ON THE OFFENSE

An attacker, or cyber attacker, is someone who tries to bypass system or network security without authorization for malicious purposes. A threat actor, or malicious actor, is an entity that poses a cybersecurity threat. Examples of such entities include people, groups, or organizations. Simply put, a threat actor is a potential attacker. They might not have tried to attack yet, but they intend to do so. While the terms attacker and threat actor have similar meanings, threat actor emphasizes the potential threat that the entity poses.

Cybersecurity professionals often discuss threat actors in terms of threat actor groups. These groups vary substantially in motivation, resources, and techniques. the five main threat actor groups: Script kiddie, Hacktivist, Criminal gang, Nation-state hacker, Malicious insider.

Script kiddies are the least advanced group. A script kiddie, or novice hacker, is someone who uses programs, often basic hacking tools, without truly understanding what is happening behind the scenes. Script kiddies typically rely on automated programs and techniques that more experienced hackers create. But they don’t understand the concepts underlying how these tools work. And though they might display a basic understanding of networking and programming, they often lack technical skills, patience, or strategic intent.

In practice, this demographic is mostly teenagers or young adults who are self-taught through forums, videos, and experimentation. For many script kiddies, the main motivations for their hacking efforts are reputation, status in the eyes of the hacking community, entertainment, or settling grudges. From a resourcing standpoint, script kiddies rely on off-the-shelf penetration testing tools and publicly available exploits. Script kiddies use artificial intelligence tools, such as chatbots, to create malicious scripts for them. In most cases, script kiddies are very underfunded and display little tradecraft knowledge.

From a defensive standpoint, organizations must ensure that their patching schedule is effective. If someone develops an easy exploit, attackers will probably deploy it. Defences must be formidable enough to ensure that another target appears easier, which should be a sufficient deterrent.

Penetration testing is a type of security testing that simulates real hacking techniques to find vulnerabilities that attackers can exploit.

Hacktivists seek political or economic change and use hacking as a means to achieve it. The term hacktivist combines hacker and activist.

The defining attribute of hacktivists is that they are driven by ideological reasons. Various types of people make up hacktivist groups. Like script kiddie groups, hacktivist groups include impressionable amateurs. But when causes align on a highly topical issue, hacktivists are joined by more experienced members within the IT security community. The aims of hacktivist groups define their motivations. Their aims vary enormously. Generally, a group’s aim involves supporting one cause that members believe in, such as a side in a Middle East conflict or political activities. Hacktivists use a range of basic tools that can be very effective at scale. Denial-of-service (DoS) programs are a notable example in this area. A single script kiddie poses little threat. But hundreds of them united by a common motive launching parallel attacks can be significantly more challenging to deal with. The most famous example of this group is the hacking collective called Anonymous(opens in a new tab). Anonymous is a decentralized international hacktivist group known for cyberattacks against corporations and governments.

If an organization does business in a sensitive area, such as animal testing or political causes, then it might come under a sustained attack from hacktivists. Such organizations must be astute. Having only good defences in place is not enough to deter all attacks, so organizations should have a plan and methods to cope with a sustained attack.

As long as there is easy money to make, criminals will be a problem. The internet has introduced a new method for criminals to prey on victims with an unprecedented scale, range, and ease. Rather than run risks in person, aspiring criminals can send millions of infected emails from halfway around the world and secure a ransom from a victim before transferring funds into cryptocurrencies to evade conventional policing methods. Capturing these criminals is extremely taxing. And because of international laws, securing a prosecution is nearly impossible. Sadly, most criminals are aware of these facts.

Criminal gangs are the fastest-growing threat actor group. Within the group are a range of activities. Consider the following examples: Gangs can run ransomware attacks, where victims must pay to regain access to their resources & Gangs can commit conventional theft of customer data or intellectual property. Being a cybercriminal is a full-time and potentially lucrative job. Gangs can range from a few people to multinational gangs with hundreds of members. You’ll often find specialists within each gang, and they can trade information on the dark web. Consequently, criminal gangs are quite advanced and well-organized. From a resourcing standpoint, criminal gangs provide cybercrime services and products. For example, gangs sell malicious software that steals personal information for financial gain. From a financial perspective, the criminals will always adopt the quickest and easiest get-rich-quick scheme.

To protect against a criminal gang, organizations should use effective defences for critical assets. Discovering ransomware on an employee’s laptop might cause inconvenience to the company. But discovering ransomware on a production server can be devastating.

The dark web is a subset of the internet comprised of websites accessible only through specialized web browsers. Activity on these sites is encrypted, private, and anonymous, making the dark web a popular hub for cybercriminals. However, some people use the dark web for legitimate reasons, such as political activists who use it to communicate anonymously to avoid government persecution.

Nation-state attackers receive the most media attention of all threat actor groups, perhaps unduly. Many military organizations worldwide consider cyberspace a fifth sphere of conflict alongside sea, land, air, and space. And many nations have demonstrated the ability to project power across national borders to a great and expanding variety of consequences.

The role of nation-state hackers is to provide a strategic advantage to their respective countries. Advantages can range from reconnaissance and information collection, such as traditional spying or signals intelligence, to information subversion and manipulation. Members of these organizations are well-educated or trained and cover a range of backgrounds. They work full-time and typically work at the forefront of their respective fields. Their motivations typically align closely with political or strategic objectives. A recent example is the Russian activities concerning the 2016 US presidential election. The aim was to interfere with the election and increase political and social discord. From a resourcing standpoint, nation-state hackers can access advanced research, dedicated infrastructure teams, and tremendous political support. Nation-state hackers are now using advanced artificial intelligence (AI) and machine learning (ML) tools to automate their attacks, making them more sophisticated and harder to detect. Also, with the rise of Internet of Things (IoT) devices, nation-state hackers have many more targets to attack.

Protection against determined nation-state hackers is highly challenging for organizations. Doing so effectively requires fully capable and coordinated security defences.

