5 CYBER THREATS

In this chapter, we shall examine the various types of threat that individuals and organisations face, including types of attacker, types of attack, the motivations for and the benefits of launching an attack, the risks involved in doing so and how attacks typically are conducted.

There are a number of terms associated with cyber threats that are worth exploring before we look into the types of threat in greater detail:

- **Threat source or sponsor** is the person or organisation that wishes to benefit from attacking an information asset. Threat sources often pay or otherwise pressurise threat actors to attack information assets on their behalf.
- **Threat actors or agents** are the individuals or groups of individuals who actually execute a cyber-attack.
- **Threat actions** describe the actual attacks. These are often not a single isolated event, but can consist of many discrete activities, involving surveillance, initial activities, testing and the final attacks.
- **Threat analysis** describes the process of understanding the level of threat – this is referred to in more detail in Chapter 6.
- **Threat vectors or attack vectors** are the tools, techniques and mechanisms by which an attacker conducts the attack on their target.
- **Threat consequences or impacts** are the results or impacts of a cyber-attack, which we dealt with in Chapter 4.

While some attacks are more likely to take place than others, the level of impacts does not necessarily mirror the type of organisation affected or the likelihood that they will occur. Any individual or organisation can be attacked, and many very probably have been.

Before we can begin to plan to put preventative measures in place or to develop the means to respond to cyber-attacks, we need to understand the kinds of people and organisations that will attempt them, together with their possible motivations for doing so. Once we have a clear understanding of this aspect of cyber security, we will be much better placed to deal with them.

Any attacker or criminal requires three distinct things in order to achieve their goal:

- Motive – there must be a reason for them undertaking a cyber-attack – even if it appears to be a rather futile one. Most cybercrime is motivated by money, but there are elements who attack systems for revenge; to establish their perceived superiority; to make a political statement; or simply to be a nuisance.

- Means – the attacker must possess a minimum level of skill in order to mount a successful attack. Often attackers with little or no skill will fail in their endeavours and will probably be identified and face justice, while those with sufficient motivation will persist, and further develop their skills over time.
- Method – a more experienced attacker will develop a plan for their attack. This may require an interim break-in, followed by extended periods of reconnaissance before the real attack takes place.

Some of these attackers will be individuals, operating entirely on their own; some will be groups of individuals, often organised into a loose community (such as the Anonymous group); while others will be highly organised criminal gangs. At the other end of the spectrum are the nation states, and while some will be using the attack for purely espionage purposes, others will have a far more sinister agenda.

TYPES OF ATTACKER

Attackers fall into a number of categories:

- script kiddies;
- hacktivists;
- lone wolves;
- investigative journalists;
- minor criminals;
- organised criminals;
- terrorists;
- insiders;
- security agencies.

Before we examine their motives, means and methods, it is worth examining attackers' capabilities, as these will vary considerably.

External attackers

We shall begin with those attacker types who conduct cyber-attacks from outside conventional organisations.

Script kiddies

Script kiddies are beginners in the cyber security game. They need not be young but are generally relatively inexperienced in computing and cyber security matters and are on a learning curve. Their attacks will typically involve downloading free malware from internet resources and attacking 'soft' targets where there is less chance of causing damage, leading to their being caught. More experienced hackers tend to look down on script kiddies, despite that fact that this is where many of them may have started.

Hacktivists

Most hacktivists already have a cause to support. Some of these will be political; some religious; some may be concerned with the protection of civil liberties; some will be attacking a major corporation whom they feel has caused them some injustice; some will be trying to save the planet from destruction by humanity.

Whatever their cause, hacktivists will invariably target major websites, often defacing the organisation's landing page, or replacing them with their own versions of what they perceive to be the 'truth'.

Since hacktivists rarely attack individuals, and are not usually motivated by theft, they present relatively little threat to us as individuals, unless, for example, we work in a laboratory that conducts experiments on live animals, or in some other similarly controversial area. To organisations, however, they are a major nuisance, causing public embarrassment and occasionally causing the targeted organisation some financial loss, both of which are usually very much the hacktivists' primary objectives.

Hacktivists normally take advantage of known vulnerabilities in website applications to conduct their attacks. Once identified, these are relatively easily corrected, but in the meantime, if they have enjoyed sufficient exposure, the hacktivists feel that their point will have been made.

A small minority of hacktivists are just out to cause mischief and are usually less concerned about making a particular point; rather they have identified and exploited a vulnerability, and deface a website just to show their prowess.

However, some hacktivist attacks have had a much higher profile, as in the example of the Anonymous attack on the Church of Scientology following its legal action against YouTube for publishing one of its propaganda videos.[1]

Lone wolves

Lone wolves are frequently newcomers to hacking. Although not restricted to the Hollywood vision of a brilliant teenager hunched over a computer in a darkened bedroom, they often begin as 'script kiddies', who learn their basic hacking skills from chatrooms and blogs on the internet, download malware and try their hand at attacking increasingly high-profile websites.

Their motivation is usually to gain kudos from their peers but may also be to cause a certain amount of mischief, and this type of lone wolf sometimes graduates from minor hacking into minor crime or hacktivism.

Another, more benign type of lone wolf is motivated purely by inquisitiveness, and is more reminiscent of the original hacking community, who simply wanted to find out how things worked, and if possible, to improve them. This type of hacker will often graduate to become a security specialist or penetration tester.

Investigative journalists

Investigative journalists are an interesting group. While their intentions may be honourable, they frequently resort to underhand methods to achieve their goals. Some

[1] See https://abcnews.go.com/Technology/GadgetGuide/story?id=4194143

such activity has been hacking into the voice mailboxes of celebrities, politicians and members of the UK royal family – deemed 'illegal interception' – and attributed largely to journalists working for the News International group of papers during the mid-2000s.

