Top 50
Cybersecurity
Threats
splunk>
data
SOLUTIONS

Table of Contents

Account Takeover 5
Advanced Persistent Threat 7
Amazon Web Services (AWS) Attacks 9
Application Access Token 11
Bill Fraud 13
Brute Force Attack 15
Business Email Compromise 17
Cloud Cryptomining 19
Command and Control Attack 21
Compromised Credentials 23
Credential Dumping 25
Credential Reuse Attack 27
Cross-Site Scripting 29
Cryptojacking Attack 31
DNS Amplification 33
DNS Hijacking 35
DNS Tunneling 37
DoS Attack 39
Drive-by Download Attack 41
Insider Threat 43
IoT Threats 45
Macro Viruses 47
Malicious Powershell 49
Malware 51
Man-in-the-Middle Attack 53
Masquerade Attack 55
Meltdown and Spectre Attack 57
Network Sniffing 59
Open Redirection 61
Pass the Hash 63
Phishing 65
Phishing Payloads 67
Spear Phishing 69
Whale Phishing (Whaling) 71
Privileged User Compromise 73
Ransomware 75
Router and Infrastructure Attacks 77
Shadow IT 79
Simjacking 81
Social Engineering Attack 83
Spyware 85
SQL Injection 87
Supply Chain Attack 89
Suspicious Cloud Storage Activities 91
Typosquatting 93
Watering Hole Attack 95
Web Session Cookie Theft 97
Zero-Day Exploit 99
Learn More 101

Foreword

Now more than ever, cybersecurity is essential to our future — after all, it's vital to protecting everything we rely on today. From banking and online commerce, to developing medicine and life-saving vaccines, to simpler things — like keeping our favorite video streaming services running.

Yet in the wake of mass migrations to the cloud and digital transformation, many organizations still haven't reached the peak of their security operations because of a few key challenges: An always-evolving threat landscape that pits us against creative and well-funded bad actors; the increasing complexity of hybrid and multi-cloud environments; security teams are bogged down by an endless list of monotonous tasks and time-consuming manual processes; and data silos caused by the proliferation of tools used inside our organizations, which create inefficiencies and blind spots.

These four challenges add up to a single reality: Security is a data problem. This is why a data-centric approach to security is paramount — arming us with the right information at the right time, and connecting tools and teams through all the noise and complexity. An analytics-driven solution, drawing upon end-to-end visibility and powered by machine learning (ML), is key to any organization's success. These advanced capabilities not only give a complete picture of your environment, but also move operations away from human intervention and basic diagnostics, towards an automated and strengthened security defense.

How? By stitching together and contextualizing swathes of highly complex datasets, addressing threats faster with automated alert triage, investigation and response, and honing in on anomalous behavior thanks to out-of-the-box ML models and algorithms. All of this helps organizations improve their cyber resilience — the ability to anticipate and adapt to compromises or attacks on cyber resources — so they can more effectively automate security operations and safeguard the business, all the while accelerating growth and innovation.

At Splunk, we're excited by the possibilities that data brings for a better — *and more secure* — future. But to get there, we must be prepared. We need to know what we're up against, including the threats that loom large. That's why we've put together this book of cybersecurity threats — so you can better identify the different types of attacks out there, mitigate risk and make your business even stronger.

Gary Steele
Splunk President and CEO

It may be quite a while before we fully understand the impact the pandemic years have had on the global information security (InfoSec) landscape. More has happened in this time than many security professionals saw in their entire careers before 2020. The fact is that the challenges we're facing are bigger than ever.

The "Great Resignation" as well as plain-old burnout may make the task seem more daunting just as the security world needs to attract and retain top talent. Those who haven't already succumbed are overwhelmed by more alerts than ever. They're spending too much time on repetitive, manual tasks, which can't possibly be helping their morale. What's more, they lack insights into the data they need to understand the greatest threats to your security.

But there is hope. Most security operations platforms have failed to fundamentally address security as a data problem. That is actually where the opportunity lies for security professionals.

The ability to field a resilient cybersecurity response is directly related to the quantity and quality of data collected, analyzed, and implemented in the battle to reduce business risk.

Realizing that the future is uncertain, organizations are investing with resilience in mind, to withstand the latest threats to the business and spring back stronger. In this context, resilience means flexible. Fast. Prepared. Proactive. Resilient organizations have a strong data and technology foundation, allowing them to engage rapidly with whatever comes their way.