Malicious insiders are arguably the most concerning threat actor group. An insider is someone authorized to access an organizational resource, such as a system or data. A malicious insider intends to use that access to harm that resource or organization.

Some insiders have a negative mindset toward the organization from the start. Others become resentful over time. Motivations vary greatly and can cover just about everything. Financial interests and bitterness are two of the most common motivations. Other motivations include notoriety or fame. Insiders rarely rely on technical skills to attack. Some might use social engineering, which involves manipulating others into divulging confidential information usable for fraudulent purposes, such as gaining system access. But typically, insiders use their own corporate access and permissions. One common insider threat is an employee being extorted into giving someone access to the employee’s corporate accounts. Another common example is a disgruntled employee who steals corporate secrets before being fired. Perhaps the most famous insider attack of all time was Edward Snowden, who stole many National Security Agency (NSA) files from the US before giving them to WikiLeaks.

Defence against insider threats is best achieved by vetting employees, managing effectively, and applying technical controls. Resorting to technical controls might seem like too easy of a solution for companies, but it frequently fails because they are trying to stop users who are familiar with the system. Often, many warning signs precede an inside attack. Some examples of warning signs that someone is planning an attack include working alone, expressing resentment, producing lower-quality work, or doing unexplained activities. Identifying these signs can help prevent an attack.

These descriptions of the types of cyber attackers are not always precise. In operations, hacktivists might recruit script kiddies, and nation-state hackers might recruit criminal gangs. Also, some cyber attackers disguise their work to appear less advanced than they are. These facts can make attributing threats to the correct party difficult.

Five common types of cyber attackers have personal motivations or threatening, often illegal motivations. But not all hackers hack for malicious purposes. Offensive security researchers choose to use and monetize their skill set for good rather than criminal or exploitative activity. Often called ethical hackers, they take on a hacker mindset to use the same methods as real-life attackers but with the goal of testing and fortifying systems to help clients and consumers be better protected from the real incident.

Attackers can use various methods to enter and exploit systems. Some attacks target vulnerabilities in technology. Others exploit vulnerabilities in humans, specifically the flawed ways in which humans interact with systems. The most common types of cyberattacks: Denial-of-service (DoS) attack, Distributed denial-of-service (DDoS) attack, Phishing, Spear phishing, Malware, Man-in-the-middle (MitM) attack, Domain Name System (DNS) attack.

A denial-of-service (DoS) attack is any attack that causes a complete or partial system outage. DoS can occur when a person or system floods a website or online service with too much network traffic, much like a traffic jam on a road. This traffic overflow makes the website or service slow down or shut down completely, denying access to legitimate users. DoS can also occur when traffic consumes enough system resources to slow down or crash the system.

An attacker uses a billion laughs attack, also known as an XML bomb, where the attacker creates a small, seemingly harmless piece of code in an Extensible Markup Language (XML) document. The attacker then submits this document to the target organization’s system. When the system processes the code, the code continually replicates. The replications consume more and more system resources, eventually slowing down or even crashing the system.

A distributed denial-of-service (DDoS) attack is an attack that comes from multiple sources simultaneously to cause a complete or partial system outage. To perform DDoS attacks, attackers use bots. A bot, or zombie, is an internet-connected device infected with malware that enables the attacker to control the device remotely. For DDoS attacks, attackers manipulate multiple bots under the same instance, forming a network of bots called a botnet. A botnet can include hundreds or even thousands of bots, each sending data or requesting access from the target server simultaneously. This sudden traffic surge overwhelms the server, causing a denial of service to its users. Attackers can use AI to analyze patterns and predict the optimal number of bots needed to effectively overwhelm a target’s server without wasting resources. AI also helps attackers monitor each bot’s performance in real time to maximize effectiveness.

An attacker can send many page requests to a web server over a brief period, overloading the server. Similarly, spikes in user demand on ticket sale websites can overload systems.

Phishing is the practice of sending messages, seemingly from a trusted source, to trick users into taking a specific action. It combines social engineering and technical trickery. After opening the message, unsuspecting users might install malware, enable remote access, or divulge confidential information.

An attacker might send an email with a file attachment or link to a fake website. When the recipient clicks the attachment or link, they unwittingly install malware on their computer.

Spear phishing is a type of phishing that targets a specific person, group, or organization. Attackers take time to research targets. Attackers use this research to create personal and relevant messages, making them more effective. Some attackers use AI to automate the email creation process. They generate personalized and convincing emails that are more likely to deceive users into revealing sensitive information.

An attacker collects a target’s details from social media and then calls the target, pretending to be a bank representative. The attacker claims that the target’s account is compromised and asks them to transfer money to a safe bank account. The attack is convincing because the attacker uses legitimate knowledge about the client.

Malware is a catch-all term for malicious software. Malware is software designed to harm data or systems without the user’s informed consent. It often triggers secretly when a user runs a program or downloads a file. This user action is often unintentional. Once active, malware can block access to data and programs, steal information, and make systems inoperable. AI can help malware adapt to evade detection, enabling them to cause more damage within an infected system.

Many types of malware exist and often, the malware’s name indicates its function. For example, keyloggers capture a victim’s keystrokes, and ransomware holds a victim’s files captive in exchange for a ransom payment.

A man-in-the-middle (MitM) attack occurs when attackers insert themselves into communications between a client and server. With this attack, attackers can view everything that both sides send and receive.

An attacker might set up a free wifi hotspot in a popular public location. If someone connects to that network, the attacker can examine their communications. In turn, the attacker can redirect the victim to a fake login screen or insert advertisements over web pages.

