50+ CYBER security threats

DIGITAL PANDA

50+ CYBER security threats

With recent data showing that the UK is the third most-targeted nation for cybercrime attacks, it's more important than ever to be aware of the tactics used by malicious actors.

In this ebook we've listed 50 of the top cyber security threats that need to be on your radar.

DIGITAL PANDA

Contents

DIGITAL PANDA

50 CYBER security threats

01. Account Takeover

Account takeover or ATO occurs when an attacker poses as a genuine user, customer, or employee of a business to gain entry to your accounts. In some cases, they'll speak to their victims directly to deceive them, but with the increase of user credentials on the dark web this step can be bypassed. Attackers can easily buy user credentials from the deep web or use bots or other tools to gain unauthorised access to accounts.

Once they're in, criminals can wreak all sorts of havoc, from transferring money to taking out new credit agreements or even claiming product replacements under warranties. The types of accounts most vulnerable to ATO attacks include:

- Online banking accounts
- Email accounts
- Social media accounts
- Gaming and entertainment accounts
- Government service portals
- Utility accounts

How does the attack happen?

Any account that requires login details is susceptible to an account takeover attack. Cybercriminals can access accounts by; purchasing user credentials from the deep web, using phishing techniques to steal credentials, brute force bots, and malware that tracks online activity.

Login information can also be accessed physically by 'dumpster diving' where personal details have been left in discarded mail and used to build a profile of the victim. In fact, it's not uncommon for full packages of identifying information to be sold on the black market.

Where does the attack come from?

Account Takeover attacks can originate from anywhere in the world. The market for login credentials is thriving online and can be sold all across the globe.

in the news

One of the most famous account takeover attacks happened to Fitbit in 2016. Bad actors were able to gain access to genuine user accounts when email addresses and passwords were leaked from third-party sites. Using these credentials, they falsely ordered replacement devices under the users' warranties.

02. Advanced Persistent Threat

An Advanced Persistent Threat or APT is a sophisticated, highly targeted and covert threat carried out by an individual or an organised group of cyber-criminals. These attacks require significant resources including security and development expertise, time, and money.

During an APT, the bad actors manage to 'break into' a system or specific computer using a variety of techniques, where they proceed to access protected and sensitive information.

How does the attack happen?

As the name suggests, APT attacks are advanced cyber-attacks carefully orchestrated by the attackers. It involves a mixture of typical techniques such as malware and phishing attacks combined with intelligence gathering to find a way into the protected system.

Attackers will usually start by targeting one computer and discovering which machines have different access levels allowing them to infiltrate the entire system. Once they've gained access to a computer, APT attackers also deploy backdoor programs (like Trojans) to ensure that access is maintained even if the login credentials are changed.

Where does the attack come from?

Advanced Persistent Threat attacks are usually carried out by organised crime groups or by hostile nation-states for political espionage purposes. The main objective is often financial gain or to access sensitive and restricted data.

Many APT attacks happen to organisations that hold classified or sensitive data such as government and financial institutions. APT attacks have also been used to steal intellectual property, infrastructure data and personal information & login credentials.

in the news

A well-known APT attacker is the group GhostNet. Originating in China GhostNet uses spear phishing emails that contain malware to infiltrate its targets. So far, the group has been able to gain access to computers in over 100 different countries turning them into covert surveillance devices by operating cameras and microphones.

03. Amazon Web Services Attacks

The rise of home working and cloud computing means more businesses using online environments like Amazon Web Services or AWS. As one of the largest cloud-service suppliers, it's no coincidence that Amazon is a primary target for cyber-criminals.

How does the attack happen?

The AWS model leaves room for mistakes with Amazon adopting a 'shared responsibility' method. Under this model, Amazon is responsible for protecting the host environment while the customer is responsible for protecting the guest operating system including updates and security patches.

Attackers are able to take advantage of deployment errors and misconfigurations to access data stored in AWS. Organisations are advised to be vigilant to prevent attacks and to take simple measures like spotting when an unfamiliar device from an unfamiliar location accesses the environment. Regularly reviewing activity and looking out for anything suspicious activity can help.

Where does the attack come from?

As we highlighted earlier Amazon is one of the largest suppliers offering a variety of cloud-services. Therefore attacks can originate from practically anywhere in the world.

in the news

One of the most recent examples of AWS attacks happened to Turkish flight operator Pegasus Airlines in March 2022. An investigation found that customer data was stored in an unprotected cloud storage bucket leading to a breach of almost 23 million files (around 6.5 TB of data) containing sensitive client information.

04. Application Access Token

Often used as part of an Advanced Persistent Threat attack, an application access token attack is used to manipulate higher-level access once a users system has been compromised.

How does the attack happen?

During an access token attack, the attacker will exploit vulnerabilities in a system to find access tokens that they can manipulate, allowing themselves higher-level access. This enables them to perform actions on behalf of the user they are impersonating or access sensitive data.

One of the ways an access token attack happens is through Open Authentication (OAuth) tokens often used for free webmail accounts like Gmail and Yahoo mail. These OAuth tokens can be used to bypass normal authentication processes and access restricted accounts. Once the attackers have access to the account through the OAuth token, they can perform functions such as email search and enumeration.

Where does the attack come from?

Attackers use access tokens to infiltrate other services. For example, performing forgotten password actions in other apps and services where that email has been used so they can log in and create new passwords.

As the attacker has direct API access normal protections such as multi-factor authentication and changing passwords can be easily bypassed.

in the news

In April 2022 hackers were able to use API keys to gain access to hundreds of Mailchimp accounts. Similarly, in January 2023 threat actors were able to gain access to Slack's GitHub repositories using a limited number of stolen Slack employee tokens. Using these they were able to access and download private code repositories.

05. Bill Fraud

Bill fraud happens when cyber criminals falsely create invoices or divert payments through a variety of means.

How does the attack happen?

Hackers have various ways to carry out bill fraud including.

- Phishing to gather personal details, credit card information, and logins.
- Pagejacking where criminals divert traffic away from an ecommerce site by hijacking part of it and sending traffic to a different website.
- Merchant identity fraud which allows criminals to create a merchant account in an apparently legitimate business name and then using stolen credit cards, process payments. The hackers and money will then quickly disappear before the fraudulent payments come to light.
- Scammers may also create fraudulent invoices using the logos and branding of real businesses to trick targets into thinking it is a bill for a service they have actually used.

Where does the attack come from?

Bill fraud can happen from anywhere in the world, although it is a more sophisticated attack that requires the ability to create genuine-looking emails and invoices.

in the news

In September 2022 during the UK's energy price hike a number of fake emails and texts were circulating, some designed to look as though they were from energy regulator Ofgem. Unfortunately, these fake communications fooled a number of people.

06. Brute Force Attack

A brute force attack uses automated tools to guess all password combinations until it finds the right ones. This is one of the simplest ways of gaining access to a user account but requires time and patience.

How does the attack happen?

Attackers will usually use automated tools to do the guesswork for them. However, there are also approaches such as the dictionary technique where hackers will systematically work through a dictionary or wordlist trying different combinations as they go.

Where does the attack come from?

As this is one of the least sophisticated attacks, they often come from inexperienced hackers with enough time and computational power to run the required software.

in the news

In 2018 the Northern Irish Parliament fell victim to a brute force attack. The attackers were able to access the mailboxes of assembly members by trying different passwords. The affected accounts were deleted and parliament members were told to change their passwords to more secure passphrases.

07. Business Invoice Fraud

Business invoice fraud happens when cyber criminals falsely create invoices or divert payments by creating realistic-looking fake invoices targeting businesses.

How does the attack happen?

Cybercriminals choose their targets and send fake invoices in the hopes that their victims won't notice they are being defrauded. They often use terminology to suggest the payments are overdue to rush victims into paying.

Where does the attack come from?

Many business invoice fraud attacks can be traced back to fraud rings that operate all over the world.

in the news

In 2013-2015 Evaldas Rimasauskas posed as an employee of legitimate company Quanta Computer. He emailed fake invoices to Facebook and Google over the course of two years causing them to pay him over $120m before he was arrested and charged with fraud, money laundering, and identity theft.

