phase of the attack when planning defence and working back down the chain.

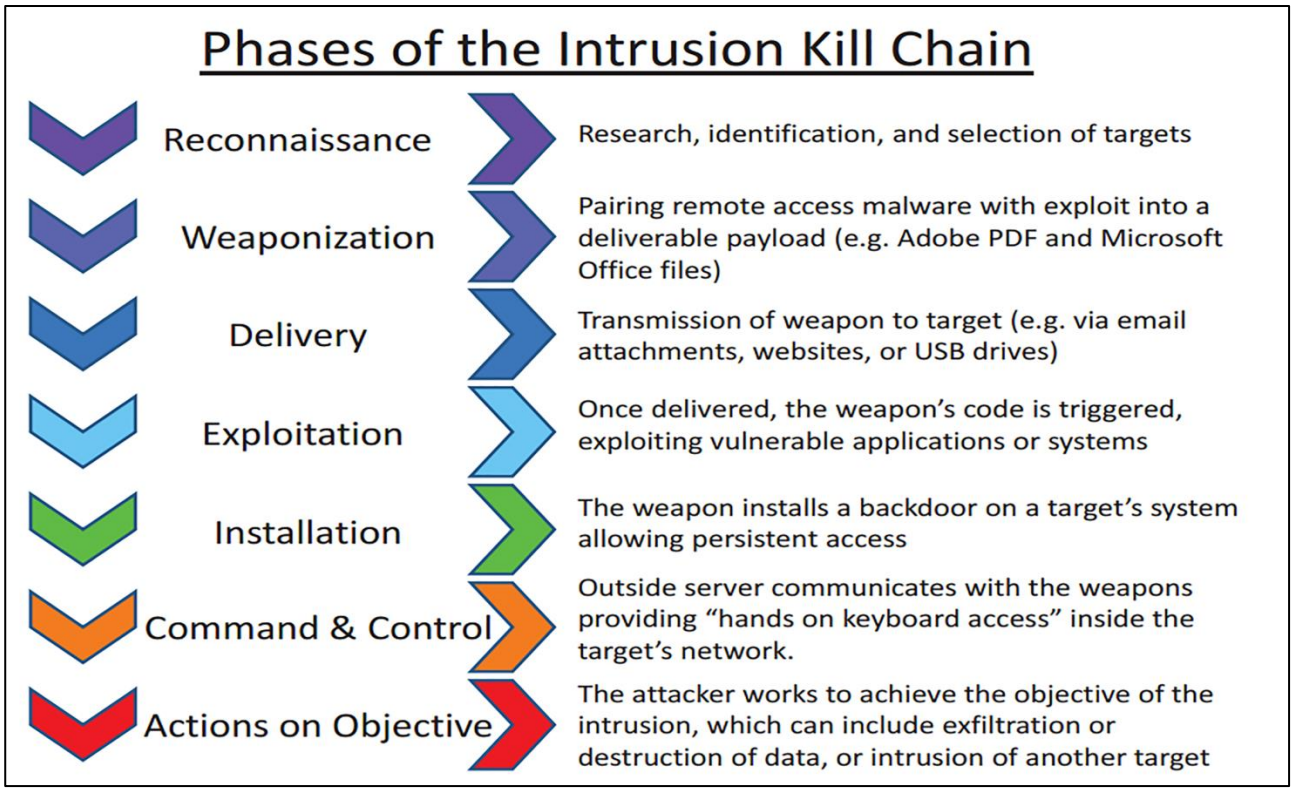

Figure 1 - Phases of the Intrusion Cyber Kill Chain

DETER, DETECT & DEFEND

Now that we know how attackers operate, we can look at a successful 'quick-win' strategy for protecting our services from the majority of the cyber-attacks that we will face. By following basic cyber hygiene practices, it is possible to successfully prevent the majority of the threats that are encountered from having an effect on our operations.

The majority of the equipment that is being operated in the broadcast industry does not support traditional security controls, however it is imperative that at the very least, the networks should be separate (Management, Production (Operational) and Corporate).

Where possible, there should also be a “Jump Box” that can provide enhanced network access control. A high level architecture diagram can be seen in Figure 2 below. This figure shows a satellite transmission management control network being protected via a Virtual Desktop Infrastructure system.

Most companies have already been breached but they do not know it yet and as such it is important to implement a secure architecture as soon as practically possible before embarking on the bigger cyber security picture which will be covered below.