Resilient security teams deliver cybersecurity solutions to protect every aspect of the business, unlock innovation and empower the organization. Resilient teams address challenges with data at the center of everything they do. And it shows in the results. Data-centric security operations can reduce the risk of data breach, IP theft and fraud by as much as 70%.

This is where it helps to know what threats to look out for and where this book can help. Based on the research of the Splunk Threat Research Team, we present 50 of the biggest cybersecurity threats to help security professionals make us all feel more secure.

Account Takeover

Account takeover is considered one of the more harmful ways to access a user's account. The attacker typically poses as a genuine customer, user or employee, eventually gaining entry to the accounts of the individual they're impersonating.

In 2022 alone, 84% of organizations fell victim to identity-related breaches, with 96% reporting that the breach could have been avoided or minimized by implementing identity-centric security.

Without the correct technologies and policies in place (e.g., zero trust and vendor management), identifying anomalous user behavior can be incredibly tricky. As a result, these attacks often go undetected, as the authentication performed by a bad actor can look the same as a legitimate user, depending on how expansive the identity and access management (IAM) framework in place is (let alone if it even exists).

Account Takeover

What you need to know:

Rather than stealing the card or credentials outright, account takeover is more surreptitious, allowing the attacker to get as much use out of the stolen card as possible before being flagged for suspicious activity. Banks, major marketplaces and financial services like PayPal are common targets, and any website that requires a login is susceptible to this attack.

Organizations need to move away from network security in order to better protect and authenticate user identities. Up until recently, certain technologies simply lacked the necessary integration capabilities, limiting an organization's ability to centrally monitor the overall security of their resources. Now there are countless technologies available that revolve around access control, like multifactor authentication (MFA).

To avoid illegitimate authentication on cloud applications, no user or device — whether internal or external to the organization — should be implicitly trusted, and access to all resources should be explicitly and continuously authenticated and authorized.

How the attack happens:

Some of the most common methods include proxy-based "checker" one-click apps, brute force botnet attacks, phishing and malware. Other methods include dumpster diving to find personal information in discarded mail, and outright buying lists of "Fullz," a slang term for full packages of identifying information sold on the black market. Once the profile of the victim is purchased or built, an identity thief can use the information to defeat a knowledge-based authentication system.

The threat or attacker can also easily penetrate the network/breach the perimeter when there's a distinct lack of or a weak IAM framework, and when an organization is still relying on network/endpoint security. In both instances, because the identity access controls are so lax, the attacker can easily log in with the stolen credentials without being detected — ultimately giving them free reign.

Where the attack comes from:

An enormous volume of our transactions — financial and otherwise — take place online. For cybercriminals, acquiring account credentials and personal information (like social security numbers, home addresses, phone numbers, credit card numbers and other financial information) is a lucrative business, whether they choose to sell the acquired information or use it for their own gain.

Between the growing number of phishing attacks, increasing number of user identities and the continued growth of cloud adoption, this type of attack can come from anywhere, including third-party vendors, employees, remote workers and contractors.

Advanced Persistent Threat

In one notable attack, a Chinese advanced persistent threat (APT) breached 25 Microsoft Exchange accounts across various U.S. agencies. The attack allowed the APT group to forge access to “multiple types of Azure Active Directory applications, including every application that supports personal account authentication, such as SharePoint, Teams, OneDrive, customers’ applications that support the ‘login with Microsoft’ functionality, and multitenant applications in certain conditions,” according to reports.

Advanced Persistent Threat

What you need to know:

An advanced persistent threat (APT) is a highly advanced, covert threat on a computer system or network where an unauthorized user manages to break in, avoid detection and obtain information for business or political motives. Typically carried out by criminals or nation-states, the main objective is financial gain or political espionage. While APTs continue to be associated with nation-state actors who want to steal government or industry secrets, cyber criminals with no particular affiliation also use APTs to steal data or intellectual property.

How the attack happens:

An APT usually consists of highly advanced tactics, including a fair amount of intelligence-gathering, to less sophisticated methods to get a foothold in the system (e.g., malware and spear phishing). Various methodologies are used to compromise the target and to maintain access.