It is not hard to imagine that a journalist willing to illegally access someone's voicemail would also be prepared to illegally access someone's computing device, email messages or internet browsing records, whether they achieved this themselves or by some form of proxy – that is, paying a hacker to undertake the technical aspects.

Minor criminals

I have referred to this group as minor criminals simply because they represent a community who will usually target individuals and smaller businesses, rather than major corporations. Their motivation is generally either financial or information theft.

In the first instance, they will enjoy direct financial gain from someone's bank account or by abuse of their credit card; in the second, they may simply post copies of software, music or films on torrent websites so that others may download them free of charge. Naturally, this causes a financial loss to the copyright owner of the pirated material.

Minor criminals can drift either into major crime, especially if their expertise comes to the attention of the organised criminal fraternity, or can become respectable security specialists. Their choice is sometimes decided by how much money they can make, and whether or not they have been caught.

Organised criminals

We now move up another layer in the hierarchy of cybercrime to that of organised criminals. This group are almost exclusively motivated by financial gain, although instances have been reported in the media where known organised criminal gangs have undertaken cyber-attacks on behalf of terrorist groups or nation states in order to disguise the true identity of the sponsor.

Occasionally, the threat actors (as opposed to the threat sponsors) will be acting in their own interests and will benefit in full from their activities. At other times, they will be acting on behalf of others, who will pay either a fixed fee or a cut of the 'take' for executing the cyber-attack.

Organised criminals will often purchase information such as lists of valid credit card names and numbers for use in mass financial scams or will set the threat actor a specific task to obtain information of value, which can then be sold on to the highest bidder.

Terrorists

Terrorist groups tend to use cyber-attacks for a number of reasons. The first is to make or reinforce a political or religious point – defacement of western websites is quite typical of this variety. The second is the theft of money from organisations in order to further their beliefs and aims. The third, and far more dangerous, is to attack the infrastructure of their political or religious enemies.

Since the first two methods have already been covered, it is worth focusing on the third here.

All nations have some degree of critical infrastructure. As we saw in Chapter 3, the sectors include:

- chemicals;
- civil nuclear;
- communications;
- defence;
- emergency services;
- energy;
- financial services;
- food;
- government;
- health;
- space;
- transport;
- water.

Of these, the communications and energy sectors are prime targets for terrorism, since a successful attack on either of these will cause enormous disruption to an enemy. All other sectors of course will be considered as useful targets, but the impact may not be felt with such immediacy.

There is a crossover here between cyber-attacks by terrorist organisations and those initiated by nation states. The term 'cyber warfare' is frequently used to describe cyber-attacks by one nation state on another, and although there remains no absolute proof of Russia's guilt, it is widely believed that the cyber-attacks on Estonia in 2007 were essentially an act of cyber warfare by Russia.[2]

Internal attackers

Having examined those attacker types that conduct cyber-attacks outside conventional organisations, let's now look at those who do so from within them.

Insiders

Until now, we have examined the threats from individuals and groups who are physically located outside the organisation. However, one of the greatest threats comes from people already within the organisation itself. Many of the cyber incidents they cause are unintentional – often brought about by a lack of understanding of the risks involved when someone clicks on a malware link in an email. Others are more deliberate acts, in which an insider steals money or goods, or copies and subsequently steals corporate information that is of value to a competitor or a criminal organisation, or aims to cause system, information or network damage.

[2] See https://cyberlaw.ccdcoe.org/wiki/Cyber_attacks_against_Estonia_(2007)

In terms of dealing with unintentional insider incidents, this can best be addressed by awareness and training, which we shall explore in much greater detail in Chapter 10.

In the case of deliberate insider activity, the active monitoring of user accounts, internet access and the use of intrusion detection software will identify some of this activity, but organisations can never be certain of completely combating insider cyber security attacks.

An insider who has been well trained and placed specifically within the organisation in order to cause loss or damage will probably be fully aware of the organisation's capabilities in identifying potential attackers and will behave in a way that does not arouse suspicion.

Security agency surveillance

Depending upon the country employing them, security agencies should normally be viewed as 'the good guys', unless of course you are one of 'the bad guys'. There is, however, a very active debate as to whether security agencies are operating completely within the law since they have the ability to intercept our communications at many different points.

It is well known, for example, that GCHQ monitors satellite and fibre optic cable transmissions and that the resulting intelligence is shared with the NSA through their 'special' relationship. It is reasonable to assume that the NSA performs the same kinds of interception, and that they also hand over their results in a 'quid pro quo' arrangement.

However, let's for the moment look on the positive side, and remember that the key role of security agencies is to provide support to the police and the military and to protect the UK from cyber threats, terrorism, serious crime and espionage.

MOTIVES: WHAT DRIVES AN ATTACKER

Different types of attacker will have widely differing motives for conducting cyber-attacks. Although there may be other reasons, the following are the most prevalent.

Financial gain

Many, if not most, cyber-attackers are motivated by the prospect of 'easy' money, which will permit them to enjoy a more lavish lifestyle, or to fund further activities that go against the common good (such as crime and terrorism).

Attacks motivated by financial gain generally break down into three distinct areas:

- ransom;
- theft;
- fraud.

Ransom

Ransomware attacks are very much on the increase. According to a survey from Forbes, the incidence of ransomware increased by 50 per cent from 2020 to 2021.[3] All the attacker has to do is gain access to a victim's computer – usually through some form of email scam in which the user either follows a link to a website containing malware or accidentally executes an application disguised within the email.