The Domain Name System (DNS) is one of the core protocols used on the internet. With the DNS protocol, a computer can resolve a domain to an IP address. For example, imagine a user types bmw.com into a browser’s search bar and then presses Enter. The DNS protocol resolves this domain name to the IP address for the main BMW website, taking the user to the site. This function is convenient because domain names are far easier to remember than IP addresses! A DNS attack targets the DNS by manipulating or disrupting the resolution of domain names and possibly redirecting users or hindering access to websites. It involves tactics such as domain hijacking and cache poisoning.

Attackers associated with the Roaming Mantis criminal gang have compromised wireless routers so that entering the URL for a valid website redirects the user to a malicious website. This site delivers malware called Wroba to the user’s device. When the device is infected, the attackers can use it as a bot, and then use it to compromise other wireless routers.

Structured query language (SQL) is a programming language for accessing, managing, and querying databases. SQL injection is the placement of malicious code in SQL queries, usually via web page input. With a successful attack, attackers can run common commands, including commands to delete the database itself! SQL injection is one of the most common web hacking techniques. Attackers can use AI to automate the process of discovering and exploiting vulnerabilities in a database’s security.

In the UK, two teenagers managed to target TalkTalk’s website in 2015. Using SQL injection, they stole hundreds of thousands of customer records from a database that was remotely accessible.

Attackers are increasingly turning to AI. With AI, attackers can enhance the structure and sophistication of their attacks in several ways.

Task automation: AI can automate repetitive tasks, enabling attackers to launch attacks at a speed and scale otherwise impossible. For example, AI can automate the creation and dissemination of phishing emails, increasing the likelihood of success.

Detection evasion: AI can help attackers create malware that changes and adapts to evade detection by traditional antivirus solutions. To do so, attackers often use machine learning (ML) algorithms that can learn from each detection attempt and alter the malware’s code to avoid future detections.

Target identification: AI can help attackers identify optimal targets for attacks. Sophisticated algorithms can analyze vast amounts of data to identify vulnerable systems or high-value targets, thus increasing the effectiveness of attacks.

Social engineering: Attackers can use AI technologies, such as deep learning, to enhance the effectiveness of social engineering attacks with convincing fake audio and video content. One notable example is deepfakes, which are fake images, videos, or audio created through deep learning. For example, an attacker might call a victim and use an audio deepfake to impersonate someone that the victim knows and trusts.

AI has introduced a new challenge for cyber defence systems. The cybersecurity landscape must continually evolve, incorporating AI in its strategies to effectively counter these advanced threats. DoS attacks on organizations are commonly reported in the news. Phishing attacks are the most effective on a personal basis. Malware attacks are increasing in number and constantly evolving.

Lockheed Martin Corporation is an American global aerospace, defense, security, and advanced technologies company. Researchers at Lockheed Martin identified parallels between the US military concept of a kill chain, which refers to the structure of a military attack, and intrusions in digital networks. Here, the word chain refers to a series of steps attackers must take to infiltrate a system successfully.

Cybersecurity professionals use this framework to understand and prevent cyberattacks. Each step of the chain represents a different stage of an attack, and the steps must occur in order because each step depends on the previous step’s completion. With this framework, you can view the attack as a process, not a single event.

Step 1: Reconnaissance: During this step, the attacker gathers information about the target. They can do so through probing digital servers, speaking with people close to the target, or just reading the news!

Step 2: Weaponization: During this step, the attacker designs a piece of malware to exploit an identified vulnerability. After identifying a specific vulnerability, the attacker designs a piece of malware to exploit it. This process can range from downloading a database sample, purchasing a tool from a third party, or developing something custom.

Step 3: Delivery: During this step, the attacker sends the chosen malware to the target somehow. The attacker must send the chosen malware to the target somehow. Despite more recent technological developments, email is still the most common delivery method. Other methods include website downloads and infected or modified USB flash drives.

Step 4: Exploitation: During this step, the malware attempts to get some element of persistence within the target system by creating backdoors. When the target activates the malware by opening the infected attachment in the email or accessing the USB flash drive, the malware performs a series of instructed steps. This process varies considerably and depends on many details about the programs and operating system. This process is known as exploiting a vulnerability, and the software used to do it is known as exploit code or an exploit.

Step 5: Installation: During this step, the target activates the malware, and then the malware performs a series of instructed steps. The malware attempts to get some element of persistence within the target system. It can do so by creating backdoors, such as through the following methods: 1. Creating new accounts. 2. Installing remote access programs. 3. Introducing new vulnerabilities into the system. These factors mean that even if the original vulnerability is patched, it is too late because the attacker can still access the system through the backdoors that the malware created.

Step 6: Command and control (C2): During this step, the attacker establishes a method to communicate with the compromised systems. By doing so, the attacker can send instructions and upgrades to the target and receive data back from the target. The attacker must establish a method to communicate with the compromised systems. By doing so, the attacker can send instructions and upgrades to the target and receive data back from the target. The attacker can establish communication through websites, direct connections, and even social media sites such as X.

Step 7: Actions on objectives: During this step, the attacker accomplishes their objectives, such as stealing data or destroying key system elements. After all the previous steps are complete, the attacker can accomplish their objectives. For example, they might steal data, modify data, or destroy key system elements.

MITRE is an American non-profit organization that solves world problems with data-driven solutions. Its areas of focus include cyberthreat information sharing and cyber resilience. MITRE collected a set of tactics, techniques, and procedures (TTP) that cyber attackers use. It used this research insight to develop ATT&CK, which stands for Adversarial Tactics, Techniques, and Common Knowledge. This acronym is pronounced as “attack”. MITRE created a matrix based on this collected knowledge to help organizations examine cyberattacks in a simplified form. The ATT&CK matrix is open and freely available to any person or organization. The following graphic shows an excerpt from the ATT&CK matrix. Access https://attack.mitre.org to examine the entire matrix.

The column headers identify an attacker tactic, such as persistence. You can think of each tactic as an attacker’s objective. The items listed for each column are the many techniques that the attacker can use to achieve the tactic or objective. You can select each technique to learn more about it.