The most common plan of attack is to escalate from a single computer to an entire network by reading an authentication database, learning which accounts have the appropriate permissions and then leveraging them to compromise assets. APT hackers will also install backdoor programs (like Trojans) on compromised computers within the exploited environment. They do this to make sure they can gain re-entry, even if the credentials are changed later.

Where the attack comes from:

Most APT groups are affiliated with, or are agents of, governments of sovereign states. An APT could also be a professional hacker working full-time for the above. These state-sponsored hacking organizations usually have the resources and ability to closely research their target and determine the best point of entry.

Amazon Web Services (AWS) Attacks

The number of creative attacks on virtual environments has exploded with the rise of cloud computing. And as one of the largest cloud-service providers, Amazon Web Services has certainly had its share of threats.

There are several vulnerabilities that threaten the security of cloud providers. One digital marketing company, for example, didn't password protect its Amazon S3 bucket when it went out of business. The lapse exposed the data of 306,000 people.

The full leak exposed 50,000 files, totaling 32GB of full names, locations, email addresses, phone numbers and hashed out passwords, from clients such as Patrón Tequila.

Amazon Web Services (AWS) Attacks

What you need to know:

Amazon's "shared responsibility" model says AWS is responsible for the environment outside of the virtual machine but the customer is responsible for the security inside of the S3 container.

This means threats that take advantage of vulnerabilities created by misconfigurations and deployment errors have become a bigger problem as companies have adopted cloud technologies rapidly and the organization using AWS is responsible for securing their environment. The problem is there are more threats that AWS customers have to worry about

How the attack happens:

An attack on an AWS instance can happen in a number of ways. It's important to stay vigilant for activities that may be as simple as suspicious behavior inside of an AWS environment — activities to look out for are S3 access from unfamiliar locations and by unfamiliar users.

It's also important to monitor and control who has access to an organization's AWS infrastructure. Detecting suspicious logins to AWS infrastructure provides a good starting point for investigations. Actions, such as abusive behaviors caused by compromised credentials, can lead to direct monetary costs because users are billed for any EC2 instances created by the attacker.

Where the attack comes from:

Because of the diversity of services being hosted on AWS and the new types of cloud threats being spun up daily, these attacks can virtually come from anywhere and anyone.

Application Access Token

An active and unknown threat actor employed different strategies to gain and leverage information from key targets. One method was to abuse Open Authentication (OAuth) tokens targeting high-profile organizations' repositories, including Github npm's production infrastructure as well as apps integrated with Heroku and Travis-CI cloud products.

Application Access Token

What you need to know:

With an OAuth access token, a hacker can use the user-granted REST API to perform functions such as email searching and contact enumeration. With a cloud-based email service, once an OAuth access token is granted to a malicious application, it can potentially gain long-term access to features of the user account if a “refresh” token enabling background access is awarded.

How the attack happens:

Attackers may use application access tokens to bypass the typical authentication process and access restricted accounts, information or services on remote systems. These tokens are typically stolen from users and used in lieu of login credentials.

Where the attack comes from:

Compromised access tokens may be used as an initial step to compromising other services. For example, if a token grants access to a victim’s primary email, the attacker may be able to extend access to all other services that the target subscribes to by triggering forgotten password routines. Direct API access through a token negates the effectiveness of a second authentication factor and may be immune to countermeasures like changing passwords.

Bill Fraud

Paypal is a financial service and online payment system that allows customers to easily send and receive money. Yet the very same features that make Paypal so quick and efficient for transferring funds are *also* exploited by cyberthieves for monetary gain. Hackers and scammers use the system to pilfer funds away from consumers in payment fraud schemes, sometimes wiping out entire bank accounts.

Bill Fraud

What you need to know:

Bill fraud — or payment fraud — is any type of bogus or illegal transaction in which the cybercriminal will divert funds away from consumers. And these schemes work — according to recent data from the FTC, consumers reported losing nearly $8.8 billion to fraud in 2022, an increase of more than 30 percent over the previous year.

How the attack happens:

This attack tricks a large number of users into repeatedly paying small or reasonable amounts of money so they don't notice the scam. In this ploy, attackers send fraudulent but authentic-looking bills instructing customers to transfer funds from their accounts.

Knowing that most customers regularly use fee-based digital services, the attackers rely on the fact that their targets may mistakenly assume the fraudulent bill is for a service they actually use. Consumers will then initiate a funds transfer or credit card payment to pay for the phony "bill."