As an example, Fusob now accounts for a substantial proportion of the currently active ransomware. Fusob masquerades as a video player of pornographic films, detects whether the PC's language is of eastern European origin, and if not, locks the device. Purporting to originate from an official authority, it then demands a payment of between 100 and 200 US dollars to unlock the device.[4]

Theft

Theft breaks down into two slightly different areas. The first is one in which the target's banking or credit card credentials are stolen – a crime in itself – and the second is one in which these details are used to purchase goods or services, and the rightful owners of the money are parted unwillingly from it. The credentials may also be sold to other criminals as part of a larger undertaking.

Fraud

This is considered to be slightly different from theft, since fraud leads people to part willingly with their money, and usually delivers little or nothing in return. Cyber fraud often offers for sale expensive computer software (for example Adobe Photoshop) at a knockdown price. The software (if actually delivered) may be useless, impossible to register or may contain malware.

Remember the adage – if it sounds too good to be true, it very probably is.

There is also the love scam, in which people receive an email purporting to be from a family member or close friend who has allegedly run out of money, is stuck in another country, requires urgent medical treatment or is experiencing some similar plight, none of which are actually true. They are asked to help by sending funds, which are paid directly to the scammer.

Some years ago, I received such an email purporting to be from a colleague with whom I was working at the European Union Agency for Network and Information Security (ENISA). The sender claimed to be in Wales when I knew for a fact that she had just flown home to Portugal. The best thing to do with such emails is to delete them.

[3] See https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/

[4] See https://www.cyber.nj.gov/threat-center/threat-profiles/ios-malware-variants/fusob

Another example of this is CEO fraud in which someone with financial sign-off rights at the CEO's organisation is tricked into authorising funds to be transferred to the attacker who may use either phishing techniques to gain access to the CEO's email account or may email an employee from an email domain name chosen to resemble the target company's true domain name. This is sometimes referred to as business email compromise or BEC fraud.

Revenge or malicious damage

Some cyber-attacks are carried out in response to an action undertaken or perceived to have been undertaken by the victim. The action itself may have been fully justifiable, but the attacker perceives that they have suffered some injury, deprivation or harm from the action and decides that a cyber reprisal is an appropriate response. The results of revenge or malicious damage attacks can be quite devastating and have almost ruined many careers, since the statements made and accusations levied in the attack may well be believed, whether they are true or false.

Attacks of this type can lead the attacker into difficult waters, especially if libel actions ensue, or if the material they post is deemed defamatory, racist, homophobic or fits into any one of a number of proscribed categories. These attacks tend to be either one individual against another; one individual against an organisation; or a number of individuals against an organisation, as in the case of the Anonymous attacks on PayPal, Visa and Mastercard in 2010 in response to the blocking of payments to WikiLeaks, known as Operation Payback.[5]

Although the cyber-attack was considered to have been a success for the Anonymous collective, it was less so for the attackers themselves, as they were identified, tried and convicted.

Espionage

Espionage has been included in this section because whatever its purpose, in the cyber security context it invariably involves some form of cyber-attack, and regardless of whose side the attackers are on, the 'other' side will see them as hostile. One must assume that the security services are extremely well versed in cyber espionage, and that identifying and tracking down criminals and terrorists is an activity that they undertake just as much as discovering the enemy's intentions and capabilities.

There is also a distinction between corporate or industrial espionage conducted in order to gain a commercial or other advantage over another organisation; legitimate surveillance conducted by the police and security services; and finally, espionage conducted by one nation state against another.

However, espionage is a difficult area for many people, since it cuts across our desire for privacy, and although we are generally confident that the security services have our best interests at heart, we do worry that our privacy is being invaded whether it actually is or not.

[5] See https://www.theguardian.com/media/2010/dec/08/operation-payback-mastercard-website-wikileaks

Cyber espionage generally falls into one of two categories – commercial or military/nation state. In the case of the Lockheed Martin attack mentioned both in Chapter 3 and below, both of these appear to have been the case.

Intellectual property theft

The theft of IP covers many areas including, but not limited to, music, filmography, formulae, industrial processes, software, designs and development. Industrial espionage has been around for decades.

In the 1960s, the then Soviet Union obtained plans for the supersonic Anglo-French Concorde aircraft, and developed their own Tupolev Tu-144, which for many reasons was not an outstanding success.[6] The potential consequences for British Aerospace and Aerospatiale were of an economic nature but did not amount to much of a blow in the long term. However, it was later suggested that the development team knew of the Soviets' intention to steal the designs and allowed them to acquire blueprints with inbuilt design flaws.

In another example, from 2009, in an operation known as Night Dragon purported to originate from China, attackers stole proprietary information from six American and European oil exploration companies, including Exxon Mobil, Royal Dutch Shell and BP. The attackers' targets were computerised topographical maps that located potential oil and gas reserves and resulted in the loss of financing information for a number of oil and gas field bids and operations.

Investigative journalism

Another area that touches a raw nerve is investigative journalism. After the Leveson Inquiry, the press managed to convince the government that there was no need for additional regulation for investigative journalism, and that self-regulation would suffice.[7] This may be true, and as long as an investigation is genuinely 'in the public interest', there would be little or no objection other than from those who are under scrutiny.

However, the press in the UK is notorious for its loose interpretation of its own code of conduct, and frequently crosses the line, becoming invasive and causing great distress to innocent people. Hacking into a celebrity's voicemail may not be a difficult thing to do, but this often results in mere gossip rather than exposing genuine wrongdoing.

It is also worth bearing in mind that some newspapers and television channels prefer to depict fake news (at least on the surface) as true investigative journalism in an attempt – sadly, often successful – to influence public or political opinion.

[6] See www.aviastar.org/air/russia/tu-144.php

[7] Following the News International phone hacking scandal, the Leveson Inquiry recommended an independent body be set up to oversee the press, but this was rejected by the UK government.