08. Cloud Access Management

Moving systems to the cloud has been beneficial for many businesses, especially during Covid-19 where remote and home working became the norm. However, with these added benefits comes increased risk.

Cloud access management can be particularly vulnerable to human error and needs to be monitored diligently.

How does the attack happen?

Cloud access management breaches usually occur where there is a lack of security protocol or poor communication between employees. Once the attacker manages to find a way into your cloud environment, they can find ways to access other remote entry points locating unprotected databases or insecure apps.

They can then access and steal data without being noticed until it is too late.

in the news

The largest data leak in China occurred when attackers were able to steal the data of more than 1 billion Chinese citizens from a Shanghai police database. They were able to gain entry through a database hosted by Alibaba Cloud (a subsidiary of Alibaba) through a management dashboard that was accessible via the open internet.

09. Cloud Cryptomining

Mining or creating cryptocurrencies needs a lot of computer power. It was intentionally designed like this to ensure the creation of new blocks remains steady. However, the resource-heavy nature of crypto mining has created a black market for computational power, where hackers hijack or 'cryptojack' the computer power of large enterprises.

How does the attack happen?

The wider public first heard about cryptojacking in 2017 when the mainstream media began to report on its rise in popularity. During this time, criminals were targeting mobile phones, home computers and laptops. However, with an increase in cloud services, cybercriminals have now moved their target to enterprise services such as Amazon Web Services, Google Cloud Platform (GCP) and Microsoft Azure.

When this happens, the impact can be devastating. Undetected hackers can quickly add hundreds of new instances to an account resulting in crippling bills, often reaching tens of thousands of pounds in fraudulent usage.

Where does the attack come from?

Cloud crypto mining attacks can come from anywhere due to the decentralised nature of cryptocurrency.

With these attacks being notoriously difficult to detect, the best course of action is to carefully monitor any cloud environments for suspicious activity. For example, an unusually higher number of new instances, access from previously unknown regions, and compute instances started by unknown users.

in the news

In 2018 the website of Manchester City Council was infected with a code that mined the open-source cryptocurrency Monero. Other affected sites included NHS bodies and other UK councils. This prevented certain services and websites run by the council from working causing disruption for citizens.

10. Command and Control

During a command and control attack, a hacker will remotely take control of a computer to bring down other systems in the network through commands or malware. These attacks, also known as C2 and C&C, can also occur secretively, allowing attackers to infiltrate networks unseen and gather sensitive information.

How does the attack happen?

A command and control attack originates from an already compromised machine. To gain access to this first machine attackers will use tactics like phishing emails, Malvertising, vulnerable web browser plug-ins, or through directly installing malware on a machine.

The infected device then executes commands coming from the attacker which often includes the installation of even more malware. From there, hackers are able to target other computers on the network, building a 'bot-net' of infected computers.

Where does the attack come from?

Command and control attacks can happen on any device including desktops and laptops, tablets, smartphones, and IoT devices. Notable attacks have come from Russia and Iran, but can originate from anywhere in the world.

in the news

In 2013, tech-giant Apple was hit with a command and control attack that affected a small number of computers on its Cupertino campus. The attackers were able to exploit a java vulnerability to gain access to the machines.

11. Compromised Credentials

Many accounts still rely on user access with a single username and password, leaving them vulnerable to attacks. Credentials can be found through the deployment of password sniffers, malware attacks, and phishing attempts.

How does the attack happen?

The basis of a compromised credentials attack is unauthorised access to a legitimate account. Once bad actors have access to these credentials they can infiltrate password-protected devices, and networks undetected with ease.

Where does the attack come from?

Attackers usually have a motive to target specific organisations, often to gain access to restricted data. However, in terms of location, these attacks can come from anywhere in the world.

in the news

Recently Crossword Cybersecurity's Trillion risk monitoring service found the stolen credentials of 2.2 million breached credentials linked to the UK's top 100 universities for sale on the dark web. This means the data of staff, students and employees was left at risk

12. Credential Dumping

Credential dumping or password dumping is an attack that targets a system to gather login credentials such as usernames and passwords. Even if these credentials are encrypted, attackers can use their own systems to decode the encryption and access the protected information.

How does the attack happen?

Credential dumping attacks usually happen through compromised devices or systems. For example, if an attacker has access to a device they can easily find stored credentials within the Random Access Memory or RAM.

Credential dumping attacks can cause serious problems when user accounts with additional privileges are compromised. These accounts often have access to sensitive information or system controls and hackers can use these to disrupt systems and steal data.

Where does the attack come from?

Stolen credentials are a popular listing on the dark web and are purchased by criminals all around the world. Credential dumping attacks are common and can come from almost anywhere.

in the news

Recently, an estimated 35,000 PayPal accounts were impacted during a credential dumping attack in December 2022.

13. Credential Reuse Attack

Following on from a credential dumping attack is the credential reuse attack. Once malicious actors have obtained user credentials, they can use them to compromise other systems. That's why we always advise our customers never to use the same username and password for different accounts.

How does the attack happen?

Once the attackers have obtained valid credentials for one system, they will try the same username and password on other systems. Usually targeting bank accounts and other consumer accounts.

To find the first set of credentials, cybercriminals use phishing techniques including emails or websites that look legitimate to trick users into entering their login information.

Where does the attack come from?

Credential reuse attacks happen when cybercriminals have sold compromised credentials to other attackers and can originate from anywhere in the world. However, they can also come from targeted attacks either from an organisational level or a personal level where an attacker wants access to specific accounts for personal, financial, or professional reasons.

in the news

In April 2020 just as the world was adapting to remote working as a result of the coronavirus pandemic, Zoom suffered a credential reuse attack. A massive 500,000 usernames and passwords were exposed on the dark web.

14. Credential Stuffing

Credential stuffing is the same as credential reusing but on a much larger scale. The attack uses bots to take stolen credentials and use them on multiple different services.

How does the attack happen?

Credential stuffing attacks rely on victims using the same login details to access multiple accounts. Hackers can easily buy stolen credential lists and automation bots to try these credentials elsewhere until they get a hit.

It's estimated that around 0.1% of compromised credentials will allow criminals to log into another service.

Where does the attack come from?

Credential stuffing attacks mostly come from cybercrime hotspots and can be carried out by individuals or organised criminal organisations. Sophisticated attackers use proxies to hide their location so it can be hard to track them down.

in the news

In 2012, Spotify suffered two credential-stuffing attacks, with the second compromising over 100,000 user accounts.

15. Cross-site Scripting

Cross-site scripting or XSS attacks are insidious attacks used to infiltrate benign and trusted websites. Attackers inject malicious code into these sites which executes in a visitor's browser, allowing the bad actors to access user cookies, read session IDs, change the content of the affected website, or even redirect users to another site.

How does the attack happen?

Cross-site scripting attacks take advantage of vulnerabilities in web applications that generate input from a user without validating or encoding it. Unfortunately, these vulnerabilities are widespread and because the user's browser believes the code has come from a trusted source it automatically executes the script.

Once the scripts have been executed, they're able to gain access to cookies, session tokens, and other sensitive information stored within the browser. In some cases, the scripts can even change the content within the HTML page.

There are two types of XSS attacks: stored and reflected. Stored attacks are more damaging because the malicious script is injected into the server. These attacks are usually found on websites that allow users to share content such as forums and social media sites. Then every time the infected page is viewed, the script infects the user's browser.

A reflected XSS attack, the malicious script is provided to the user in response to a request. For example through a search results page.

Where does the attack come from?

Cross-site scripting attacks were very common, however, with advances in browser technology and security, their numbers have fallen. Although they are still within the top ten cybersecurity threats according to the Open Web Application Security Project.

in the news

In 2019, the popular multi-player game Fortnite fell victim to an XSS attack. Hackers were able to infiltrate the game through an unused and unsecured page gaining unauthorised access to the data of game players.