Where the attack comes from:

Bill fraud organizations originate all over the world, including the U.S. It's typically sourced to attackers with the resources, bandwidth and technology to create fraudulent bills that look real. Like phishing, bill fraud generally targets a broad, random population of individuals.

Brute Force Attack

Brute force attacks can happen across all manner of services, with one recent example involving Windows Remote Desktop Protocol (RDP). Starting in early 2020 up to present day, Microsoft has recorded a significant uptick in RDP brute force attacks due to a large number of exposed endpoints, which allows threat actors to successfully exploit weak or commonly used passwords to gain unauthorized access to a wide range of systems.

Brute Force Attack

What you need to know:

A brute force attack aims to take personal information, specifically usernames and passwords, by using a trial-and-error approach. This is one of the simplest ways to gain access to an application, server or password-protected account, since the attacker is simply trying combinations of usernames and passwords until they eventually get in (*if* they ever do; a six-character password has billions of potential combinations).

How the attack happens:

The most basic brute force attack is a dictionary attack, where the attacker systematically works through a dictionary or wordlist — trying each and every entry until they get a hit. They'll even augment words with symbols and numerals, or use special dictionaries with leaked and/or commonly used passwords. And if time or patience isn't on their side, automated tools for operating dictionary attacks can make this task much faster and less cumbersome.

Where the attack comes from:

Thanks to the ease and simplicity of a brute force attack, hackers and cyber criminals with little-to-no technical experience can try to gain access to someone's account. The people behind these campaigns either have enough time or computational power on their side to make it happen.

Business Email Compromise

Business email compromise (BEC), similar to business invoice fraud, has evolved over the years, especially with the rise of video calls post-COVID-19. The attack is frequently carried out by bad actors posing as legitimate business contacts via phony meeting invites. According to one report, the FBI IC3 has "received an increase of BEC complaints involving the use of virtual meeting platforms to instruct victims to send unauthorized transfers of funds to fraudulent accounts."

Business Email Compromise

What you need to know:

Business email compromise attempts to trick victims into paying out a fraudulent (yet convincing) bill addressed to their organization. In reality, the funds go to imposters mimicking suppliers, co-workers or business partners. Often going beyond ordinary fraud, attackers can target banks in emerging markets with limited cybersecurity infrastructure or operational controls, or lure high-profile targets with sophisticated and believable phishing scams. These cybercrime syndicates are after one thing: money. And lots of it.

How the attack happens:

In one attack scenario, cybercriminals use sophisticated malware to bypass local security systems. From there, they gain access to a messaging network and send fraudulent messages to initiate cash transfers from accounts at larger banks. In another attack scenario, the bad actors use targeted spear phishing campaigns to convince stakeholders to transfer large sums of money to their coffers. Victims are sent fake invoices attempting to steal money in the hopes their marks aren't paying attention to their accounts payable processes.

Hackers will pick targets based on the size of their business, location and the suppliers used and create phony invoices that appear legitimate. With the hopes that the victim's accounts payable department is backlogged, they send false invoices with high demands like "90 days past due, pay now!"

Where the attack comes from:

While there are numerous individual scammers pulling off business invoice fraud, many are sourced to fraud rings that have the organization and the resources to research their victim's banking institution and create a billing experience that feels real. Fraud rings conducting invoice scams can be found all over the world.

Highly organized international and nation- state cybercrime groups, such as APT 38 and Lazarus Group, have historically been behind wire attacks. These groups have the necessary infrastructure and resources to successfully carry out complex and multi-faceted assaults. While it's unclear who exactly is behind these groups, some reports have indicated that they might have ties to North Korea. But hacking groups from China and Nigeria have also been found to be at the source of elaborate wire transfer attacks. A note of caution: High-value wire attacks at institutions with more robust systems likely involve the use of insiders to gain access to systems.

Cloud Cryptomining

Cloud cryptomining doesn't need gas to go. Look no further than Github for evidence. The cloud-based repository for software code fell victim to a cloud cryptomining attack when threat actors conducted a far-ranging freejacking operation — encompassing 30 GitHub accounts, 2,000 Heroku accounts and 900 Buddy accounts, as well as 130 Docker Hub images — abusing a large number of free accounts with as little human effort as possible.