It is for the individual to try to separate truth from fiction, frequently relying upon the reputation of the media company concerned and the level of trust they are able to place in it.

Whistleblowing

Until recently, few people would have associated whistleblowing with cyber security; then along came Edward Snowden and everything changed.[8]

In early 2013, Snowden, who had been working as a National Security Agency contractor, revealed to three carefully selected journalists that the NSA had been running mass- surveillance programmes against its own citizens. This included information stored by some of the USA's largest technology companies, and data intercepted from global telephone networks and the internet to compile information on millions of US subjects. Snowden also identified the UK's GCHQ as having collected, stored and analysed vast amounts of personal information from global email messages, telephone calls and other resources. Snowden described this as 'probably the most invasive intercept system in the world'.

Governments on both sides of the Atlantic began hasty (and possibly ill thought-out) changes to legislation to either make some of their activities legal, or conversely to wrap their more nefarious activities in such legal jargon that they appear to be legal, while providing sufficient leeway for 'interpretation'.

Snowden, now resident in Russia, was not alone in blowing the whistle on some of these operations – Bradley (now Chelsea) Manning also felt sufficiently strongly about some of the US activities and gave more than 700,000 classified or sensitive documents to WikiLeaks,[9] which landed Manning in prison. At the time of writing, Julian Assange of WikiLeaks is now in prison awaiting the outcome of an appeal in the UK, potentially pending extradition to the USA.

Whistleblowers must be completely committed to their cause, in the full knowledge that although what they expose may be morally or legally reprehensible, the state will probably find ways to present them as criminals and they will almost certainly be punished for doing what they and many other people believe is morally appropriate.

MEANS

Now we should understand how a hacker may go about attacking an individual or an organisation. A quick search on the internet for the term 'hacking tools' returned more than seven million results, so it should be no surprise that somewhere in there should be a software tool that will achieve almost any objective.

[8] See https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

[9] See https://www.justiceinitiative.org/litigation/united-states-v-private-first-class-chelsea-manning

Many of these tools are freely downloadable, while others may demand some form of payment – either as a one-off fee or on a subscription basis. Hackers, and especially those who possess good coding skills, are becoming increasingly commercially aware.

The low cost and high availability of hacking tools is just one side of the coin – the other is that the tools are becoming much simpler to use, so it is easy to see that almost anyone who has more than a little motivation can mount a cyber-attack, often with little concept of the damage they might cause (as in the case of script kiddies) or the depth of trouble they might eventually find themselves in. More experienced attackers will fully understand both the tools and the possible consequences and will plan their activities accordingly.

As an example, this is just a small selection of the commonly used tools for penetration testing and for hacking:

- Kali Linux,[10] as the name suggests, is a specialised Linux distribution that can be downloaded for most computing platforms. It contains over 600 penetration testing tools that, among other things, are capable of cracking Wi-Fi passwords, creating fake networks and testing for vulnerabilities.
- John the Ripper[11] is a password cracking tool that uses a brute force attack method together with dictionaries of commonly used words. As with all such password cracking tools, the complexity of the password (mix of character types and length of password) will determine how long this takes.
- Nmap[12] is a network scanning tool that allows the user to understand what host systems are available on the network, what services (application names and versions) those hosts are offering, what operating systems (and OS versions) they are running, and what type of packet filters/firewalls are in use.
- Aircrack-NG[13] is a wireless network tool that includes the capability for capturing packets and exporting data to text files for further processing by third-party tools; replay attacks, de-authentication and fake access points; checking Wi-Fi cards and driver capabilities; and cracking Wired Equivalent Privacy (WEP) and Wireless Protected Access Pre-Shared Key (WPA-PSK) (WPA 1, 2 and 3) passwords.
- Wireshark[14] is a network protocol analysis tool for both Unix and Windows networks. It is able to capture live packet data from a network interface; open files containing captured packet data; import packets from text files containing dumps of packet data; display packets with very detailed protocol information; save captured packet data; export packets in a number of capture file formats; and many more features.
- Nessus[15] is a vulnerability scanning tool that can assess systems, networks and applications for weaknesses; detect malware as well as potentially unwanted and unmanaged software; audit system configurations and content against standards;

[10] See https://www.kali.org/

[11] See www.openwall.com/john/

[12] See https://nmap.org/

[13] See www.aircrack-ng.org

[14] See https://www.wireshark.org/

[15] See www.tenable.com/products/nessus-vulnerability-scanner

ensure that IT assets are compliant with policy and standards; and identify private information on systems or in documents. Nessus is available in both free and paid-for versions – updates to the free version are generally around six months behind the paid-for version.

- Angry IP Scanner[16] is a network discovery tool that 'pings' each IP address on the network to check whether it responds. It can then resolve the hostname, determine the MAC address, and scan its ports. The amount of information gathered about each host can be extended with plugins.
- Metasploit[17] allows an attacker or a penetration tester to search for security vulnerabilities within networks and systems and has an audit capability. Additionally, Metasploit permits testing of intrusion detection systems.
- Pegasus is a highly sophisticated spyware hacking tool designed by Israel's NSO Group, and (in theory at least) sold to governments for use in the fight against organised crime and terrorism. Pegasus is designed to be installed on most iPhone Operating System (iOS) and Android smartphones without the user taking any action, and is virtually undetectable. Pegasus can be installed either by gaining physical access to the device, or through a nearby wireless transmitter, and can relay the content of emails and text messages, photos, contacts, browsing history and location data as well as information provided by apps on a smartphone.

  Although some Android devices appear to have been infected, it is mostly the Apple iPhone that appears to be the major target, and it has been suggested that this happens through the iMessage applications. It is said that Pegasus can self-destruct if it is unable to contact its command-and-control server for 60 days.