Imagine the following cyberattack:

An attacker wants to gain credentialed access to a system. Credentialed access is the tactic. If the attacker identifies poor security mechanisms for logging into the system and discovers that no account lockouts are in use, they can use the brute force technique. Brute force is one of many techniques for gaining credentialed access listed in the ATT&CK matrix. In this technique, the attacker runs a program that can try millions of username and password combinations until a successful one is identified. If the chosen technique fails, the attacker can switch to another technique and continue trying.

Attackers can be persistent. Rarely do they give up after a single interruption to their attack. Think of a cyberattack as part of a longer campaign. Many attacks last months, with attackers spreading their influence and defenders trying to identify and stop them. Good defenders try to anticipate an attacker’s next move. Frameworks such as the MITRE ATT&CK matrix help them to do so.

The following scenario will help you explore the significance of these frameworks.

Initial access: The first two tactics in the MITRE ATT&CK matrix are reconnaissance and resource development. Because the breach has already occurred, Janina starts her investigation with the next tactic: initial access. She identifies the initial breach point.

Phishing: Janina investigates the initial access further to discover the technique used. She determines that the attacker used the phishing technique, which is listed as one of the techniques under initial access. Specifically, the attacker used spear phishing. They tailored their phishing email to a company executive, tricking this person into providing their login credentials.

Execution: Next, Janina turns to the MITRE ATT&CK matrix to predict the likely next steps of the attacker. She examines the tactic that follows initial access in the matrix: execution. She reads that at this stage, attackers use various types of commands and scripts to run malicious code on systems. As a cybersecurity professional, she knows that scripting is a common technique after spear phishing. Putting all this information together, Janina predicts that the attacker used scripts to automate their malicious operations and move further into the system.

Scripting: Janina immediately checks for signs of scripting in the system logs. She finds evidence that the attacker used a PowerShell script to perform malicious commands. This finding confirms her hypothesis that the attacker used scripts to move further into the system.

Persistence and privilege escalation: Having identified the attacker’s current tactics and techniques, Janina uses the MITRE ATT&CK matrix to prepare for the next likely steps. She focuses on the persistence and privilege escalation tactics; these tactics typically follow execution. She counters the cyberattack with the mitigation strategies listed for both techniques.

A vital element of the cybercrime economy is a robust and growing underground ecosystem with a vast, interconnected network of illegal platforms and forums. In this digital black market, cybercriminals buy, sell, and trade tools and stolen data. They also use this space to collaborate and train themselves and others. They can seek advice, learn new attack methods, and even hire skilled people to perform specific tasks. Like a traditional economy, specialism drives efficiency and allows criminals to focus on what they each do best.

The underground ecosystem continually evolves, with new forums and platforms appearing as authorities shut down others. Its dynamic nature and global reach make it a challenging threat to cybersecurity efforts.

To make money criminals use one of these three methods.

Theft: The most direct method for cybercriminals to make money is trying to steal money from targets. They can do so by compromising accounts or banking systems, but the most common means is fraud or deception. These scams are often technical support scams or similar tricks aimed at persuading a victim to give away bank details, personal information, and other data usable for making money off the victim.

Work for hire: Sometimes, criminals offer their services to carry out illegal tasks to regular people and organizations. In this model, the criminal does not take money from the victim. Instead, an organization or person pays them. A typical illegal task performed for hire is using a denial of service (DoS) attack to overload key parts of a service. For example, a criminal might offer an organization or person the ability to disable a competitor or rival. Another common task is stealing a competitor’s intellectual property or destroying their databases.

Extortion: Another way to make money is extortion. In this model, the criminal gains the ability to disrupt a victim by disabling key systems or threatening to divulge sensitive data. Extortion has become increasingly popular with the advent of ransomware. In a ransomware attack, a victim’s key systems and files become encrypted, rendering them inoperable. To restore the systems and files, the victim is asked to pay money as ransom to receive the decryption key. Other extortion-themed approaches include threatening to divulge organization or customer data, such as embarrassing executive emails or customer databases.

In ransomware attacks, cybercriminals require victims to pay a ransom. Typically, victims must pay in the cybercriminal’s preferred currency: cryptocurrency. But what exactly is cryptocurrency, and why do cybercriminals prefer it?

Cryptocurrency is a digital or virtual currency that uses cryptography to secure financial transactions, control the creation of new currency units or coins, and verify asset transfers. Each cryptocurrency has its own rules and protocols, but they all operate on an emerging technology called blockchain. Blockchain is a distributed ledger that records all transactions across a computer network. The system encrypts each transaction, adds it to a block, and then adds that block to a chain of previous blocks. This process creates a permanent and transparent record of all transactions, making altering or manipulating the data difficult.

Cryptocurrencies offer several advantages over traditional currencies, such as faster and cheaper transactions, increased privacy and security, and potential service for unbanked or underbanked individuals. But cryptocurrencies also pose risks, such as volatility in their value and challenges from regulations. The most relevant risk for cybersecurity is their potential use in illicit activities.

Cybercriminals often use cryptocurrencies because the currency is anonymous and typically decentralized, meaning that it operates independently of a central authority, such as a government or bank. These features make tracing transactions difficult for law enforcement agencies. Cryptocurrencies, especially Bitcoin, have become the primary currency of the dark web, where criminals trade illicit goods and services. Consider the following examples: In ransomware attacks, cybercriminals demand payment in Bitcoin because its anonymous nature masks the receiver’s identity. In many money laundering schemes, cybercriminals use Bitcoin to erase the funds’ illicit origins by moving money through virtually untraceable networks.

The five general steps of the cybercrime economy are:

Design malware: In the first step, a criminal gang produces a piece of malware that records keystrokes and screens.

Attack victims: In the second step, the gang attacks multiple victims’ accounts. It buys a list of known email addresses from another party and sends the malware as an email attachment. The malware aims to infect victims’ machines, steal their banking logins and other passwords, and send these credentials to the gang. At this point, the gang’s work is done. It has a list of banking logins and other credentials.