Cloud Cryptomining

What you need to know:

Cryptomining is an intentionally difficult, resource-intensive business. Its complexity was designed to ensure that the number of blocks mined each day would remain steady. So it's par for the course that ambitious, yet unscrupulous, miners make amassing the computing power of large enterprises — a practice known as cryptojacking — a top priority.

How the attack happens:

Cryptomining has attracted an increasing amount of media attention since its explosion in popularity in the fall of 2017. The attacks have moved from in-browser exploits and mobile phones to enterprise cloud services, such as Amazon Web Services, Google Cloud Platform (GCP) and Microsoft Azure.

It's difficult to determine exactly how widespread the practice has become, since hackers continually evolve their ability to evade detection, including employing unlisted endpoints, moderating their CPU usage and hiding the mining pool's IP address behind a free content delivery network (CDN).

When miners steal a cloud instance, often spinning up hundreds of new instances, the costs can become astronomical for the account holder. So it's critical to monitor systems for suspicious activities that could indicate that a network has been infiltrated.

Where the attack comes from:

Because cryptocurrency is a global commodity, the attacks can originate from anywhere. Instead of focusing on where the attacks come from, it's key to monitor cloud computing instances for activities related to cryptojacking and cryptomining, such as new cloud instances that originate from previously unseen regions, users who launch an abnormally high numbers of instances, or compute instances started by previously unseen users.

Command and Control Attack

Cobalt Strike is a commercial penetration testing tool used by cybersecurity professionals to simulate advanced threat behaviors and assess an organization's security posture. It provides a range of capabilities, including reconnaissance, exploitation and post-exploitation activities, with its most notable feature being its "Beacon" payload.

In recent years, this payload allows for command and control (C2) of compromised hosts, enabling stealthy communication, lateral movement and various in-memory attack techniques. While Cobalt Strike is a legitimate tool intended for red team operations and threat emulation, bad actors have also used cracked versions of this software in cyber attacks due to its powerful features and evasion capabilities.

Command and Control Attack

What you need to know:

A command and control attack is when a hacker takes over a computer in order to send commands or malware to other systems on the network. In some cases, the attacker performs reconnaissance activities, moving laterally across the network to gather sensitive data. These types of attacks continue to grow in popularity, with the number of command-and-control servers (C2) increasing by a staggering 30% in 2022 alone.

In other attacks, hackers may use this infrastructure to launch actual attacks. One of the most important functions of this infrastructure is to establish servers that will communicate with implants on compromised endpoints. These attacks are also often referred to as C2 or C&C attacks.

How the attack happens:

Most hackers get a foothold in a system by phishing emails then installing malware. This establishes a command and control channel that's used to proxy data between the compromised endpoint and the attacker. These channels relay commands to the compromised endpoint and the output of those commands back to the attacker.

Where the attack comes from:

There have been prominent command and control attacks originating from Russia, Iran and even the U.S. These attackers can come from anywhere and everywhere — but they don't want you to know that.

Since communication is critical, hackers use techniques designed to hide the true nature of their correspondence. They'll often try to log their activities for as long as possible without being detected, relying on a variety of techniques to communicate over these channels while maintaining a low profile.

Compromised Credentials

Group-IB — a global cybersecurity leader — suffered a massive data breach in 2023. The coordinated attack compromised tens of thousands of accounts with saved chat GPT credentials — unsurprisingly, the large language model-based chatbot has gained massive popularity with cybercrime syndicates, particularly when it comes to gaining unauthorized access to accounts and exposing sensitive information for far-flung campaigns against companies and their employees.

Compromised Credentials

What you need to know:

Most people still use single-factor authentication to identify themselves (a pretty big no-no in the cybersecurity space). And while stricter password requirements are starting to be enforced (like character length, a combination of symbols and numbers, and renewal intervals), end users still repeat credentials across accounts, platforms and applications, failing to update them periodically.

This type of approach makes it easier for adversaries to access a user's account, and a number of today's breaches are thanks to these credential harvesting campaigns.