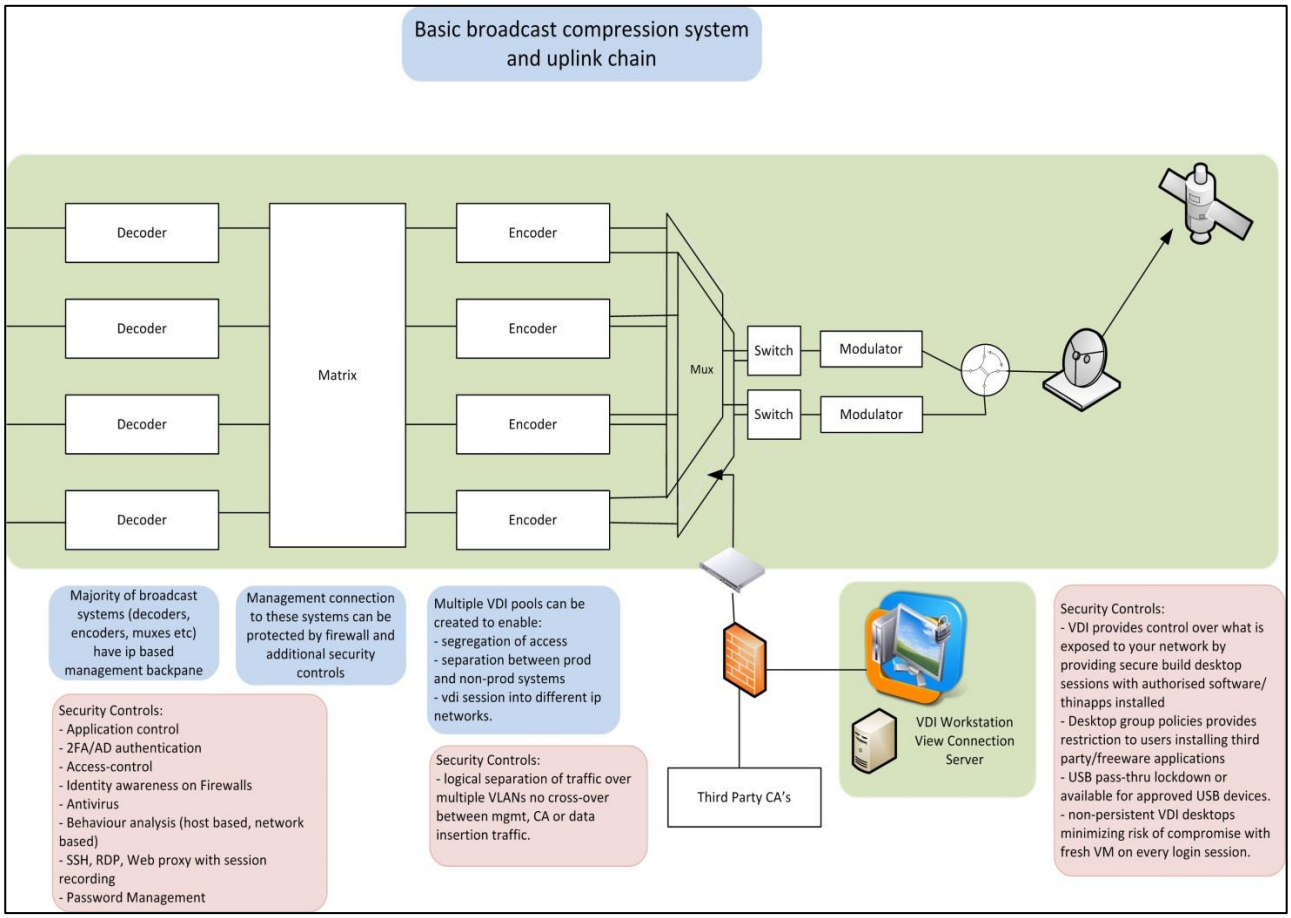

Figure 2 - Broadcast Secure Management Architecture

Deter

Deterrence is generally the best form of defence in the cyber world. As can be seen from the kill chain methodology, attackers look for several nuggets of information in order to successfully breach a company. Generally, most cyber criminals attempt to attack targets for which they have the most information. The harder it is for an attacker, the more chances are that they will move on to the next easier target. This also depends on the motivation, Nation States attackers have been known to be very motivated and get into systems regardless of the obstacles, including combining a physical and cyber-attack.

Employee awareness is one of the first steps to deterring an attack; employees should be educated on what is appropriate to put on social media with regards to their work, even on professional sites such as LinkedIn. An attacker will search for the company name on those sites and then harvest details such as email address (if available), connections at work, skills (to enable guessing of what equipment is used) or even the employee's physical location. Security by obscurity does not work, however a bit of difficulty will deter the average attacker.