Withdraw money: In the third step, the gang tries to withdraw money from the accounts or sell the account logins to another gang to finish the process.

Involve money mules: In the fourth step, the gang tries to log in using the credentials and make transfers to money mules that they have previously worked with. Money mules are gullible or desperate individuals who have agreed to allow a stream of money through their accounts in exchange for a payment.

Use cryptocurrencies: In the fifth step, the gang finishes the process by forcing the mules to buy cryptocurrencies and then transfer them to the accounts that the gang controls. With this action, the campaign is also complete. If law enforcement investigates the crime, the trail often ends with only the money mule being traceable.

Social engineering is the art of making someone do what you want them to do. It overlaps heavily with academic fields involving psychology, biology, and even mathematics. In cybersecurity, social engineering is the use of deception to manipulate individuals into divulging confidential or personal information for fraudulent purposes. Basically, how can someone trick another person into giving up something private? Social engineering attacks are the dark art of using social interactions to trick people into making security mistakes.

Attackers can employ social engineering tactics in person, over the phone, or online through websites, email, and social media. When an attacker makes someone perform a certain action, the attacker can gain access to sensitive systems, steal assets, or advance a more complex attack. This notion of focusing on persuading or tricking people might sound unreliable. However, many case studies show that social engineering is an incredibly powerful technique.

Effective social engineering tactics can result in defrauding vulnerable people of their savings through scams and confidence tricks. For organizations with physical buildings, social engineering also includes tailgating, which is when a person enters a secure area without authorization by closely following an authorized person.

Social engineering works because humans are imperfect. In short, attackers exploit people’s propensity to take shortcuts and make quick decisions based on false promises.

Human nature and social norms: Social engineering takes advantage of human psychology and our natural inclination to trust and help others. Attackers exploit social norms and expectations to manipulate people into divulging information or performing actions that they wouldn’t perform otherwise. For example, an attacker might pose as a coworker in distress, urgently needing access to a particular system to meet a deadline. The target, driven by the desire to be helpful, provides the requested information without second-guessing the authenticity of the request.

Trust and authority: Attackers often exploit people’s trust in authority figures or institutions. They can gain credibility and deceive targets by impersonating someone in a position of power or using official-sounding language. For example, an employee might receive an email from someone claiming to be the company’s chief executive officer (CEO). The supposed CEO demands immediate action on a sensitive issue, such as providing access to a client’s records. Because the email seemingly comes from the top executive, the employee hastily complies without verifying the authenticity of the request. As a result, the employee provides confidential client data to the attacker.

Emotional manipulation: Social engineering often uses emotions such as fear, curiosity, or excitement to influence decision-making. Attackers create a sense of urgency or exploit personal vulnerabilities to manipulate targets. For example, someone might receive a phone call from an attacker posing as a representative for the lottery. The attacker congratulates the person for winning the grand prize. The excitement and lure of a large monetary reward cloud the victim’s judgment. In turn, they share their bank account information to ensure the lottery company can transfer the supposed prize into their account.

Lack of awareness: Social engineering works well on people less informed about common security and potential risks. And people unfamiliar with social engineering tactics are especially susceptible to manipulation. For example, a person might receive an email that seems to be from a trusted banking institution instructing them to update their password because of a security breach. Unaware of standard social engineering tactics such as this one, the person promptly follows the instructions and unknowingly gives their login details to the attacker.

A social engineering attack typically has these elements.

It is well-researched. If an attacker is trying to impersonate a member of a company, then they will use the company’s letterhead, jargon, or format to help build credibility. Not all methods are equally effective against everyone. Cyber attackers research to determine the best driver for their target.

It is delivered confidently. In-person, good social engineers are prepared and confident, and they reassure targets. Knowing when to launch an attack and how to develop a rapport with the target is essential. Usually, attackers build up a high-value social engineering attack over a series of exchanges, lending credibility and reducing inhibitions with each exchange. Rushing the attack can backfire and lead to attackers revealing themselves through desperation.

It is plausible and realistic. The best social engineering attacks are often the ones where the victim doesn’t even know that they’ve been tricked.

Everyone should be aware of and guard against common social engineering attacks. Aside from never trusting anyone, you should follow this simple rule to defend against social engineering attacks designed to trick people like you. If something seems too good to be true, it probably is.

But how do organizations defend against social engineering? They should focus on the three key elements of cybersecurity: process, education, and technology. Process: They should implement policies that outline the acceptable use of corporate resources and procedures for handling sensitive information. Education: They should hold regular cybersecurity training sessions to ensure that every employee understands the policies and the risks associated with violating them. Technology: They should invest in security software, such as spam filters and antimalware software, that can detect and thwart social engineering attacks.

Phishing emails are one of the most common forms of social engineering, and if you let your guard down, you can fall prey to this tactic. Follow these tips to detect phishing emails, whether personal or business-related. Note that no single phishing email will contain all the signs of phishing mentioned in this list. But the more of these clues that you find in an email, the more likely that it is a phishing attempt.

If you receive an email that you think might be phishing, don’t respond in any way, click any links, or open any attachments. Most email services have a method to report an email as spam. When in doubt, you can contact the sender via a trusted channel, such as a previously saved contact phone number. You can also access the service web address from your records.

Interest in open-source intelligence (OSINT) has grown over the last decade, both within the government and private sectors. Open-source intelligence (OSINT) is intelligence gathered from publicly available sources. These sources include blogs, news sites, and other publicly available websites. Anyone with reliable internet access, including journalists, researchers, and attackers, can conduct open-source investigations. You can easily collect OSINT without active collection methods, such as hacking or wiretaps.