  There have been numerous reports of investigative journalists and anti-government activists in oppressive regimes being targeted, some of whom it is claimed have been arrested, tortured or even killed as a result of the spyware's results.

  In April 2022, it was alleged in *The Guardian* newspaper (among others) that a smartphone in the office of the UK's Prime Minister – 10 Downing Street – had been infected with Pegasus, and that the UAE was the country responsible for the attack.[18]

A quick search on the internet will reveal many more hacking tools.

CYBER-ATTACK METHODS

In this section, we shall examine approaches to conducting cyber-attacks and the methods employed by attackers to achieve their objectives.

Tools and approaches

Cyber-attacks can occur as seemingly random events – often these will be untargeted attacks, in which the attacker uses a scattergun approach to try and hit as many targets

[16] See http://angryip.org/about/

[17] See https://www.metasploit.com

[18] See https://www.theguardian.com/politics/2022/apr/19/boris-johnson-must-pay-attention-to-basic-cybersecurity-rules-says-security-adviser

as possible. This type of attack may require some preliminary investigation work but is more likely to result from the purchase of something like an email address list or a list of credit card users. The resources or tools required to undertake this type of attack will almost certainly be commodity resources that can be found or bought from sources on the internet.

Another type of attack is posed by more organised individuals or groups, and will usually be targeted directly at individuals, groups of individuals or organisations. Some of the resources or tools required to undertake this type of attack will almost certainly be the 'commodity' type referred to above, but in those cases where specialist attackers have been hired, the tools will often form a bespoke malware payload, and may be individually crafted or modified for that particular attack.

For a more complex cyber-attack, it would be unusual for the attacker to use just one tool to carry out the attack. It is much more likely that they would use a mixture of tools, each designed to carry out a portion of the overall plan, and these are often referred to as 'blended' attacks.

Stages of an attack

While the stages of an attack will vary, a sophisticated cyber-attack will typically take a highly structured form, such as the model described by Lockheed Martin's 'Cyber Kill Chain'.[19] There are seven distinct stages:

1. Reconnaissance. In the first stage, the attacker will reconnoitre the target's networks and systems, looking for known vulnerabilities that can be exploited as a means of entry. This reconnaissance itself is likely to be highly sophisticated since it must achieve its aims without alerting an intrusion detection system.
2. Weaponisation (preparation). Once the target has been surveyed and the detailed objectives are understood, the attacker will prepare the software tools required to achieve them. This may involve the modification of existing commodity tools, or in extreme cases the development of specialist bespoke tools.

   Attackers may also take the opportunity to elevate their network or system access status, at least until they have deployed and tested the payload.
3. Delivery. The attacker will now upload the tools onto the target system or systems, or to a targeted user, checking that they are hidden both from normal view and from detection by more sophisticated means. Delivery could be as simple as loading it onto a USB memory stick that will be found by or given to a user, attaching the malware to an email, or placing it on a social media website or in a 'watering hole' website.
4. Exploitation. The attacker needs to be certain that the final attack will be successful, so a known vulnerability on the target system will be exploited in order to execute the malware. This might also be the action of a user clicking on a link or opening an email attachment.

[19] See https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

5. Installation. Having gained access to the target system or systems, the attacker will now install the malware. Often the malware suite will contain additional code to ensure that it cannot be deliberately removed and may also be time-stamped by the attacker so that it appears to blend in with other legitimate operating systems or application software.
6. Command and control (C2). Having verified that the tools will work as expected, the actual attack can be executed, by possibly choosing the most appropriate moment, for example when many of the security support staff are not at work; or by staging a major diversion that will draw attention away from the real attack.

   The attacker may use a channel over the internet, DNS or email protocols to achieve this.
7. Actions on objectives. Now the attacker can begin the real work, which may be to harvest user credential information, to escalate privileges so that they can gain access to systems currently out of reach, to exfiltrate other data, or simply to modify or delete data or destroy systems, or to install ransomware.

The theory of the Lockheed Martin Cyber Kill Chain is that if the defending organisation understands the type of attack, with the right tools and techniques they can stop it at any of the earlier stages and prevent the attacker from achieving their final objectives. However, this presupposes that the defending organisation can either be ahead of the attacker or can at least keep pace with the attack.

In some extreme cases, there will be two separate attacks – the first to establish the exact details of the target, and the second to conduct the actual attack. The whole process can take many months, especially if there is a significant amount of bespoke software to be developed and tested. A simpler approach would be used for commodity-type attacks, in which no further software development is required, and following the initial reconnaissance the payload is deployed and the attack executed very quickly, so as to take advantage of the element of surprise, which might be lost if the time interval is too great.

TYPES OF CYBER-ATTACK AND ATTACK VECTORS

There are numerous types of attack used to breach computers – far too many to list them all in this book, so here is a selection of the most common attack types.

Dark patterns

While not actually a cyber-attack as such, dark patterns are an excellent starting point, since they show what can be achieved while remaining just on the right side of the law.