How the attack happens:

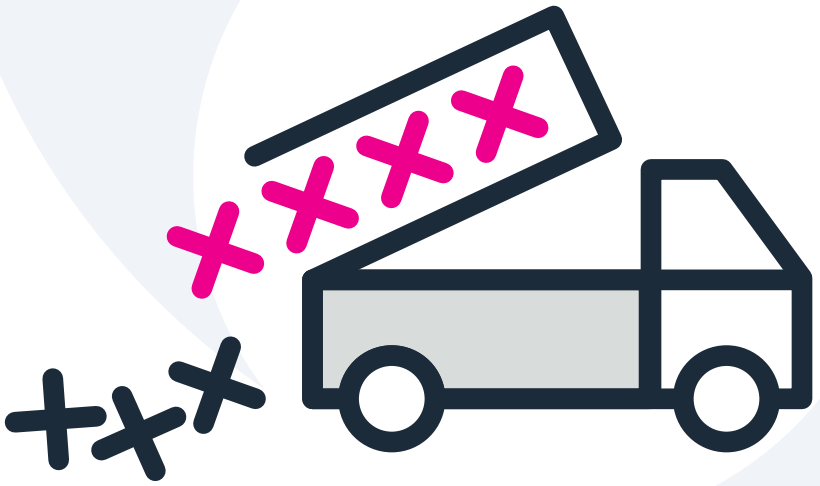
A password, key or other identifier that's been discovered can be used by a threat actor to gain unauthorized access to information and resources, and can range from a single account to an entire database.

By leveraging a trusted account within a targeted organization, a threat actor can operate undetected and exfiltrate sensitive data sets without raising any red flags. Common methods for harvesting credentials include the use of password sniffers, phishing campaigns or malware attacks.

Where the attack comes from:

Compromised credentials represent a huge attack vector, giving threat actors a way into computing devices, password-protected accounts and an organization's network infrastructure with relative ease. These perpetrators are often organized, with their sights set on a specific organization or person. And they're not always outside of the organization — they could very well be an insider threat who has some level of legitimate access to the company's systems and data.

Credential Dumping



A new ransomware named Trigona was recently identified, which targets Windows using unique methods, specifically employing the Mimikatz tool for various credential-related tasks and to extract sensitive data from Windows, including Windows memory, the Local Security Authority Subsystem Service (LSASS) process, and the Windows registry. Mimikatz then extracts and dumps the credentials to a file, ranging from usernames and passwords to hashes and Kerberos tickets.

Credential Dumping

What you need to know:

Credential dumping simply refers to an attack that relies on gathering credentials from a targeted system. Even though the credentials may not be in plain text — they're often hashed or encrypted — an attacker can still extract the data and crack it offline on their own systems. This is why the attack is referred to as "dumping."

Often, hackers will try to steal passwords from systems they have already compromised. The problem becomes amplified when users replicate the same password across multiple accounts through multiple systems.

How the attack happens:

Credentials obtained this way usually include those of privileged users, which may provide access to more sensitive information and system operations. Hackers often target a variety of sources to extract the credentials, including accounts like the security accounts manager (SAM), local security authority (LSA), NTDS from domain controllers or the group policy preference (GPP) files.