16. Cryptojacking

Mining for cryptocurrency takes a lot of computer power and one of the easiest ways for cybercriminals to gain the necessary amount of power is by cryptojacking computer systems. During a cryptojacking attack, devices including computers, laptops, tablets, and even smartphones are hijacked for their processing power.

How does the attack happen?

Cryptojacking attacks occur when malicious actors secretly use a victim's computing resources to mine cryptocurrencies without their consent. Typically, these attackers infect a target's device with malware, often through infected websites, malicious email attachments, or software vulnerabilities.

Once the malware is deployed, it runs in the background, consuming the victim's CPU and electricity to perform complex cryptographic calculations required for cryptocurrency mining. The mined coins are then sent to the attacker's wallet, all the while degrading the victim's device's performance and potentially causing damage.

Where does the attack come from?

Cryptojacking attacks can be deployed from anywhere in the world and require little to no technical skill. Crypojacking software is available on the dark web for under $30 with full instructions on how to use it.

Attacks are likely to come from within organisations as well as outside. If an employee has access to a business server or special permissions on the network they can easily install the necessary malware.

in the news

In one example, cyber security software company DarkTrace detected crypto mining software within an anonymous organisation's network. Upon further investigation, the activity was traced to one of their warehouses where they found a collection of what appeared to be empty cardboard boxes sitting on a shelf.

However, upon closer inspection, these cardboard boxes contained a cryptocurrency farm running off the company's network power.

17. Data From Information Repositories

A "Data from Information Repositories" attack, sometimes referred to as a "Data Exfiltration" attack, is a type of cybersecurity breach where unauthorised individuals or entities gain access to sensitive or confidential data stored in information repositories or databases.

These repositories can include databases, data warehouses, cloud storage, or other data storage systems. Because these data repositories often have large user bases it can be difficult to detect unauthorised users.

How does the attack happen?

The attackers exploit vulnerabilities in the security measures protecting repositories to access, steal, or manipulate the data for malicious purposes, such as theft, extortion, or espionage. These attacks can have serious consequences, including data breaches, privacy violations, and financial losses, so they should be of significant concern for organisations storing valuable information.

Protecting data from such attacks often requires robust security measures, including encryption, access controls, and regular security assessments.

Where does the attack come from?

These attacks are largely co-ordinated by groups such as APT28 targeting government agencies, telecoms and IT companies. However, they can also come from individual and opportunistic attackers, as well as from employees working within a company.

in the news

Fox Kitten, a threat actor with suspected links to the Iranian government has been active since 2017 targeting the Middle East, North Africa, Europe, Australia, and North America. Targets have included multiple industries such as oil and gas, technology, government, defence, healthcare, manufacturing, and engineering.

18. DDOS Attack

During a DDOS attack a website, network, or online service is brought down by overwhelming it with a large amount of traffic.

How does the attack happen?

This is a brute force attack where hackers, hacktivists, or cybercriminals attempt to disrupt a website's usual performance either slowing it down or taking it offline completely. Targets include popular websites, financial sites such as banks, and news and government websites.

Where does the attack come from?

DDOS attacks are targeted attacks that originate from numerous distributed sources that are almost impossible to trace. This makes it hard to identify and stop the attacks before they happen.

in the news

In February 2023, what is believed to be the largest ever DDOS attack was launched at CloudFlare an American IT services company with customers including Tinder, Lyft, and Udemy. The attack registered a massive 71 million requests per second (54% higher than the previous record of 46 million RPS) The targets of these attacks included a popular gaming service, several cryptocurrency companies, hosting providers, and cloud computing platforms.

19. Disabling Security Tools

There are many options on the market to protect against cyber threats, from firewalls to End-Point security tools. But what happens when the attackers use the very tools meant to protect to cause harm? That's what happens when a disabling security tools strategy is used.

How does the attack happen?

The plan of attack is to prevent security tools from doing their job so it's easier for threat actors to gain unauthorised access to a device and carry out malicious activity. Hackers have several ways to do this, including disabling or overwhelming detection systems like firewalls and endpoint security tools. They can also attempt to bypass systems completely, or even take advantage of vulnerabilities in unpatched systems.

Where does the attack come from?

These attacks can come from anywhere and can target any type of security tools.

in the news

One of the most famous examples of this attack strategy is the Novter or Nodersok attack targeting Microsoft Vista's inbuilt security tool Windows Defender. This was a Trojan attack that took down the Windows protection features and then downloaded malware to the system.

20. DNS Amplification

DNS amplification is a form of DDOS attack that increases the severity and amount of damage done. These attacks have been around for almost as long as DDOS attacks, but they are becoming increasingly sophisticated and more harmful.

How does the attack happen?

Attackers trick vulnerable open DNS servers into sending massive responses to the target's IP address by pretending to be the target. This floods the target with traffic leading to a slowdown or even a full shutdown of service.

Where does the attack come from?

Similar to DDOS and DNS hijacking attacks, these attacks can come from anywhere in the world. With the relatively small amount of effort required to be successful, they can also come from solo hackers just as easily as organised criminal networks.

in the news

In 2020, Amazon Web Services (AWS) was hit by a huge DDOS attack targeting an unidentified customer. The attack used a technique called Connectionless Lightweight Directory Access Protocol (CLDAP) reflection and was able to amplify the amount of data sent to the victim's IP address by 56-70 times. It does this by using vulnerable third-party CLDAP servers.

This attack lasted for three days and peaked at a huge 2.3 terabytes per second.

21. DNS Hijacking

DNS hijacking, also known as DNS redirection or DNS poisoning, is a malicious attack during which an attacker takes control of a Domain Name System (DNS) server to redirect DNS queries to a different, often harmful, destination.

How does the attack happen?

The DNS system works in a similar way to a phone book. It translates human-friendly domain names (like www.example.com) into IP addresses (like 192.168.1.1) that computers use to locate and connect to websites and online services.

However, DNS is known for its vulnerabilities and is often prone to attack. This is because it is a distributed service that relies on connections between millions of clients and servers using insecure protocols.

Where does the attack come from?

DNS hijacking attacks can have various purposes, such as phishing, spreading malware, intercepting communication, or simply causing disruption. Therefore, it is hard to point to one specific type or person or group likely to carry out hijacking attacks.

in the news

In 2013, The Syrian Electronic Army made up of hacktivists who were loyal to Bashar Al-Assad were able to gain access to the domain name of the New York Times. They set it to map to a Russian hosting service instead which delivered a defacement message stating the site had been hacked by the Syrian Electronic Army.

22. DNS Tunnelling

A DNS tunnelling attack is another way hackers are able to abuse insecure DNS connections. The attack gets its name from the hackers using the DNS to bypass, or tunnel under, security systems.

DNS tunnelling itself is not inherently bad and is in fact used for legitimate purposes such as anti-virus software that updates customers' malware profiles in the background. However, it is a system that can be easily taken advantage of by bad actors.

How does the attack happen?

DNS is not designed for data transfer and so the majority of the traffic passing through is unmonitored. This enables attackers to add malicious data into a DNS query and redirect traffic to their own server which creates a connection with the targeted network.

Once this connection is active, the threat actors can then initiate other attacks including command and control, and data exfiltration.

Where does the attack come from?

DNS tunnelling is one of the most common cyberattacks and there are tools readily available across the web. However, it does require the hacker to have in-depth knowledge if they wish to access secure systems.

in the news

xHunt, a group targeting government organisations in the Middle East was found using a backdoor called Snugy. This used DNS tunnelling to communicate with its C2 server giving access to various systems.

23. DoS Attack

Dos attacks also known as Denial of Service aim to cause disruption to their victims by taking a website or service offline by overloading it with traffic and information. These attacks are very common and it's estimated that a third of businesses have been targeted with DoS attacks.

How does the attack happen?

One of the main ways DoS attacks are deployed is by flooding or crashing a targeted network. In these flood attacks, targeted networks are bombarded with more traffic than they can handle, causing them to slow down or shut down completely.

Other avenues for DoS attacks involve exploiting vulnerabilities in the system with malware that causes them to crash or stop working.

Where does the attack come from?