The company's digital footprint must also be understood. There are search engines online such as "Shodan" which scan the internet for devices and display details including the companies that these are registered to. Unused IP ports and risky ports should be blocked on the firewall. Figure 3 below shows a simple search on Shodan from Microsoft IIS server. This search can be modified to show systems of interest e.g. Encoders or Multiplexers. This information has just brought an attacker one step closer to the attack. Organisations need to follow the same steps as the attacker and use the search engine to look for themselves.

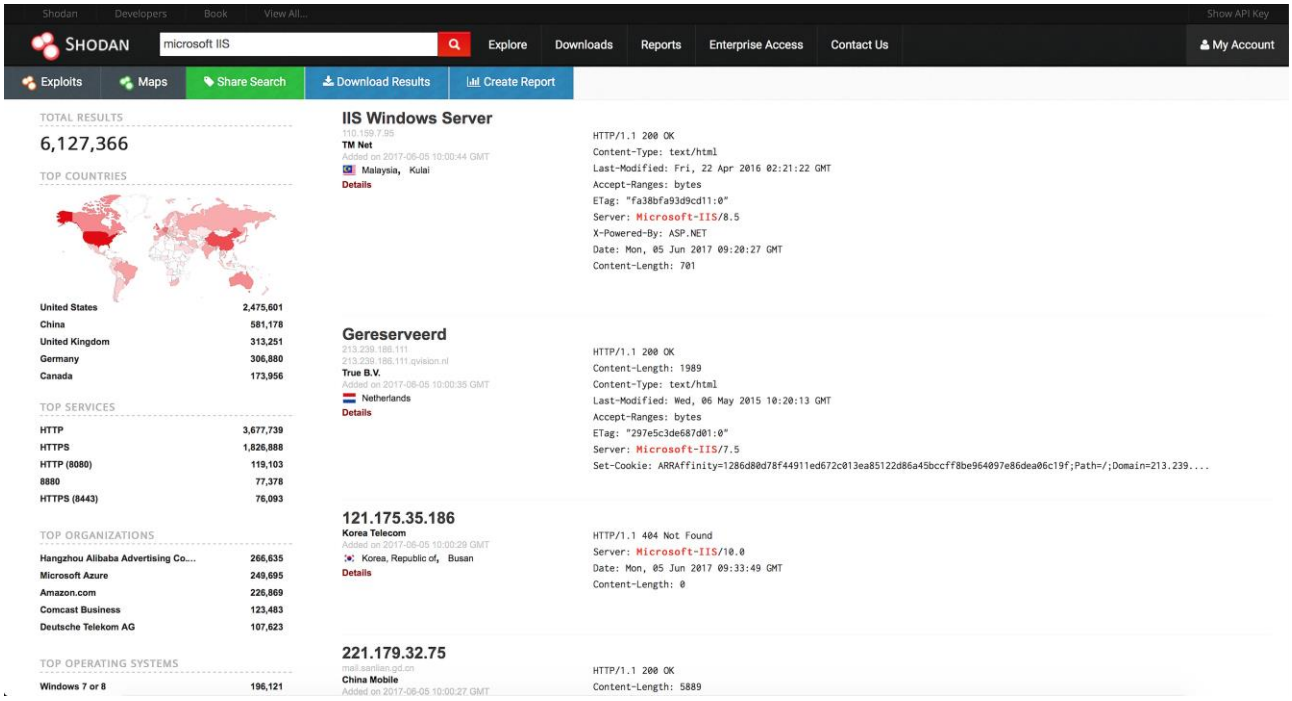

Figure 3 - Shodan Search

Systems should be patched regularly, in order for known exploits to be fixed. This will ensure that the attacker will have to go the extra mile to successfully exploit the system. An example of it being easy for an attacker is the Wannacry attack which infected over 270,000 computers on the internet. All the attacker had to do was scan using Shodan for open ports, modify the exploit that was published online and push this exploit to the list of discovered IP address. If the systems had been patched it would have made it much harder for the attacker to infect such a large number of systems. Where patching is not supported and to resolve Zero Day flaws, Intrusion Prevention Systems (IPS) should be used. These can either be an agent installed on the server or a network based appliance. IPS vendors typically release the signature for the exploit a couple of hours after the exploit is disclosed or even sooner if they discovered it. In a complicated broadcast landscape where traditional tools are not supported this will be a good method for interim patching until end-to-end testing can be completed of the vendor patch in a test environment.