Dark patterns are perfectly legal (but usually unethical) methods used by website designers to tempt the unwary into making a choice or selection they might not normally make. Each method has a link to an example from www.darkpatterns.org/ in the notes. There are many more such examples of these on their website. Examples of dark patterns include:

- Bait and switch techniques – an example of which was included in a Windows 10 upgrade offer by Microsoft. When the user clicked the red 'x' button, expecting to reject the upgrade, the upgrade was actually initialised instead.[20]
- Disguised adverts, in which clicking on what appears to be a legitimate link to a website the user wishes to visit takes them to somewhere different, and this can be a malware site.[21]
- Enforced subscriptions, in which the user finds they have committed themselves to an ongoing subscription rather than a one-off transaction. Often, the only way to get out of this is to call the organisation's helpline, which can involve a premium rate call.[22]
- Friend spam, in which you register your email, Facebook or Twitter account with a website, which then publishes content or sends out bulk email, Facebook messages or Twitter messages using your account.[23]
- Hidden costs are a common example of dark patterns. The user begins to make a purchase on a website, but as they progress to the payment they find that additional charges, such as transaction fees, taxes and so on have been added. In other cases the original advertised cost does not include delivery charges to make it appear more attractive.[24]
- Misdirection techniques are used to increase revenues from websites. In one case, Ryanair's website led customers to believe that it required some 'Passenger details', which they duly completed. It then added travel insurance to the total cost of the flights, and the only way to remove this was to select the 'No travel insurance' option carefully concealed in a drop-down menu described as 'Country of residence', which defaulted to United Kingdom.[25]
- With price comparison prevention techniques, users are either not permitted to copy and paste details from a supplier's website, as a means of discouraging them from finding a better price, or the organisation refuses to allow its products to appear on price comparison websites, claiming that this gives the shopper a better deal.[26]
- Roadblocks, also known as Roach Motels, are frequently used in order to prevent a user going further with a transaction until they have agreed to something. It frequently requires considerable effort to bypass this type of dark pattern.[27]
- Basket extras can be items in a user's website shopping basket that have unexpectedly changed cost. You may be purchasing a subscription and find that the website has changed your choice to a three-year deal, when in fact a one-year

[20] See https://www.deceptive.design/types/bait-and-switch

[21] See https://www.deceptive.design/types/disguised-ads

[22] See https://www.deceptive.design/types/forced-continuity

[23] See https://www.deceptive.design/types/friend-spam

[24] See https://www.deceptive.design/types/hidden-costs

[25] See https://www.deceptive.design/types/misdirection

[26] See https://www.deceptive.design/types/price-comparison-prevention

[27] See https://www.deceptive.design/types/roach-motel

subscription is actually better value for money. This type of dark pattern can also include additional items such as insurance in a user's website shopping basket without their knowledge.[28] However, legislation is currently in development in a number of jurisdictions that would outlaw this practice.

Application layer attacks

Application layer attacks take place when firewall ports are left open for an attacker to use as a means of entry. Unfortunately, if an organisation is to be able to conduct business, at least one port (port 443 – Hypertext Transfer Protocol Secure (HTTPS)) must always be open for general internet traffic. Port 80 – Hypertext Transfer Protocol (HTTP) tends to be less commonly used nowadays. A further port (port 25 – Simple Mail Transfer Protocol (SMTP)) is used for email traffic. Port 445, used by Microsoft file and printer sharing services, is normally blocked by firewalls. It is through these and other ports that a cyber-attacker can target specific applications – for example a web server application – and take advantage of a known vulnerability.

Botnets

Botnets are a means by which cyber criminals can target a large number of potential victims, most of whom are almost certainly unwilling recipients. Botnets consist of a very large number of malware-infected computers, known as 'zombies', which deliver the payload, whether this is spam email or a DDoS attack. These computers will have been accessed at some time by the botnet owner, sometimes known as a 'herder', who will probably have gained access either by the user clicking on a link in a spam email or by clicking on a link on a web page, either of which will have downloaded some form of malware onto the user's computer without their knowledge.

This malware will allow the botnet owner to take control of the computer when they require, using one or a group of command-and-control computers. In cases such as this, the computer's user is unlikely to be aware that their computer has been compromised.

The botnet owner may not actually make use of the botnet themself but may sell the service to people or organisations who wish to send spam email or mount DDoS attacks without having to create their own botnet.

It is important, however, to understand the difference between botnets, which are an aggressive means of conducting a cyber-attack, and distributed computing, where many computers are linked together in an organised endeavour in research.

Occasionally the law enforcement agencies manage to identify the botnet's command-and-control servers and are able to take down the entire botnet, as in the case of the 'GameOver Zeus' botnet, which at its peak included over a million zombie computers and had been designed to be impossible to be disabled.[29]

[28] See https://www.deceptive.design/types/sneak-into-basket

[29] See https://www.vice.com/en/article/539xy5/how-the-fbi-took-down-the-botnet-designed-to-be-impossible-to-take-down

Brute force attacks

Brute force attacks are those in which a cyber-attacker attempts to discover something – for example, a password – by testing every possible combination of characters until the correct password is revealed.

Brute force attacks can take extended periods of time to succeed but will invariably find the correct result eventually. The development of faster distributed and parallel computing will reduce the time taken, but it is still a time-consuming activity, and it can often be more efficient to try and discover a password by other means such as social engineering.

Buffer overflow attacks

This type of attack is a well-tried and trusted method of breaking an application by providing it with more input than its designer expected or planned for. For example, if an application suggests one uses a username of up to 20 alpha-numeric characters and the user inputs 21, the application might go into an unknown state unless the programmer had applied a check to discard the input if the total was greater than 20 characters. One method of deploying malware is to hide it within user input of this type.

Once an application has been broken in this way, it is quite conceivable that a cyber-attacker might be able to use the application's functions as if they were a bona-fide user.

Most recently written software usually takes account of buffer overflows, but occasionally a new one turns up and the cyber-attackers have a field day until a fix can be developed and installed.

Backdoors

Occasionally, programmers will build a 'backdoor' into their code. This will allow them to make changes while the code is being tested. Unfortunately, unless these backdoors are removed prior to the software being sold or distributed, anyone who is able to find such a backdoor will have instant access to the entire code, and (in theory at least) will be able to do anything they like, such as extract personal data, block selected users, skim off money – the world is suddenly their oyster.