DoS attacks are usually targeted at larger corporations, financial institutions, and government services. They can come from anywhere in the world and attackers can easily mask their locations to evade detection.

in the news

The first recorded DoS attack happened in February 2007 when 16-year-old Canadian hacker 'Mafia Boy' unleashed a series of DoS attacks against sites including Amazon and Ebay. The disruption caused an estimated $1.7 billion in damages and Mafia Boy was arrested and sent to juvenile detention.

24. Drive-by Download Attack

A drive-by download attack infects a user's device by downloading malware without their knowledge or consent. It usually happens when unsuspecting visitors land on a website or page that has been compromised.

How does the attack happen?

Drive-by attacks exploit vulnerabilities in web browsers, browser plugins, or the underlying operating system to deliver and execute malicious code on the victim's system. The attack gets its drive-by name as the malicious code is designed to start downloading onto a device when the victim visits the site without their knowledge. Users don't need to open a malicious email, download, or click anything to become infected.

Cybercriminals use these attacks to steal and collect personal information. To avoid falling victim to these attacks we recommend staying up to date with software and system upgrades which usually include patch fixes for identified vulnerabilities. You should also steer clear of insecure or malicious websites.

Where does the attack come from?

Drive-by download attacks can come from anywhere, especially with the increase in the sale of drive-by download attack kits on the dark web. This makes it easy for hackers of all levels to use these attacks so it's vital to protect yourself as much as possible.

in the news

In 2016, the England V Iceland football match at the European Football Championships was one of the most tweeted-about events, attracting 2.1 million users. Cybercriminals took advantage of Twitter's automatic link-shortening feature to disguise malicious links to sites that enabled drive-by download attacks.

25. Insider Threat

As the name suggests, this type of attack comes from within an organisation and is one of the most difficult types of threat to protect against.

How does the attack happen?

Insider threats come from malicious actors who already have authorised access to a system, network, and resources. Whether it is a disgruntled employee, or a threat actor posing as a contractor, third party or remote worker, these insider attacks are hard to detect and prevent.

With the privileges granted to them with legitimate intentions, malicious insiders often have access to important systems or data, making it easy for them to get around security controls, steal data, and disrupt a business.

Where does the attack come from?

Insider threats come from individuals who have authorised access to a system or network. These individuals could be acting alone and out of revenge or for self-gain, or they could have links to malicious nation-states, crime organisations or even competitors.

in the news

In 2017, an employee at UK-based Bupa copied and deleted sensitive data from the healthcare company's CRM system. He then went on to sell the data on the dark web, compromising the personal data of nearly 550,000 Bupa customers.

26. IoT Threats

Smart devices, like cameras, thermostats, or even your fridge, are vulnerable to hackers. Their internet connectivity leaves an avenue for hackers to snoop on your data, control your devices, or use them to launch cyberattacks.

There are currently 1.3 billion IoT devices around the world, a number expected to increase to 30 billion by 2030.

How does the attack happen?

IoT devices often lack robust security measures, leaving them vulnerable to hackers. Threat actors can exploit these devices with malware, DDoS attacks, and ransomware. IoT devices can also be used in social engineering attacks with cyber criminals using them to monitor users and steal classified or personally identifying information, and other data.

Where does the attack come from?

As they're easily carried out over the web, IoT attacks can come from anywhere. However, with government, healthcare and manufacturing organisations using IoT technology, many are falling victim to attacks from hostile nation-states and organised criminal groups.

in the news

In March 2021, cloud-based surveillance software Verkada was hacked, giving cybercriminals access to over 150,000 cameras in factories, hospitals, schools, prisons, and other sites.

27. IoMT Threats

Similar to an IoT threat, an IoMT or Internet of Medial Things attack targets connected devices being used for medical purposes.

How does the attack happen?

IoMT devices are being used to transform healthcare. They can aid diagnoses, treatment, and care for a range of health conditions helping to improve patient health and wellbeing. However, just like IoT devices, connected medical devices are also prone to vulnerabilities.

IoMT breaches can occur through a lack of robust security measures, buggy or unpatched software, or through compromised devices and networks.

Where does the attack come from?

IoMT attacks are usually targeted at healthcare organisations using out-of-date systems and devices. Unfortunately, many medical settings rely on outdated equipment and software due to a lack of resources and the fact that digital technology quickly outpaces physical technology. Add into this the realisation that manufacturers typically don't allow customers to troubleshoot and patch their own devices and you have the perfect conditions for a cyber-attack.

in the news

In the Spring of 2017, a new ransomware attack spread around the globe infecting an estimated 200,000 computers in 150 countries. Amongst those affected was the NHS which was brought to a standstill for several days as the ransomware affected hospitals and GP surgeries across England and Scotland.

Following this lawmakers have highlighted the importance of taking the right cybersecurity precautions within a medical setting.

28. Macro Viruses

Macros are small programs or scripts embedded within software applications, such Microsoft Office programs like Word, Excel, and PowerPoint. These viruses exploit macro scripting capabilities to carry out malicious actions on a computer, such as damaging files, stealing data, or spreading to other documents.

How does the attack happen?

Macro viruses were more prevalent in the past, primarily in the 1990s and early 2000s, and they often targeted Microsoft Office documents. That's why it's long been advised not to open suspicious attachments or documents from senders you don't know.

Macro viruses are spread through phishing emails which impersonate legitimate users. Once opened and executed, the macro virus can spread to every file stored on the compromised computer. As they run on applications and not operating systems, macro viruses can be easily spread.

However, most anti-virus programs now detect macro viruses, so they are becoming less common today.

Where does the attack come from?

Whilst macro viruses aren't as prevalent as they once were, it's still a threat to be taken seriously. Macro virus attacks can come from any attacker with an internet connection and the ability to follow instructions.

in the news

Perhaps the most famous example of a macro virus was the Melissa virus which first appeared in March 1999 and considered the fastest spreading virus of its time. Once it had infected a user's computer, the virus would send itself via email to the first 50 people in the victim's address book: repeating the process and claiming more victims.

29. Malicious PowerShell

PowerShell is a command-line and scripting tool built on .NET by Microsoft. It's used by system administrators to automate tasks and change system settings. However, bad actors were quick to realise that many companies do not monitor these code endpoints leaving themselves vulnerable to attack.

How does the attack happen?

In a malicious PowerShell attack, the hacker is able to use PowerShell scripts or commands to execute unauthorised actions on a victim's device. Once the attacker has access to PowerShell they can spread malware, steal data, or gain control of an entire system.

Attackers usually send phishing emails that include malicious attachments, which execute encoded or obfuscated PowerShell commands intended to install further malicious code.

Where does the attack come from?

Only experienced hackers can perform malicious PowerShell attacks and get away with it. An attack like this requires the knowledge to get into the system undetected and to ability to cover their tracks to remain unnoticed.

in the news

In April 2023, it was reported that over 76% of ransomware attacks involved PowerShell. One such example included an attack by the Vice Society threat group which launched a custom-built, automated Microsoft PowerShell script to exfiltrate data from a victim's network.

30. Man-in-the-Middle Attack

A man-in-the-middle attack (MiTM), also known as an Adversary-in-the-middle (AiTM) is a difficult attack to detect. During these attacks, hackers use phishing tools to steal login credentials and session cookies, which allow them to bypass security measures like multi-factor authentication.

How does the attack happen?

With pre-built phishing kits and the implementation of HTTPS Everywhere, Man-in-the-middle attacks could be launched by anyone. However, with improvements in cyber security technologies, it is harder to execute these attacks effectively.

Therefore, they're usually commissioned by hostile nations or organised crime groups targeting specific organisations.

Where does the attack come from?

During an MITM attack, the hacker sets up a proxy server that creates a gateway between the user and the service they are logging in to. This allows the bad actor to intercept sensitive send and receive data with both parties being unaware of the intrusion.

31. Masquerade Attack

Just as the name suggests, a masquerade attack involves cybercriminals masquerading or impersonating a legitimate system user to gain unauthorised access to a computer, network, or data.

How does the attack happen?