Traditional forms of information gathering can be expensive, complex, and illegal. Examples of such approaches include hacking into private databases, conducting phishing email campaigns, and designing and deploying malware that tracks user activity. Conversely, open information can be considerably easy and even free to acquire. Another benefit of open-source intelligence is that it is usually undetectable to the target.

What if a journalist wants to determine a political party member’s location at any time? They can try to place a piece of malware on the person’s mobile phone illegally to acquire GPS coordinates. But monitoring the person’s social media account might be far simpler. All this approach takes is for one of the politician’s aides to post a location-tagged message or a photo with a recognizable landmark. Though this example seems simple, military units have used the same techniques to track their counterparts in foreign countries, and law enforcement has used them to track criminals and fugitives.

What if an attacker wants to gather information about the control systems inside a power plant? If they try to scan the power plant’s external network, the attacker might be detected, potentially compromising the secrecy of their infrastructure. Alternatively, the attacker might find a system engineer discussing sensitive plans on a blog. The blogging platform might have access records usable for identifying users such as the attacker. However, the company that owns the power plant would not.

Imagine that an attacker wants to collect basic information about an organization or person. Where might they start? Below are a few examples of common sources of open information.

Company website: A company’s website is an obvious source. Examining the type of information that the company chooses to make publicly available can be revealing. It can reveal helpful information such as points of contact, external social media profiles, and building addresses. And companies might mistakenly publish more details than they should. Attackers can augment searches with advanced search features, a practice often called Google hacking. This technique helps them find more advanced information and unintentionally revealed files. They can also explore options, such as the Wayback Machine, for retrieving a company’s legacy website. These tools can help attackers determine what a website was used for at certain times.

Media and news: If someone has already done the hard work, then why repeat the effort? Some good journalists are skilled at processing open information. An attacker is unlikely to find an article that contains all the information that they are looking for. Still, some articles will probably provide helpful information for further investigations. Other sources of pre-processed or foundational information might include industry analysts, rating agencies, and other assessing bodies.

Social media: People happily share information on social media, making it widely available. By piecing various bits of social media information together, attackers can get an accurate perspective about someone’s personal and professional lives. Some victims make this work too easy. For example, employees have been known to share photos of ID badges, network diagrams, and even sticky notes with passwords. Every small piece of information can add credibly to a social engineering attack. For example, consider an attacker that finds out that a target recently attended a conference. The attacker can create a convincing spear phishing email. It might say that the sender found the target’s name on the attendee list and wants to follow up.

Government or public records: Many countries keep detailed records of citizens and companies. These records can provide highly valuable information to attackers. For example, hospital records might list someone’s place and date of birth, and an electoral roll might list someone’s address. Other entities might have public records helpful for attackers. For example, many stock exchanges require that companies make a certain amount of financial information available.

Forums and discussion boards: Online platforms like Reddit, Quora, and technology-specific message boards might contain a plethora of helpful information. People often share expertise, experiences, and insights on these platforms, inadvertently disclosing valuable information about an organization’s people, technologies, or security.

Job posts: Job posts can contain various details helpful in planning an attack. For example, a post might list software that applicants must be proficient with, indicating that employees use this software. An attacker can research it for known vulnerabilities to help plan an effective attack. Other helpful information about the company can include proprietary technologies, upcoming projects, and organizational structure.

DNS records: An attacker can use various online tools to examine an organization’s DNS records. For example, WHOIS is a protocol that you can use to query databases that store registered users or assignees of an internet resource, such as a domain name. It provides information about the organization or person who registered a domain, including their contact details. Attackers might also discover subdomains that can reveal the organization’s network infrastructure.

Remember that attackers aren’t the only ones that use OSINT. For example, journalists and cybersecurity experts can use this research for beneficial purposes, such as criminal investigations. Anyone can do it, including you! How do you get started with open information research? As you become more experienced at gathering open information, you’ll learn plenty of tips and tricks. But the following guidelines provide a good starting point.

Get lots of information: Quantity is valuable. The more information, the better. Analyst tools that search for links between data sets operate better with more information. You never know what the key piece of information will be, so save everything initially before refinement.

Get a range: Build a picture from many perspectives. Not everything online is true. Don’t rely on a single source. Someone can easily falsify a single source, such as a social media profile with many flattering photos. However, falsifying multiple sources is much more difficult. You might discover that a target has deleted or attempted to conceal information. This very fact can be valuable.

Don’t get stuck: Be prepared to fail, and don’t get frustrated. Open-source intelligence is very powerful. But you’ll encounter many dead ends, and the amount and type of open information on a target depends somewhat on luck. You might need to take a different approach or explore a new area. Teams of trained researchers often need weeks to complete a successful investigation.

Often, open information is not obtainable. Some organizations and people will not have as much public information as others. Good operational security can be one reason why.

In our highly connected world, people overshare all the time. Everyone should be aware that what they share online is virtually permanent. Someone can combine a few small pieces of information to reveal something of external interest. This process is called information aggregation. Though your place of work, commuting information, and typical evening plans might be harmless in isolation, someone can combine them to map out your life.

Consider an organization in which 100 employees each reveal 1% of a sensitive piece of information. If an external party combines these disclosures, then they might make significant breakthroughs or discoveries.

When designing information management policies, organizations should consider the OSINT techniques that attackers employ. The bottom line is that information leakage harms organizations. Organizations must act to ensure that as little information as possible is unintentionally disclosed and made vulnerable to collection. Often, organizations have to make certain information publicly accessible, so they must take caution to avoid oversharing.

Technical scanning techniques play an essential part in an organization’s network administration and analysis. Think about how attackers collect information about computers and networks. While investigating a target device on a network, an attacker might want to learn more about the device’s technical configuration. They might try to find out information such as the following: What operating system is in use? What services are running on the device? Are any of the services vulnerable to well-known exploits? Some typical technical scanning techniques are: Ping test, Traceroute, Port scanning, Vulnerability scanning, Search engine for the internet, Network scanning.