The US and UK security agencies have long been concerned that Huawei's networking equipment might contain backdoors, and although they have not explicitly said that such things have been discovered, there is now a move to ensuring that their equipment does not form a major part of the countries' telecommunication networks.

While this is a laudable endeavour, it appears to ignore the possibility that 'home-grown' suppliers might also have backdoors in their operating software.

Injection attacks

Another form of attack is the injection attack, in which the attacker either injects software code into a program, or otherwise inserts forbidden characters that might cause an application to terminate, leaving access clear for the attacker. An example of this in Structured Query Language (SQL) databases is to inject an '&' character in order to execute SQL commands.

Network protocol attacks

As mentioned in the preface to this book, the protocols that underpin the internet are far from secure. These include the following protocols, without which the internet does not work:

- User Datagram Protocol (UDP),[30] defined in Request for Comments (RFC) 768;
- Internet Protocol (IP),[31] originally defined in RFC 791;
- Transmission Control Protocol (TCP),[32] originally defined in RFC 793, now RFC 9293;
- Network Time Protocol (NTP),[33] originally defined in RFC 1305;
- Internet Protocol Version 6 (IPv6),[34] originally defined in RFC 2460, now RFC 8200;
- Border Gateway Protocol (BGP),[35] originally defined in RFC 1654, now RFC 4271.

There is no real need for the reader to understand exactly how these work or inter-relate – as with the earlier analogy of the motor car engine, we can still surf the internet without this knowledge, but suffice it to say that if attackers can subvert any of these (and some others), they can do considerable harm.

Rogue update attacks

Rogue update attacks are an extremely popular method of conducting a cyber-attack. They often take advantage of unsuspecting or inexperienced users by suggesting – often in an email or as a pop-up on a website – that some element of the user's computer is out of date and requires an urgent update. This may be either an operating system or a commonly used application and will inevitably end with the computer being infected with some form of malware or ransomware.

Email-borne attacks

Email is very commonly used as a vector for conducting cyber-attacks, since many usernames can be easily guessed by simple software that combines known first names with known surnames, placing a full stop between them, and adding '@' and a known email provider's domain name, such as 'john.smith@gmail.com'.

[30] See https://www.ietf.org/rfc/rfc0768.txt

[31] See https://www.ietf.org/rfc/rfc0791.txt

[32] See https://www.ietf.org/rfc/rfc9293.txt

[33] See https://www.ietf.org/rfc/rfc1305.txt

[34] See https://www.ietf.org/rfc/rfc8200.txt

[35] See https://www.ietf.org/rfc/rfc4271.txt

Software can generate such email address lists extremely quickly, and emails using these addresses can be delivered at little or no cost to the cyber-attacker, potentially reaching thousands of email users at a keystroke. The malware, ransomware or other message that these emails contain will invariably result in some successes, and spammers rely on people's susceptibility to great offers.

Following the Monty Python 'Spam' sketch[36] in 1970, this form of email was dubbed 'spam', and the name has stuck. Fortunately, an increasing number of internet service providers are on the case very promptly and can identify spam and delete it before it can reach its destination. However, this may, in some cases, require the end user to pay for a premium service. Alternatively, they could purchase the anti-spam service from an independent provider such as Message Labs or AVG.

Wireless network attacks

Cyber-attacks that use wireless connectivity can generally be in one of three areas:

- cyber-attacks on a Wi-Fi (802.x) infrastructure;
- cyber-attacks on a Bluetooth infrastructure;
- cyber-attacks on the Global System for Mobile Communications (GSM), third generation (3G), fourth generation (4G) and fifth generation (5G) cellular mobile infrastructure.

Wi-Fi attacks

Wi-Fi attacks are extremely common and can usually be conducted in one of two ways. The more difficult approach is for the attacker to intercept the signal of a wireless access point, to store the intercepted data, and to attempt to recover the access key by 'brute force' searching. Those access points that only have WEP or the original WPA encryption will be much easier to break into than those with WPA versions 2 and 3.

The second (and often more straightforward) method is for the cyber-attacker to introduce their own access point with an SSID similar or identical to that of a genuine access point, for example in any public space offering 'free' Wi-Fi. When an unsuspecting user tries to connect, and gives their access key, the attacker's computer will capture the data and the attacker will be able to access the real network as if they were a genuine user. Further, if the attacker is even more skilled, they will allow the user's computer to make an onward connection to the real network, creating a 'man-in-the-middle' attack. The attacker can now monitor the user's application login details, providing the attacker with access to at least one system within the organisation, from which they may be able to access other systems, or even find they have administrative access.

Bluetooth attacks

Bluetooth attacks tend to be focused on end-user devices that have their Bluetooth wireless connection enabled, and which can be intercepted and accessed from the attacker's device. These generally lead less to full network access, and if the attacker is targeting a particular user, Bluetooth will be an excellent way of achieving their objectives.

[36] See https://vimeo.com/329001211

Through Bluetooth, an attacker can gain access to the victim's address book, calendar, email and much more besides. An example of the misuse of Bluetooth is in the case of Dublin Airport, which uses a passenger's Bluetooth identity to track them as they pass through the airport.[37]

If you ever want to see how easy it can be to select a target for a Bluetooth attack, simply go to the Bluetooth settings on your smartphone or laptop computer when you're on public transport, especially a commuter train, and you will see literally dozens of Bluetooth devices advertising their presence.

Similarly, if you go to the Wi-Fi settings, you may see the name of a user followed by the words 'Personal Hotspot' if they have previously used their device as a means of connecting another device to the internet.

A successful cyber-attack based upon either Bluetooth or Wi-Fi also requires a further lack of security awareness on the part of the user, such as blank or easy-to-guess passwords, which may frequently turn out to be the case.