Masquerade attacks happen when malicious actors use forged or stolen login credentials to gain unauthorised access to a system. These attacks can quickly escalate if the compromised account has a high level of access permissions, giving the attacker advanced access.

Where does the attack come from?

Attackers can steal user login credentials by spoofing login domains or using keyloggers to record login details. Masquerading attacks can also happen in person, for example by taking advantage of unguarded computers.

in the news

In 2013, Target suffered a huge data breach which compromised the data of 70 million customers. Attackers stole the credentials of HVAC contractor Fazio Mechanical Services, giving them access to Target-hosted web services dedicated to vendors.

After accessing Target's web services, the attackers exploited a vulnerability and used a technique known as 'pass the hash' which allowed them to impersonate the Active Directory administrator. With this, they created a new domain admin account and added it to the Domains Admin Group, which enabled them to steal the payment details and personal information of Target customers.

32. Meltdown and Spectre Attack

Meltdown and Spectre attacks are two highly publicised security vulnerabilities that were disclosed in 2018. What makes these attacks different to other attacks? They target computer hardware, specifically the processors.

How does the attack happen?

Both Meltdown and Spectre take advantage of vulnerabilities in modern CPUs, giving attackers access to data located in memory storage. Meltdown refers to the breakdown of the protective barrier that lies between an operating system and a program. Whereas Spectre is a breakdown between two applications designed to keep information from each other.

These attacks can target any device with a processor, not just laptops and computers. This means tablets and smart phones are also at risk.

Where does the attack come from?

It's not possible to pinpoint an exact location or threat actor responsible for these attacks as they can come from anywhere. As an attack that is relatively new on the scene, most of the research into the Meltdown and Spectre attacks has been focused on how they work instead of where they come from.

in the news

When the Meltdown and Spectre attacks were first identified by researchers in Google's Project Zero it came with the realisation that anybody with a PC, smartphone, or tablet is at risk. Essentially, every device with Intel processor chip made after 1995 is affected.

33. Network Sniffing

Network sniffing or packet sniffing, refers to the process of intercepting and analysing network traffic to eavesdrop on unencrypted data including credentials, emails, passwords, and other sensitive data.

How does the attack happen?

Network sniffing is easily accessible to attackers of all abilities with network sniffing devices freely available for purchase. A sniffing device is placed on a network through the installation of software or hardware that is plugged into a device which allows the sniffer to intercept and log all traffic passing between the host device and the wired or wireless network.

Where does the attack come from?

Network sniffing is often performed legally by network administrators and security professionals to monitor and troubleshoot network issues, identify security threats, and analyse network performance. However, in the wrong hands it can be easily used for more nefarious purposes.

Network sniffing is a tactic used by hostile nations and criminal groups to access sensitive data and spy on governments and organisations.

in the news

In 2009, US electronic payments processor Heartlands Payments Systems was hit by a data sniffing attack that cost $12.6 million in damages. Attackers were able to sniff sensitive cardholder data crossing Heartlands network.

34. Open Redirection

An open redirection attack or host redirection is an attack that's been around for a while. However, attackers are now creating smarter, more convincing ways to get their victims to fall for these simple yet highly effective attacks.

How does the attack happen?

Attackers attempting a host redirection attack will use a variety of phishing techniques to convince targets that they're using a legitimate website or service. They use emails and messages from already compromised accounts, embedded URLs, and .htaccess files to fool unsuspecting users into entering sensitive data and credentials.

The attackers rely on uninformed internet users who won't notice small discrepancies in the URLs they are using.

Where does the attack come from?

Due to the simplicity of the open redirection attack, almost anyone can do it. Therefore, it is a threat that can't be pinpointed to one location, organisation, or hostile state.

in the news

In 2021, phishing prevention company Pixm discovered a large-scale host redirection scam. Attackers used a compromised Facebook account to send DM's to other users. The link took viewers through a series of redirects, often landing on malvertising pages, and ultimately landing on a fake Facebook campaign.

This host redirect attack is believed to have tricked 2.7 million visitors into viewing it in 2021 and 8.5 million in 2022.

35. Pass the Hash

During a pass-the-hash attack an attacker captures and uses the hashed password of a user account to gain unauthorised access to a computer or network. A password hash is an encrypted version of your password and the same password will always generate the same hash.

How does the attack happen?

Pass the hash attacks are dangerous because they bypass the need to crack the victim's actual password. Even if the password is strong and secure, if the attacker is able to get hold of the password hash they can use it to access systems.

This is because systems using NTLM authentication rely on a hashed response to a password challenge instead of the cleartext password. So, if the bad actor has both the username and the hashed password, they can easily gain unauthorised access.

Where does the attack come from?

To successfully carry out a pass the hash attack a high level of skill is required. We mostly see these types of attacks coming from large criminal groups or malicious states with a clear target in mind. Using these attacks they can access sensitive information for political or financial gain.

in the news

In April 2022, a well-known ransomware-as-a-service group called Hive used pass the hash techniques to attack a number of Microsoft Exchange Server customers targeting those in the financial, healthcare, energy, and not-for-profit sectors.

36. Phishing

Phishing attacks rely on tricking unsuspecting internet users by mimicking emails, texts, and even phone calls from trusted sources.

How does the attack happen?

Phishing attacks are becoming ever more sophisticated with fraudsters producing convincing lookalike emails and even websites. The aim of the game is to trick victims into entering login credentials and other sensitive information into these fake sites, allowing criminals to collect this information.

Sometimes the sites also contain malware that malicious actors can use to cause further damage.

Where does the attack come from?

Phishing attacks were once commonly known as 419 attacks after the criminal code given to them by the Nigerian authorities. This was because such a large amount of them were found coming from Nigeria.

However, today they're just as likely to come from other countries such as Brazil, Russia, China, and India. With phishing kits also a top-selling product on the dark web, it's an easy attack for any bad actor regardless of skill.

in the news

In 2016 Belgian bank Crelan lost $70 million to a phishing attack after an employee was convinced to send money to unknown bank accounts following an email believed to be from the company's CEO.

37. Phishing Payloads

Phishing payload attacks use phishing methods to encourage victims to click on links that deliver malicious code or software to their devices. The purpose of the attack is to compromise the victim's system, steal data, or establish a foothold for further malicious activities.

How does the attack happen?

The attacker starts by sending a phishing message, often via email, but it can also be through other communication channels like text messages, social media, or instant messaging. The message is designed to appear legitimate and may include a malicious link or attachment.

Within the phishing message is a hidden payload in the form of malware (such as a virus, ransomware, or trojan) or a link to a compromised website. When the recipient interacts with the payload by clicking on a link or opening an attachment, the malicious code is executed on their system. This results in the installation of malware, data theft, system compromise, or other forms of unauthorised access.

Where does the attack come from?

Phishing is prevalent around the world and requires very little technical skill to execute effectively. It is an attack that relies on tricking the victim into believing they are interacting with a trusted source which has either been convincingly cloned or compromised.

in the news

In 2014, Russian hacker group Dyre posed as tax consultants convincing thousands of victims to download malicious executable files resulting in a loss of millions of dollars. Victims included Ryan Air, Sherwin-Williams, and engine parts manufacturer Miba.

38. Spear Phishing

Phishing payload attacks use phishing methods to encourage victims to click on links that deliver malicious code or software to their devices. The purpose of the attack is to compromise the victim's system, steal data, or establish a foothold for further malicious activities.

How does the attack happen?

Attackers gather information about their targets and create highly convincing, personalised messages to trick them into clicking on links or revealing sensitive information. The goal is usually to steal valuable data, access networks, or deliver malware. These attacks are more sophisticated than generic phishing attempts and are highly effective due to personalisation.

Where does the attack come from?

As spear phishing attacks are personalised and targeted, they can often be traced back to state-sponsored cyber crime groups with a financial or political incentive.

in the news

Networking firm Ubiquiti lost $46.7 million after criminals used a spear phishing campaign to spoof communications from executives that lead to unauthorised international transfers. The cyber thieves targeted and managed to fool executives in the firm's finance department.