Systems should be configured in the most secure way for their use. For example if “Wireshark” is not required for the production system then it should not be installed as part of the operating system. In the event of a fault condition there can be a dedicated packet capture device that can be used for diagnosis. This may sound trivial, however if there is a vulnerability then the attacker can exploit this. If this is installed on the production system then it is one more vulnerable application to patch. Weak SNMP community strings should also not be used on the system. For example the default string of “Public” and “Private”. Attackers will first try to guess this as part of the task for achieving their desired objectives. Default usernames and password should also be changed. These are easily available online and will give the attacker remote control of the device. They should also not be the same for every device. The mind-set behind this line of thought is that one of the attackers may think if the key (password) is the same then I can open all doors (access systems) very quickly, if it is not then I cannot achieve my objective in the allotted time. The systems should also support strong authentication mechanisms. Sensitive configuration information necessary for the operation of the system should be encrypted to prevent an attacker from eavesdropping and gathering vital information to use in the attack.

Penetration tests should be carried out regularly to discover additional vulnerabilities on the system that needs to be protected. In addition to these tests when deploying equipment the Secure System Life Cycle should be adhered to. This will ensure security is built in by design and not as an afterthought.

Access control needs to be in place to act as a further deterrent. Two-Factor access control using a token (something you have) and a password (something you know) will deter the attacker even further and reduces the risk of an employee being socially engineered being the root cause of a successful cyber-attack. This will be another obstacle for the adversary as they will not only need the password but they will also need to get access to the token. This authentication mechanism should also be unique to each user and logged. Shared accounts become troublesome when investigating breaches, especially if it has been caused by an insider.

Network segregation which was briefly discussed above is one of the best ways of deterring and limiting the impact of a cyber-attack. Figure 4 below shows a detailed network access segregation system. As can be seen from the diagram, this is a choke

point on the management network and ensures that if the corporate network is compromised then that will not move the production network. This is a good starting point before maturing further and beginning to deploy segregation on the production network. In the case of the attack on TV5, public sources mention that the attackers got in via a third party supplier network. It is important that all remote access is strictly monitored and controlled.

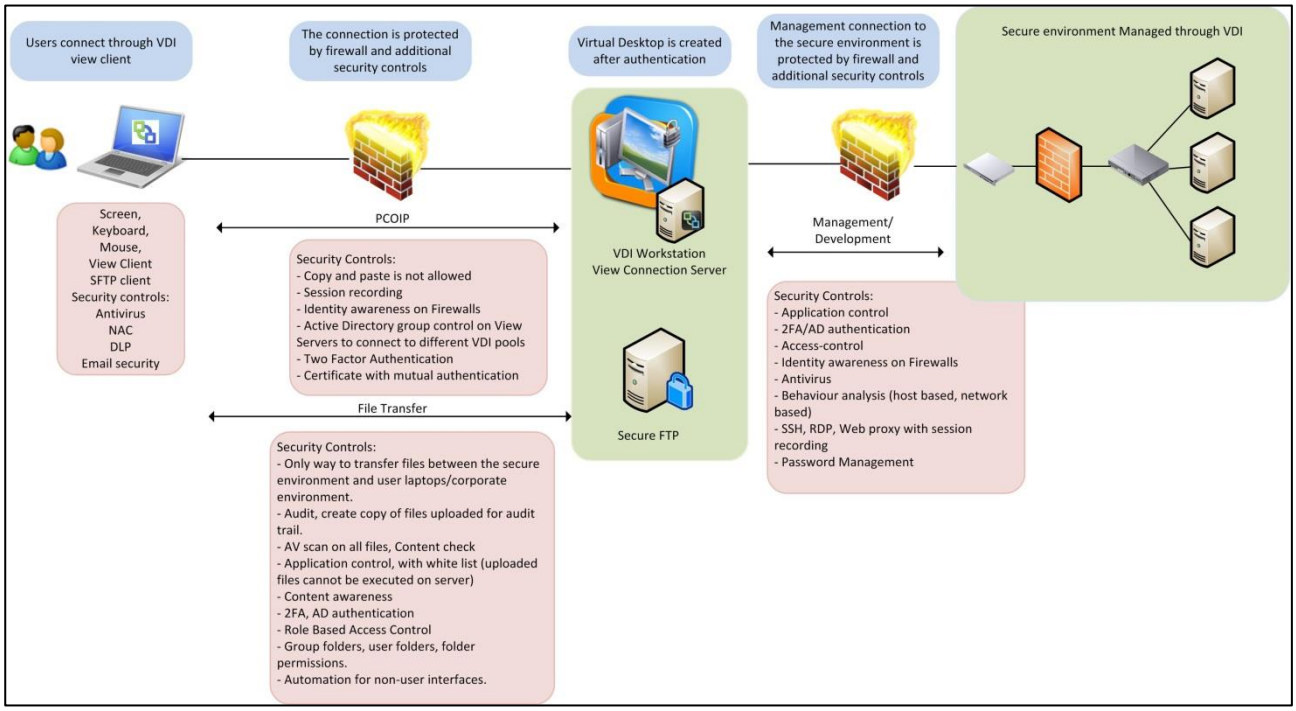

Figure 4 - VDI Secure Management Architecture

Detect

The controls in the Deter phase above not only frustrate the attacker, but they also cause the attacker to make more noise and increases the likelihood of defenders proactively detecting an attempted attack.