A ping test measures the time that it takes for a packet to travel from one device or server to another. A packet, or ping, is a small amount of formatted data analogous to the digital version of a postcard. In a ping test, a scanning device sends an Internet Control Message Protocol (ICMP) packet to the target device’s Internet Protocol (IP) address. This outbound packet is called an echo request packet. If the target device replies with an echo reply packet, then the scanning device knows that the target device is most likely active and switched on.

A ping test indicates if a machine is responsive and when repeated in a sweep, how many devices are on a network. Organizations often use a ping test to debug networking issues. It identifies a device’s status. It also indicates how “far” into a network the device is located using a property known as a packet’s time to live (TTL). Every router that forwards the packet onwards decreases the time to live by one.

Consider a packet that starts with a TTL of 120. If it reaches the destination with 108 left, then it has gone through 12 stages. You can use this feature in the next scan. On Windows, you can run a ping test from the command prompt by using the following command: *ping target\_name*.

Traceroute is another network diagnostic tool. When you run a traceroute, the scanning device sends packets to the target device. These packets have either increasing or decreasing TTLs. When a packet is in transit, and its TTL decreases to zero, the device processing the packet sends back an error message to the scanning device indicating that the packet didn’t reach its destination.

You can use a traceroute test to map a network and determine how many routers and switches exist between you and your destination. A router is a network’s hardware connection to the internet. A switch integrates all the devices on a network, including the router, allowing for seamless sharing and data transfer among them.

Imagine a target is 12 hops away. If you send a packet with a TTL of 11 toward the target, the packet will fail at the final routing step. The scanning device will receive an error message packet, and this message will reveal the IP address of the device 11 steps away. As the TTL is reduced to one over a few new tests, the traceroute command produces a complete list of the network nodes between the scanner and the target. On Windows, you can run a traceroute by using the following command: *tracert target\_name*.

In networking, applications are accessible externally through services on digital ports. A port is a connection point that sends or receives data for a specific network service, such as email. Each port is assigned a number in the Transmission Control Protocol (TCP), a collection of internet protocols that make it possible to create and maintain communication between internet-connected devices. Each port is also associated with an IP address. The relationship between IP addresses and ports is like that between a building and its floors: an IP address is like a building, and port numbers are like different floors in that building.

The usual goal of port scanning is to identify a host’s open ports. A host is a device, such as a server, workstation, laptop, or other smart device, that can communicate with other devices on a network and grant access to devices outside the network. An open port is one that accepts a connection. Given that a port number is like a floor in a building, an open port is like a floor that you can access through an open door.

Attackers want to find and exploit open ports on hosts. Conversely, network administrators want to close or block these ports while ensuring that legitimate users still have access. The scanner reports that a port is closed if the port rejects the connection or filtered if the host gives no response to the scan. No response can mean that a package filter, a type of firewall, is blocking access to the port.

By working through the list of a host’s well-known ports, a scanner can often determine what the host’s owner uses the device for. The TCP contains 65,536 ports. TCP ports 0 through 1,023 are called well-known ports: each has a specific service associated with it, and this association is internationally recognized. Some ports from 1,024 through 49,151 might also have officially registered uses of interest.

HTTP web activity always occurs on TCP port 80. If a scan reveals that port 80 is open, the investigator knows that some web-based application might be using it. For another example, Windows file sharing occurs on TCP port 445. If attackers know this port is open, they might try to exploit it with malware. Famous ransomware attacks, such as the WannaCry attacks, have targeted this port. A notable port outside the list of well-known ports is TCP port 3389, the default port for the Microsoft Remote Desktop Protocol (RDP). If attackers know this port is open and available, they can try to hack the remote desktop software.

Another form of testing is vulnerability scanning. One of its features is dynamic scanning, which simulates hacking techniques, such as SQL injection, to discover vulnerabilities to exploit. Other standard vulnerability scanning techniques include version and OS detection: Version detection reveals the version numbers of software, such as Apache web server, running on the host. OS detection reveals the device’s OS, such as macOS.

Vulnerability scanning is a powerful tool for both organizations to identify vulnerabilities in their network and for attackers to find potential victims. Some organizations run such scans periodically to identify mistakes that need remediation.

A scanner might attempt to connect to a server and check if it is running an outdated version of an application. If the application is out-of-date with a known vulnerability, then the scanner might attempt to exploit the vulnerability to confirm its existence and report this finding.

Please be aware that dynamic scanning might automatically perform actions considered illegal in some countries. Scan a target only if the owner has given consent. A network vulnerability scan will often be interpreted as the planning stage of an attack.

Another tool for technical scanning is the Shodan search engine. Its website describes the tool as “the world’s first search engine for internet-connected devices”. It is of interest to both malicious attackers and security researchers. It offers a vast catalog of collected scan results spanning billions of records. People can use these stored records to track applications at scale around the world.

Network scans collect information about a network by targeting a host. Network and systems administrators rely on network scans to assess the status and security of their organization’s network. Unfortunately, cyber attackers can use these same tools for malicious purposes.

Many network scanning applications exist, but the most well-known scanner is Nmap. Nmap, short for Network Mapper, is a free, open-source network scanner available for Windows, macOS, Linux, and other OSs. Though port scanning is its core feature, Nmap provides other valuable features for investigating networks. It can reveal the network path from the scanning device to the host, including all other hosts encountered along the way. It can perform version and OS detection. It can even identify firewalls in use.

Nmap is a command-line program, but most versions also include Zenmap, the official graphical user interface (GUI) of Nmap. Zenmap makes learning Nmap easier for beginners. With Nmap, you must determine the precise command needed to perform your scan, and the number of options and syntactic requirements can make this challenging. But with Zenmap, you can simply select choices from a user-friendly interface to customize your scan. And if you still want to learn Nmap’s command-line options, Zenmap displays the actual Nmap command and options behind your scan.