39. Whale Phishing (Whaling)

Where phishing campaigns target multiple individuals and organisations, whale phishing attacks target one highly valuable victim instead.

How does the attack happen?

Whale phishing targets high-profile individuals within an organisation, such as top-level executives, senior management, or individuals with significant authority or access to sensitive information. They're called "whales" because of their importance and access levels within an organisation.

Whale phishing shares many characteristics with traditional spear phishing but focuses on top-level targets who may have the authority to make significant financial decisions or access highly confidential information. Attackers craft personalised and convincing messages to trick these high-value individuals into clicking a link that contains malicious code or direct them to a website where they're encouraged to add sensitive information.

Where does the attack come from?

Whaling attacks can come from anywhere in the world and as they use the same tactics as phishing scams, can be carried out by anyone.

in the news

In 2015 Barbie toy manufacturer Mattel fell victim to a whaling attack that originated from China and cost the company almost $3 million. Attackers posed as newly appointed CEO Christopher Sinclair to ask a finance executive to send the money to a Chinese bank account.

The criminals had timed the attack to take place during a period where a new CEO had been introduced and the company was expanding in China, so the payment request wouldn't look out of place.

40. Privileged User Compromise

Compromised privileged user accounts are often the gateway to larger-scale network, system, or application attacks, and one of the hardest attacks to detect. Privileged accounts typically have extensive permissions, allowing their users to perform critical and sensitive tasks, such as system administration, data access, and configuration changes.

How does the attack happen?

There are various ways for attackers to compromise a user account with valuable privileges. Malicious actors can gain unauthorised access to an account through stolen credentials, weak passwords, or exploiting vulnerabilities in the system. They might use targeted spear-phishing attacks, malware, or pass the hash attacks to compromise the account.

In some cases, where an attacker has compromised a lower-level account, they're able to exploit security weaknesses to elevate the account to that of a privileged user.

Where does the attack come from?

Because of the myriad ways a privileged user account can be compromised, and the actions that can be performed with these accounts it's hard to point to a specific group responsible for the attacks. They're used by individuals, state-sponsored hacking groups, and large criminal organisations.

Privileged user compromise is not limited to external threats either. Insiders with legitimate access to privileged accounts may abuse their privileges for malicious purposes.

in the news

In January 2023, malicious actors successfully used spear phishing techniques to trick a Mailchimp employee into exposing their credentials. The compromised account gave the attackers access to at least 133 Mailchimp user accounts including those that belonged to businesses like Woocommerce, Statista, and FanDuel.

41. Ransomware

Ransomware attacks make up more than 23% of all cyber incidents affecting personal data in the UK. In 2022, criminals compromised data on more than 5.3 million people from over 700 organisations using ransomware attacks - a record high for the UK.

How does the attack happen?

During a ransomware attack, a malicious actor encrypts a victim's data or locks them out of their system and demands a ransom to provide a decryption key or access to the system. Depending on the victim and the type of data held to ransom, attackers can also threaten to leak the data if their demands are not met.

The ransomware can be deployed using spear-phishing attacks, drive-by downloads, and through remote service-based exploitation. Once the malware is successfully installed, the victim is directed to a website or is informed of the ransom via a pop-up.

Where does the attack come from?

Ransomware attacks are often targeted attacks for financial gain. Large criminal networks have used them to exploit corporate organisations and government bodies. However, with the ransoms being paid in cryptocurrency (something now easily available to anybody) these attacks are likely to be carried out by lone wolves and smaller groups too.

in the news

In September 2023, Greater Manchester Police fell victim to a ransomware attack. Attackers were able to compromise a third-party supplier holding information on its employees, exposing data potentially including the details of officers' name badges such as ranks, photos and serial number.

42. Ransomware-as-a-service

Ransomware-as-a-service (RaaS) is a cybercrime business model that allows less technically-savvy criminals to launch ransomware attacks without having to create the malware themselves or develop the necessary infrastructure.

How does the attack happen?

Cybercriminals or hacking groups develop ransomware and offer it as a service on the dark web or other underground forums. They may handle the technical aspects, such as updating and maintaining the ransomware code and command-and-control servers.

This ransomware is sold to individuals or groups who want to launch attacks. Affiliates can use various methods such as phishing emails, exploit kits, or social engineering, to infect victims' systems.

When the victim's data is encrypted, they receive a ransom note demanding payment in exchange for the decryption key. The ransom payments typically go to the service provider, who then shares a portion with the affiliate.

Ransomware-as-a-Service has made ransomware attacks more accessible and widespread. It lowers the barrier to entry for cybercriminals, as they don't need to possess advanced hacking skills or providers often operate anonymously and from different parts of the world.

Where does the attack come from?

Raas has made ransomware attacks more accessible so it's more challenging for law enforcement agencies to trace and prosecute the perpetrators. Affiliates and service providers often operate anonymously and from different parts of the world.

in the news

DarkSide is a RaaS operation associated with a crime group known as CARBON SPIDER. DarkSide traditionally focused on Windows machines targeting enterprise environments running unpatched VMware ESXi hypervisors or stealing vCenter credentials.

It's believed that the DarkSide ransomware was responsible for the Colonial Pipeline data breach - an infamous ransomware attack.

43. Router and Infrastructure Security

Although rare, criminals can exploit the security and infrastructure of routers allowing them to surreptitiously install a backdoor.

How does the attack happen?

Malicious actors install software or hardware secretly onto a network router or similar device. It allows unauthorised access, eavesdropping, and control over network traffic.

Router implants are challenging to detect and may lead to data interception, manipulation, and network disruption.

Where does the attack come from?

The nature of this attack requires some technical knowledge to access the router and stay hidden. Therefore, these attacks often come from more advanced threat actors.

in the news

In 2015, Cisco discovered a vulnerability in its Internetwork operating system. A router implant, or malware, known as SYNful Knock was found in 14 routers in 4 different countries allowing attackers to gain control over the infected device and compromise its integrity.

44. Shadow IT

With the rise in software-as-as-service, many employees are turning to different apps or software to help them do their jobs, often without the knowledge or consent of their businesses IT department. This technology is known as Shadow IT and leaves a window of vulnerability that is often exploited by malicious actors.

How does the attack happen?

Shadow IT attacks exploit vulnerabilities or weaknesses in technology solutions that are not officially sanctioned or monitored by the organisation's IT department. The attacks happen when employees store or share data on unauthorised cloud platforms which often have their own security gaps.

Shadow IT attacks can result in data breaches, malware infections, or other security incidents.

Where does the attack come from?

Shadow IT threats come from within an organisation, as employees are using unsanctioned apps and platforms to hold company data. The employee, trying to find a faster and more effective way to work, doesn't intend to put the organisation at risk but does so unwittingly.

in the news

In 2021, Insight Global an IT Management company suffered a data breach that was traced back to a shadow IT vulnerability. The personal information of around 70,000 Pennsylvania residents was compromised when employees contracted to assist the state health department's COVID-19 contact tracing efforts, started an unauthorised collaboration channel using several Google accounts.

45. Simjacking

Simjacking is an account takeover attack that targets weaknesses in two-factor authentication where the second factor is a text message or call placed to a mobile phone.

How does the attack happen?

Also known as a SIM swap scam, port-out scam, SIM swapping, and SIM splitting, SIM jacking relies on social engineering techniques to find personal information about a target such as their date-of-birth and address.

Once attackers have this sensitive data, they call the support line for the victim's mobile phone provider claiming they've lost their SIM. With all of the personally identifying information the malicious actors have gathered before the phone call, they're able to answer the security questions and fool the service provider into complying with their requests.

The attackers then have full control over the phone number and can use it to access accounts with two-factor authentication.

Where does the attack come from?

SIM jacking can come from anywhere but it's usually a targeted attack with the criminals trying to access a high-value account such as a bitcoin account or extort a high net-worth individual.

in the news

In 2021, authorities arrested a eight men in England and Wales who were part of a group targeting US celebrities with SIM jacking attacks. The gang, along with two others from Malta and Belgium, had targeted well-known sports stars, musicians, and influencers.