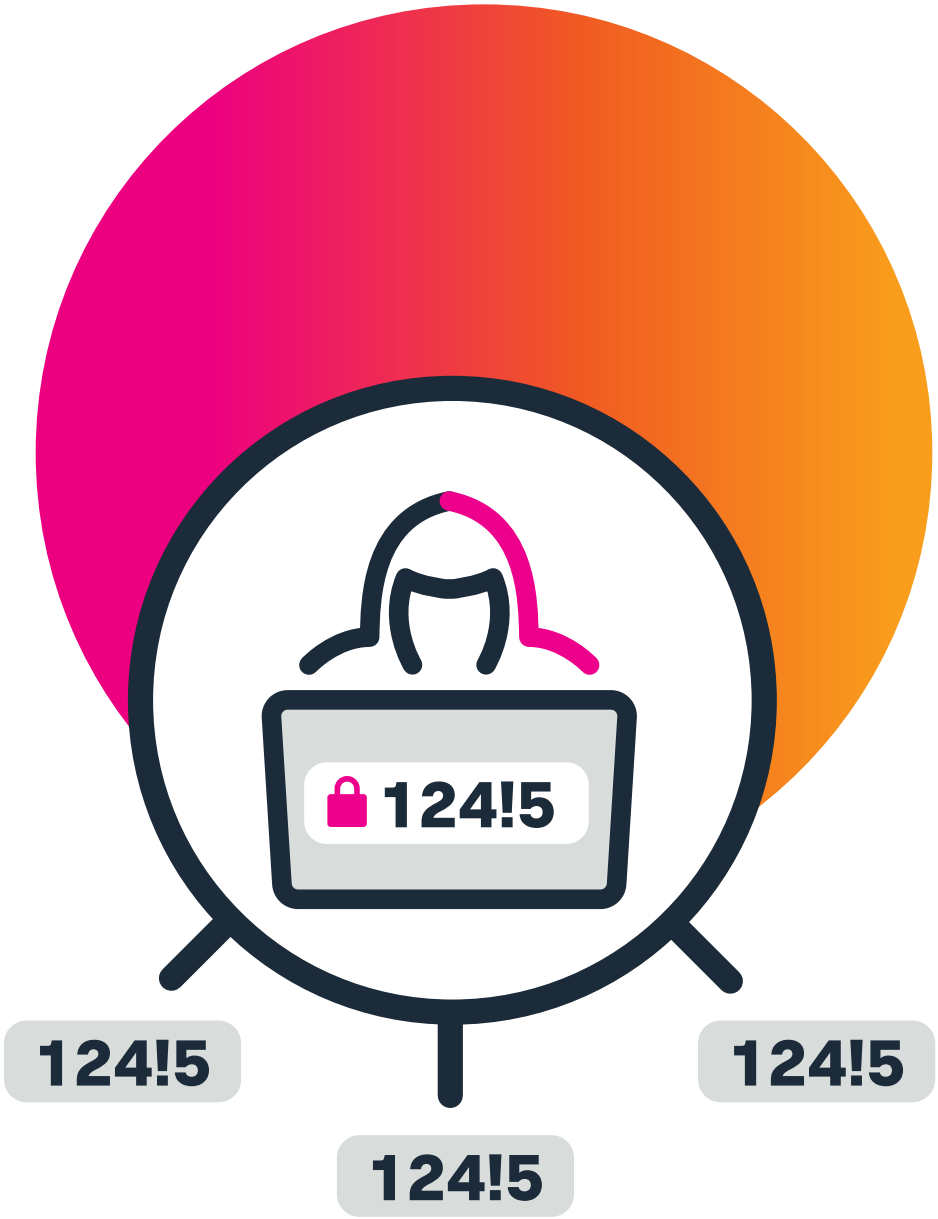
Once attackers obtain valid credentials, they use them to move throughout a target network with ease, discovering new systems and identifying assets of interest.

Where the attack comes from:

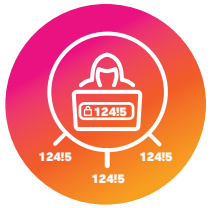
Credential dumping can originate from anywhere. And because we're all guilty of recycling passwords, that information can be sold for future attacks.

Credential Reuse Attack

One notable credential reuse attack is the 2022 Paypal breach — which, unluckily for the online payment system, compromised over 30,000 accounts over the span of a couple months. Threat actors gained access to personal data, including their "name, address, Social Security number, individual tax identification number, and/or date of birth," according to an email sent out by Paypal in the wake of the attack.



Credential Reuse Attack



What you need to know:

Credential reuse is a pervasive issue across any company or userbase. Nowadays, most users have tens (if not hundreds) of accounts, and are tasked with remembering countless passwords that meet all sorts of stringent requirements. As a result, they'll resort to reusing the same password over and over again, in the hopes of better managing and remembering their credentials across accounts. Unsurprisingly, this can cause major security issues when said credentials are compromised.

How the attack happens:

In theory, the attack itself is simple, straightforward and surprisingly stealthy (if two-factor authentication isn't activated). Once a user's credentials are stolen, the culprit can try the same username and password on other consumer or banking websites until they get a match — hence the "reuse" in "credential reuse attack."

However, gaining entry in the first place is a little more complicated. To get privileged information, attackers usually kick things off with a phishing attempt, using emails and websites that look close-to-legitimate to dupe the user into handing over their credentials.

Where the attack comes from:

This could be a targeted attack, where the person knows the victim and wants access to their accounts for personal, professional or financial reasons. The attack could also originate from a complete stranger who bought the user's personal information on the cybercrime underground.