Artificial intelligence (AI) has become valuable for network scanning. With machine learning (ML) algorithms, network scanners can perform deeper, more helpful analysis. Scanners can independently analyze and categorize network vulnerabilities. Scanners can prioritize vulnerabilities based on their severity. Scanners can learn from past scans and identify patterns and trends to anticipate future threats. AI can also streamline the scanning process. It can reduce the time needed to scrutinize large networks and reduce the possibility of human error.

An example of an AI-driven network scanning tool is IBM’s QRadar® Advisor with Watson™ application. It analyzes security incidents, identifies potential threats, and provides actionable insights. QRadar Advisor uses ML and AI to sift through vast amounts of data, investigating offenses and eliminating false positives. As a result, analysts are free to focus on confirmed threats, optimizing their time and resources.

When Stuxnet was identified in 2010, it was one of the most advanced and targeted malware collections observed within the security community. Attackers used Stuxnet to attack a specific industry control system and modify key settings. Experts have concluded that the culprits designed it to target centrifuges used within Iranian uranium processing, which is a precursor for nuclear bomb production.

This attack is interesting for several reasons. It was much more technically advanced than any previous malware. Stuxnet exploited four previously unknown security flaws. Cybersecurity professionals refer to such flaws as zero-day vulnerabilities. Also, the attack used a pair of compromised digital certificates and concealed itself at a very low level within computing systems. The malware spread through infected USB flash drives. A common mistake in cybersecurity is assuming that an adversary cannot introduce malware into the local network if a system is not connected to the wider internet. The malware’s authors were persistent. Their targeted campaign continued for months while they tweaked and upgraded the tools that they were using.

In many ways, Stuxnet was the definitive example of a cyberweapon deployed to achieve a tangible military and political objective. The incident made it clear to cybersecurity experts what they can expect for future cyberweapons.

The Los Angeles Unified School District (LAUSD), the US’s second-biggest school district, experienced a ransomware attack in 2022. This attack significantly impacted more than 1000 schools and 600,000 students. The ransomware kept LAUSD officials from accessing their systems and a great deal of critical data. Some examples of this data include Social Security numbers, login credentials, tax forms, legal documents, financial reports, health information, background checks, and student psychological assessments. LAUSD decided not to pay the ransom, following the guidance of cybersecurity experts and law enforcement for handling ransomware attacks. In response, the attackers, a Russian criminal group called Vice Society, released the data on the dark web.

This breach is one of the largest that the education sector has experienced. It demonstrates how attackers can exploit system vulnerabilities and disrupt the functions of critical public services. And LAUSD’s decision not to pay the ransom highlights the difficult choice that institutions face when dealing with ransomware. Overall, the breach exposed the need for robust cybersecurity measures in educational institutions.

In 2013, a US National Security Agency (NSA) subcontractor named Edward Snowden released a significant amount of classified information in the public domain through WikiLeaks. He could access the information because of his job role and with few technical tools and techniques.

When the files became public, the leak considerably impacted the US and its international allies. The leaked files included technical capability overviews, guidance on operations, and other highly sensitive material. As a result, several business arrangements between the NSA and US companies underwent rigorous scrutiny.

This case study is a well-known example of a malicious insider. Though the cost of the damages has not been made available publicly, the data breach is arguably the most damaging set of leaks that the US has ever suffered.

In April 2022, a former disgruntled employee at Cash App used Cash App Investing to download data from over 8 million users. Examples of data stolen include customer names, brokerage account numbers, stock trading portfolios, and stock trading activity. Alarmingly, the breach went undetected and unaddressed for four months. This case study shows the importance of strict access control policies for terminated employees. When parting ways with an employee, an organization should revoke the employee’s access privileges immediately. This example also demonstrates why organizations must rigorously monitor system activity. It ensures that if an incident such as this one occurs, the organization can identify and mitigate it quickly.

SolarWinds developed software used to manage IT systems, including a product called Orion. In 2020, researchers discovered that attackers had compromised SolarWinds and spread malware to thousands of SolarWinds’ customers. The attackers specifically compromised SolarWinds’ update process, so when customers updated Orion, they also installed the malware.

This attack is noteworthy because it highlights how prospective attackers can use trusted relations within supply chains. By compromising SolarWinds, the attackers gained access to thousands of other organizations.

Thankfully, large-scale supply chain attacks such as this one are rare. And even though the attack used the supplier’s software update process, cybersecurity experts still recommend patching software regularly.

Cybersecurity professionals categorize threat actors in five main groups: Script kiddie, Hacktivist, Criminal gang, Nation-state hacker, Malicious insider. The five main threat actor groups vary substantially in motivation, resources, and techniques. Some examples of common types of attacks include denial-of-service (DoS) attacks, malware, man-in-the-middle (MitM) attacks, and Domain Name System (DNS) attacks. With AI, attackers can enhance the structure and sophistication of their attacks in several ways, such as by automating the creation and dissemination of phishing emails. The Lockheed Martin Cyber Kill Chain® framework breaks down attacks into seven steps and helps cybersecurity professionals understand and prevent attacks. The MITRE ATT&CK matrix helps cybersecurity professionals identify an attacker’s tactics and techniques and anticipate the attacker’s next move. Cybercriminals often use cryptocurrencies because the currency is anonymous and typically decentralized, making transactions difficult for law enforcement agencies to trace. To defend against social engineering, organizations should focus on the three key elements of cybersecurity: education, process, and technology. Common signs of a phishing email include but are not limited to a generic greeting, unusual request, or suspicious link. Open-source intelligence (OSINT) is typically easier and cheaper to acquire than traditional intelligence. Common sources of OSINT include blogs, news sites, and other publicly available websites. Technical scanning helps both IT professionals and attackers assess the status and security of an organization’s systems and network. Lessons learned from high-profile cyber incidents guide future decision-making in cybersecurity.