46. Social Engineering Attack

Social engineering is a broad range of malicious tactics used by bad actors to manipulate and fool victims into giving away sensitive information or making security mistakes. It relies on exploiting human emotions, trust, and cognitive biases, often using techniques like urgency, fear, flattery, or impersonation to deceive people.

How does the attack happen?

There are 8 common forms of social engineering attacks.

Phishing: Attackers send deceptive emails, messages, or websites that appear to be from a legitimate source to trick individuals into revealing personal information like usernames, passwords, or financial details.

Spear Phishing: A targeted form of phishing, where attackers customise messages to specific individuals or organisations, often using information obtained through research to make the deception more convincing.

Baiting: Attackers offer enticing incentives, such as free downloads or media, to encourage individuals to download malicious software.

Pretexting: Attackers create a fabricated scenario, often impersonating a trusted entity, to extract sensitive information or gain access to a target's system.

Tailgating: An attacker gains unauthorised physical access to a secured area by following an authorised person or by posing as a legitimate employee or visitor.

Quid Pro Quo: Attackers offer something of value in exchange for information or access, often via phone calls.

Impersonation: Attackers impersonate a trusted individual, such as a tech support agent or company executive, to trick individuals into taking actions that compromise security.

Reverse Social Engineering: The attacker manipulates the victim into seeking information or assistance from the attacker.

Where does the attack come from?

Social engineering can come from anywhere, but it often starts with phishing emails. Attackers can range from lone wolves to criminal groups and hostile nation-states. The goal is usually stealing data, financial gain, blackmail, and espionage.

in the news

In 2018, US state Cabarrus County, NC lost $1.7 million to a social engineering attack. Using malicious emails, attackers were able to trick public employees by pretending to be legitimate county suppliers working on the construction of a new school. Using forged documentation and approvals, the hackers were able to convince employees to change the bank account to which they made payments for the construction.

47. Spyware

An ever-present threat in the cyber security space, spyware continues to develop in its efficiency and secrecy. Spyware is a type of malware designed to gather information about the user's online activities, personal data, and system usage reporting back to malicious actors.

How does the attack happen?

Spyware installs itself onto a victim's device without their knowledge or consent, usually by exploiting an existing weakness. For example, when a user clicks on a pop-up, downloads files from unknown email addresses, or uses unreliable websites.

Various types of spyware exist, all working in different ways to track the victim's actions. The data gathered through spyware can be used to capture financial information such as bank account logins and even steal a victim's identity.

Where does the attack come from?

Spyware kits are easily available on the dark web and can be used by hackers of any skill level. They're usually used to harvest information that can be sold to third parties who can use it for a variety of malicious purposes.

in the news

In 2021 researchers at Zimperium zLabs published a report identifying a spyware app found in South Korea that was affecting Android devices. The app, called PhoneSpy acts as a legitimate application to gain access and steal data or even remotely control the infected device.

48. SQL Injection

SQL or Structured Query Language (often pronounced 'sequel') is the predominant programming language used by every data-driven website and application on the internet to communicate with relational databases.

Attackers can exploit this use of SQL to manipulate or destroy databases with malicious code injections. The aim is usually to bypass security measures, access and steal sensitive data, or cause disruption.

How does the attack happen?

Attackers submit malicious SQL code or commands through user input fields, such as web forms, search boxes, or URL parameters. If the web application does not properly validate or 'sanitise' this input the attacker can manipulate the SQL queries executed by the application's database. This potentially gives them unauthorised access to the database, extracting or modifying data, and even compromising the entire web application.

Where does the attack come from?

SQL injections are one of the most common types of cyberattack, largely because so much of the internet is built upon SQL databases.

in the news

In 2020, Estonia, a well-known digitally savvy nation, fell victim to an SQL injection attack that targeted the Estonian Central Health Database. The attack compromised the health records of nearly all of Estonia's citizens, exposing private data and damaging governmental trust.

The identities of the attackers remain unknown, but Estonia has since invested in enhancing its cybersecurity protocols to prevent an attack of the same scale.

49. Supply Chain Attack

Supply chain attacks come from compromised vendors who require legitimate access to sensitive data and the systems of their customers. These are formidable attacks that are hard to detect and even harder to prevent.

How does the attack happen?

Attackers target vendor software by finding weaknesses in the source code, build processes, or updates. If left undetected, vendors unknowingly push out malware to their customer network which is used to gain unauthorised access, steal data, or carry out other malicious activities.

This is a particularly effective attack, and one software update can compromise thousands of organisations. Due to the sheer scale of access these attacks can provide, they must be taken seriously.

Where does the attack come from?

Supply chain attacks are large-scale attacks that require manpower and expertise. They're often funded by malicious nations or sophisticated threat actors.

in the news

In 2017, credit reporting company Equifax suffered a data breach that affected 147 million customers. Hackers found a vulnerability in the website software caused by a failure to patch a common security issue.

50. Suspicious Cloud Authentication Activities

With more organisations moving to cloud applications cloud security should be a priority for all. When the right identity access management (IAM) tools are not used, it's easy for malicious actors to gain unauthorised access and remain undetected.

How does the attack happen?

When organisations aren't up to date with identity access management, they become an easy target for criminals who can exploit networks that rely solely on endpoint/network security. Using stolen credentials, they can gain unauthorised access and remain undetected as they move laterally through the network.

Implementing IAM tools like multi-factor authentication (MFA) and continuously authenticating and authorising devices can help to minimise the risk of these attacks.

Where does the attack come from?

This type of attack can, and does, come from anywhere. With the rise in the use of cloud applications, attackers have a larger pool of victims to target.

in the news

In 2022 84% of organisations reported falling victim to identity-related breaches, the majority of which could have been prevented with the right IAM in place.

51. Suspicious Cloud Storage Activities

With almost every cyber security attack, there is an element of human negligence that, if addressed, could easily thwart the threat. Many organisations are working in cloud environments whether fully or in part, yet not all of them take the appropriate steps to secure the data left in these environments.

How does the attack happen?

When businesses migrate to the cloud, many do so without the proper security protocols in place, either through lack of knowledge or as an oversight. Most cloud applications also operate on a shared responsibility model where the service providers secure certain elements, processes and functions but protecting data, code, and any other assets stored in those applications is the responsibility of the client.

Where does the attack come from?

Attackers will find and exploit any unsecured areas and once they have access there are various routes to take. They can turn off controls such as access monitoring, make storage buckets accessible to the public to enable data exfiltration, and create new accounts for continued access.

It's especially important to keep up with software updates when using cloud applications. Attackers will exploit known vulnerabilities that were patched in a later version, but where the customer is using an outdated version of the software.

in the news

According to a recent survey 80% of companies have experienced at least one cloud security incident in the last year. Add to that number that 80% of those surveyed also said they do not have a dedicated cloud security team or lead and it's easy to see why these attacks are so common.

52. Suspicious Okta Activity

Okta is a cloud-based identity and access management service used by many enterprise applications and accounts. Okta uses single sign on or SSO to allow administrators to manage which users are allowed to access which applications. If the login credentials to Okta are compromised, attackers can potentially access multiple applications.

How does the attack happen?

Okta has a known SSO vulnerability that malicious actors exploit using credential stuffing attacks. These credentials are stolen through phishing scams, breached websites and brute force or password spraying attacks.

Where does the attack come from?

With the rise in automated tools for brute force attacks and password spraying Okta attacks can be carried out by almost any hacker. However, it's not uncommon for larger, organised criminal groups and hostile nations to use them.

in the news

In March 2022, Okta users were targeted by a phishing campaign called 'Oktapus' orchestrated by the hacking group Scatter Swine. Emails designed to look like the login portals of Okta lead to the compromise of nearly 10,000 Okta credentials, affecting around 130 organisations in the tech and gaming sectors.

53. Suspicious Zoom Child Activities

The use of zoom a video conferencing service has grown vastly over the last couple of years, starting as a way for remote workers to connect during COVID-19 stay-at-home mandates. However, malicious actors quickly identified flaws in both Windows and macOS systems that enable unauthorised access, allowing them to escalate privileges on targeted devices.