A 24/7 Security Information and Event monitoring (SIEM) is required on any network/system today. This can either be in-house or outsourced to a competent provider. Once the detection system is in place, it is important to review the logs and look for abnormal behavior on the system. Failed login attempts may mean that someone is trying to break into the system. A server/system beginning to communicate with another system that it does not normally communicate with may mean that an attacker is trying to carry out a lateral movement across the environment.

Experienced security professionals need to constantly monitor these feeds and others to be able give the organisation a fighting chance at defending against this attack. Early detection may mean there is much less of an adverse impact than intended. Protective and proactive monitoring can spot that an attacker has emailed a group of baseband engineers a booby trapped email. Once this is spotted by protective monitoring, the engineers can then be alerted and can operate at an increased vigilance level.

Intrusion Detection Systems (IDS) also need to be deployed to further increase the quality of the information about the network. These can either be behavioral based and/or signature-based (knowledge of attacks). IDS typically come as part of the IPS systems (used in deter). Attackers often change their tactics, the richer the information source the easier it becomes for the defended to protect the network/system.

Honeypots can also be used for detecting attacks. These are systems that are configured as decoys and are constantly monitored. Once an attacker attempts to attack it the defence team can monitor what tactics are being used and apply protection for this on the production network. Honeypots are currently being deployed with decoys. Decoys will simulate the environment and the attacker will actually think that their attack is being carried out; again this buys the defending organisation more time to bolster their security as they will see they are being targeted.

User awareness also falls into the detect/deter category. Users must be aware of what seems like suspicious activity and report it to the relevant support team. For example a slower than normal network may indicate data is being siphoned out of the organisation or it may be a Denial of Service Attack. High Process / Memory utilisation may be a sign of malware operating on the system. With the current cyber security landscape one must not default to reboot without finding out the root cause unless absolutely critical.

Attackers are often on the network for a significant amount of time (months), and in this time they will most likely make a mistake and can be spotted.

Defend

The first part of any successful cyber-attack is having a cyber incident response plan; the National Institute of Standards and Technology have produced a guide to cyber incident response (NIST 800-61). This provides a good level of details on the requirements to have a successful cyber incident response plan in place.

Network IPS also helps to defend against a cyber attacker as it can be used to block the attacker, the defence mechanism used will depend on the type of attack that is being attempted.

Cloud service providers can also be important in the defence strategy as one of the benefits of cloud offerings is the ability to grow elastically. In the case of a cloud based instance being under a DDOS attack for e.g. Streaming Media Server, this can spawn into other instances thus being able to cope with the traffic while the defence teams are working with the Internet Service Provider to sink hole the traffic.

It is important to carry out “Red Team” exercises so that the defenders are used to managing a cyber-attack and know what to do when they are under pressure. A Red Team exercise is when a group from an opposing team tries to attack the infrastructure. This can either be an in house team or a specialist competent red team provider.

Having Business Continuity and Disaster Recovery process in place as part of the defence strategy will help if the objective of an attacker is to take the system off air, since the ability for the defender to switch to a DR system will ensure that this objective is not achieved. During the recovery from a Computer Network Attack such as Wannacry, the organisation

will be able to rebuild from a last known good image. Any backup arrangements must be tested regularly to ensure they are working effectively.

Conclusion

This paper has provided a high level overview of what needs to be done to deter, detect and defend against a cyber-attack. This is a good starting point, however there is a lot more that can be done to further reduce the risk of a successful attack. All the principles listed here apply to third parties such as outsources and cloud service providers. It is imperative to ensure that one is following industry best practices and there is a robust level of auditing in place to ensure security is not an afterthought. It is not a question of “IF” but “WHEN” it will happen, will you be prepared?

In the current time of fake news it is imperative that we secure ourselves, in order to prevent rouge individuals taking controls of our systems and using them to make fake news seem legitimate.

The European Broadcast Union, North American Broadcasters Union and the Digital Production Partnership have produced technical standards are guidelines that provide more details on steps that can be taken to secure the broadcast environment.