GSM/3G/4G/5G attacks

Cyber-attacks against cellular mobile devices such as smartphones and tablet computers will mostly use either Wi-Fi or Bluetooth as a mechanism for attacking the device, since the cellular networks use a significantly more complex key management and encryption mechanism to protect the device and its data. Attacks against the GSM (2G) encryption standards are demonstrable using a false base station (similar to a fake wireless access point, but rather more complicated), but are relatively rare unless the attacker is being sponsored by a nation state government or security organisation, or a university research department.

The attacker must also ensure that the target is in close proximity to the false base station in order to verify that their phone connects to this rather than to a genuine network base station.

Attacks on third, fourth and fifth generation mobile phones are much less easy to undertake since the key management and encryption standards have been greatly enhanced so as to make interception and key recovery virtually impossible – at least for the time being.

Social media attacks

Attacks using social media methods are extremely common. These focus on two distinct areas:

- acquisition of personally identifiable information;
- tempting users to enter 'watering holes'.[38]

[37] See https://eu.usatoday.com/story/travel/roadwarriorvoices/2015/11/17/is-your-airport-secretly-spying-on-you-yes-if-you-are-in-dublin/83302142/

[38] See https://www.fortinet.com/resources/cyberglossary/watering-hole-attack

Acquisition of personally identifiable information (PII)

People using social media sites such as Facebook, Twitter, Instagram, TikTok and LinkedIn frequently provide vast quantities of information about themselves, which could be used by a cyber-attacker not only to gain access to the individual's social media account, but also to enter their bank accounts and other websites.

Equally problematic is when people's friends, acquaintances and colleagues post information about an individual on social media, often being thoughtless about the possible consequences.

Many organisations now search for the social media accounts of prospective employees, as this allows them to screen possible recruits covertly.

An attacker looking to discover the names of company directors need only search the Companies House website for free.

'Watering holes' and other user temptations

Once a cyber-attacker identifies a potential target on a social media site, they have the opportunity to tempt the target into accessing a website containing malware, known as a 'watering hole'. For example, some time ago, I received frequent requests through LinkedIn, offering me the opportunity to win an iPad. All of these were traced to malware sites, at least one of which would have resulted in additional personal information being provided as well as the planting of a virus on my computer.

Social engineering

Social engineering techniques are invariably a low-tech method for a cyber-attacker to acquire personally identifiable information or to gain unauthorised access to a computer.

Often this can begin with a simple phone call or email to tempt or invite the individual to part with information or money, or to click on a link to a malware website, as with the watering hole example above.

Other examples of methods of social engineering include an engineer tracing a fault or needing to check the gas/electricity meter; for companies, a person posing as someone from the IT department, often via a telephone call, or a 'contractor' attempting to talk their way past the reception desk. Much social engineering is performed by people skilled in 'sweet talking' the user, pretending to be trying to help (especially elderly or less technically aware users) and offering to make their computers more secure or to operate more quickly. Frequently these types of call result in the user's computer being infected with malware or ransomware.

> My younger son regularly receives scam telephone calls that refer to his recent 'accident'. He helpfully plays along by inventing details of the accident and the injuries he received in an attempt to keep the caller on the line for as long as possible. He eventually announces that he has won the prank, having wasted much of the caller's time, which hopefully would prevent someone else from being scammed.

Data aggregation

Data aggregation itself does not actually constitute a cyber-attack. It simply provides a means of bringing together items of data or information concerning an individual or group of individuals in order to gain a more detailed picture of them with a view to some form of exploitation, as discussed in earlier chapters.

However, when combined with the various methods of cyber-attack covered here, aggregating the resulting data becomes an extremely powerful tool in the hands of a more sophisticated attacker.

THE RISKS OF CONDUCTING A CYBER-ATTACK

There is an old saying, 'Thou shalt not be found out.' Much used in the past, the threat of being discovered applies just as much to cyber-attacks as it does to conventional misbehaviour. The impact of being identified as the originator of a cyber-attack varies from one type of attacker to another. Some will result in little more than public embarrassment for the miscreant; others could result in an extended holiday at His Majesty's pleasure; while some could potentially precipitate an international incident.

The likelihood of being identified will also vary, based on the attacker's technical abilities and their attention to detail. Inexperienced cyber criminals are more likely to make basic mistakes in their methods, whereas a more mature or experienced attacker or a state-sponsored group is almost certain to mount a highly professional, possibly multi-part attack, using methods described in the 'stages of an attack' section earlier in this chapter.

Although we will examine the principles of risk management in the next chapter, it is worth stating here that the impact or consequences that might befall a cyber-attacker, taken together with the likelihood of their being identified, combine to dictate the level of risk that the attacker faces, and that those individuals or organisations that undertake cyber-attacks must ensure they are equipped to handle them in a skilful manner or accept the consequences.

Prior to the advent of online banking, those who wished to rob a bank were obliged to do so in person, and while on the bank's premises placed themselves at some risk of being overcome by security guards, identified and subsequently arrested. Since the advent of the internet and the World Wide Web, these physical risks have been completely removed, and the risks of identification and subsequent arrest are much reduced.

The cyber-attacker will ultimately balance the risks against the possible benefits of success in the cyber equivalent of a cost/benefit analysis, and make an informed choice either to proceed or to leave well alone. Alternatively, of course, they may simply chance their arm.

At one extreme, an inexperienced hacker who defaces the website of a charitable organisation or posts unsavoury material might expect to find themself being 'flamed'[39]

[39] https://techterms.com/definition/flaming

by their peers. At the opposite end of the scale, American government agencies whose networks and systems have been penetrated – however innocently – have been known to demand extradition of the alleged offender.

The message is that unless you are at the very top of your cyber game, don't mess with government or military organisations if you are not prepared to accept the consequences.