How does the attack happen?

These attacks exploit vulnerabilities in the architectural design of Zoom's software by local attackers who already have control over a vulnerable computer. There are two ways for attackers to use Zoom to install malware such as spyware, trojans, and other types of malicious code.

The first attack avenue is through the Zoom installer which is designed to install without user interaction on the macOS system. The attacker can use the installer to inject malware that allows them to obtain the highest level of user privileges. With these privileges, the bad actor can access the underlying Mac system where they might install spyware or malware while the user is unaware.

Secondly, there is a bug in Zoom's local library function which allows attackers to access and change camera and microphone permissions without the knowledge or consent of the PC owner. To do this, bad actors load malicious code into the process/address space which automatically inherits all of Zoom's access rights.

Where does the attack come from?

To carry out this attack threat actors need physical access to a device, so it's often an insider threat. Alternatively, an attack could occur when a device has been previously infected by malware giving the attacker pre-existing access.

in the news

Zoom's security issues have long been in the spotlight with multiple incidents highlighting various flaws and data breaches. In 2021, Zoom agreed an historic $85 million payout for users who were victims of zoom-bombing that allowed hackers and pranksters to crash into virtual meetings.

54. System Misconfiguration

System misconfiguration is a widespread problem that has had profound consequences for many affected businesses. A simple mistake or oversight can open the doorway for attackers to compromise the full IT stack of target organisations.

How does the attack happen?

System misconfiguration attacks usually happen because of missing security protocols and documentation, missing patches, the use of default accounts and configuration, and using unnecessary services.

Examples of system misconfiguration that can be exploited by criminals include forgetting to disable administrative access for lower level employees, keeping ports open that are not required, and failing to use encryption services for sensitive data.

Where does the attack come from?

System misconfiguration is essentially human error and is not classed as a malicious act. However, if attackers are made aware of misconfiguration issues either through social engineering or tip-offs they can easily be used for malicious purposes.

in the news

In 2019, researchers revealed a misconfiguration error that led to exposed employee and project details in organisations including NASA, Google, and Yahoo. The misconfiguration was found in an app called JIRA used for bug tracking, issue tracking, and agile project management.

The issue occurs when creating a new dashboard where the visibility to “Everyone” and “All users” by default. Instead of limiting visibility to everyone within the organisation, this setting actually shares the dashboards publicly.

As part of its user picker tool, JIRA also provides a complete list of every user’s username and email address. This happens because of an authorisation misconfiguration in Jira’s Global Permissions settings.

55. Typosquatting

Typosquatting is a phishing attempt where attackers take advantage of common typing errors to deceive internet users and potentially compromise their online security.

How does the attack happen?

Typosquatting revolves around registering domain names that are very similar to legitimate ones, capitalising on minor typo errors that users frequently make. Attackers deliberately select domains with common typos, such as missing a letter or reversing characters. When users make these typing errors in the address bar, they are redirected to deceptive websites that mimic the appearance and functionality of the intended site.

In these imitation websites, users may unwittingly provide sensitive information, assuming they are interacting with the genuine platform. Attackers can then harvest this data, posing serious privacy and security risks to users.

Where does the attack come from?

This is an easy attack to carry out and can be as simple as registering a domain name and installing malicious code on that domain. This is another attack that relies on human error and unsophisticated internet users who won't spot that the domain has been misspelt.

in the news

The Career Agents Network discovered that users typing .com instead of .biz in their web address were directed to a site that warned visitors to stay away from company. It was traced back to a disgruntled customer who had established the site in 2009.

56. Watering Hole Attack

This attack involves lurking attackers that wait to strike when their victim's guard is down, like animals at a watering hole.

How does the attack happen?

During a watering hole attack, the attacker targets a specific group of individuals or organisations by compromising websites or online resources that the targeted group is known to visit regularly.

The attacker exploits weaknesses in these websites and waits for the targets to visit the compromised sites, infecting the network and allowing entry into systems that the attacker can move laterally through.

Where does the attack come from?

Watering hole attacks are largely attributed to organised threat groups from countries like Russia, China, and Eastern Europe. In 2018, Chinese threat group 'Lucky Mouse' (also known as Emissary Panda, Iron Tiger, APT 27, and threat group 3390) was identified as the source behind a country-level watering hole attack targeting manufacturing, government, and energy sectors.

in the news

In 2015 a Chinese threat group launched a watering hole attack to compromise Forbes.com leveraging two zero-day vulnerabilities. One vulnerability was in Microsoft's Internet Explorer and one in Adobe's Flash Player which was used to display malicious versions of Forbes's 'Thought of The Day' – a flash widget that loaded whenever a user tried to access a page on Forbes.com.

The attack infected anyone with a vulnerable machine when they visited Forbes.com.

57. Web Session Cookie Theft

Also known as session hijacking, web session cookie theft is a version of online identity theft allowing attackers to the same user permissions as authenticated users.

How does the attack happen?

Every web application we use from banking to social media uses authentication cookies to streamline the user process. Without authentication cookies, users would need to re-enter username and password details on every new page.

Cookie theft occurs when hackers steal a victim's session ID and mimic that person's cookie over the same network. This can happen in several ways, usually through malware that has been installed on a victim's computer after a phishing attack, cross-site scripting, or macro viruses.

Once attackers have stolen a session cookie, they can use it to access web applications used by the victim including financial systems and customer records.

Where does the attack come from?

Many cookie theft attacks can be attributed to larger criminal networks like those in Russia and China. However, they can also happen when victims do something as simple as using unprotected public Wi-Fi.

in the news

In 2019 a session cookie theft attack was traced to a group of hackers recruited from a Russian-speaking forum that targeted Youtubers. The attack involved luring users with fake collaboration opportunities (such as demoing anti-virus software, VPN, music players, photo editing or online games) Attackers would then use malware to hijack the YouTube channels and sell them to the highest bidder or use them to broadcast cryptocurrency scams.

58. Wire Attack

Wire transfer attacks see to fraudsters fooling victims into sending high-value wire transfers through targeted spear phishing campaigns and malware.

How does the attack happen?

This is a sophisticated attack that involves high-level spear phishing tactics and advanced malware. Cyber criminals use a range of tools and target specific organisations in order to convince employees to send large sums of money to their own accounts by wire transfer.

Where does the attack come from?

Due to the level of skill needed to carry out the malicious tactics used in wire attacks we mostly see them originating from organised and sometimes state-sponsored criminal groups. Infamous groups such as APT 38 and Lazarus Group have been traced back to high-profile wire attacks.

in the news

In 2019, Japan's Toyota Boshoku Corporation lost over $37 million when cybercriminals convinced a high-level financial executive to change the account information on an electronic funds transfer. It's believed the attackers were able to compromise the business email account of top level employees in order to fool the finance department.

59. Zero-Day Exploit

The scale of technological adoption correlates with a rise in zero-day threats – an attack that exploits a software vulnerability or security flaw that is unknown to the software developer or vendor. These attacks are nearly impossible to prevent due to the unknown nature of the software vulnerabilities.

How does the attack happen?

Zero-day exploits start by attackers scanning the code base of a system or application to identify any security weaknesses or vulnerabilities that they can use to their advantage. Once a flaw is found, threat actors infiltrate the system and infect it with their own malicious code and then launch the exploit.

Where does the attack come from?

Zero-day threats can originate from anywhere, and hackers often work together to find weaknesses in targeted software. However, a lot of attacks have been traced back to crime groups from nations or regions well-known for having extensive cyber-attack networks and infrastructure such as Russia and China.

in the news

In June 2021, professional social networking site LinkedIn was hit with a zero-day attack that affected 700 million users (more than 90% of the site's users) A hacker was able to scrape the data of these users by exploiting a weakness in the site's API.

The stolen data included email addresses, phone numbers, geolocation records, genders and social media details.

DIGITAL PANDA

THE BIRMINGHAM DIGITAL AGENCY

1-3 Kings Road, Sutton Coldfield, B73 5AB

0121 227 0850

enquiries@digital-panda.co.uk

www.digital-panda.co.uk