Cross-Site Scripting

A cross-site scripting (XSS) vulnerability was recently discovered in Zimbra — a collaborative software suite — which allowed threat actors to steal users' sensitive information in a targeted attack.

XSS attacks are a type of injection in which malicious scripts are injected into otherwise benign and trusted websites. It's conceptually like an SQL injection — where malicious code is entered into a form to gain access to the site's database — except that in the case of XSS, the malicious code is designed to execute within the browser of another visitor to the site, allowing the attacker to steal user cookies, read session IDs, alter the contents of a website or redirect a user to a malicious site.

Cross-Site Scripting

What you need to know:

XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are widespread and occur anywhere a web application generates input from a user without validating or encoding it.

The end user's browser has no way to know that the script should not be trusted, automatically executing on the script. Because it thinks the script came from a trusted source, it can access cookies, session tokens or other sensitive information retained by the browser. These scripts can even rewrite the content of the HTML page.

How the attack happens:

There are two types of XSS attacks: stored and reflected. Stored XSS attacks occur when an injected script is stored on the server in a fixed location, like a forum post or comment. Every user that lands on the infected page will be affected by the XSS attack. In reflected XSS, the injected script is served to a user as a response to a request, like a search results page.

Where the attack comes from:

While XSS attacks are not as common as they once were — due primarily to improvements in browsers and security technology — they're still prevalent enough to rank within the top ten threats listed by the Open Web Application Security Project, and the Common Vulnerabilities and Exposures database lists nearly 14,000 vulnerabilities associated with XSS attacks.

Cryptojacking Attack

In July 2023, cyber hackers exploited cloud workloads in up to 200 instances, secretly mining cryptocurrency without users' permission. The cryptojacking attack was initiated when fileless payloads were loaded discreetly into the target system's memory, successfully evading detection.

Cryptojacking Attack

What you need to know:

Cryptojacking is an attack where a hacker targets and hijacks computer systems with malware that hides on a device and then exploits its processing power to mine for cryptocurrency — such as Bitcoin or Ethereum — all at the victim's expense. The hacker's mission is to create valuable cryptocurrency with someone else's computing resources.

How the attack happens:

One common way cryptojacking attacks happen is by sending a malicious link in a phishing email, enticing users to download cryptomining code directly onto their computer. Another way is by embedding a piece of JavaScript code into a webpage that the user visits — known as a drive-by attack. Upon visiting the page, malicious code intended to mine cryptocurrency will automatically download on the machine. The cryptomining code then works silently in the background without the user's knowledge — and a slower than usual computer might be the only indication that something is wrong.

Where the attack comes from:

These attacks come from all over the world because cryptojacking doesn't require significant technical skills. Cryptojacking kits are available on the deep web for as little as $30. It's a low bar of entry for hackers that want to make a quick buck for relatively little risk.

DNS Amplification

In February 2022, miscreants launched massive, amplified distributed denial-of-service (DDoS) attacks through Mitel, a global business communications company. The attack pummeled financial institutions, broadband ISPs, logistics and gaming companies, and other organizations. Able to sustain DDoS attacks for up to 14 hours, with a record-breaking amplification factor of almost 4.3 billion to one, attacks like this are capable of shutting down voice communications and other services for entire organizations with a single malicious network packet.

DNS Amplification

What you need to know:

Though DNS amplification, a type of DDoS attack, has been around for a long time, the exploitation techniques keep evolving. The attack is similar to DNS hijacking in the sense that it takes advantage of the internet's directory by misconfiguring it. But the way the attacks occur are slightly different.

A DNS amplification attack typically involves sending a small amount of information to a vulnerable network service that causes it to reply with a much larger amount of data. By directing that response at a victim, an attacker can put in a relatively low amount of effort while making other people's machines do all the work of flooding a selected target offline.

How the attack happens:

In a DNS amplification attack, the attacker floods a website with so many fake DNS lookup requests that it eats up the network bandwidth until the site fails. Where DNS hacking might direct traffic to another site, a DNS amplification attack prevents the site from loading.

The difference between the two attacks is further illustrated by the word "amplification." In this attack, hackers make the DNS requests in a way that requires a more intensive response. For example, a hacker might request more than just the domain name. The attacker might also ask for the entire domain, known as an "ANY record," which requests the domain along with the subdomain, mail servers, backup servers, aliases and more.

Now imagine several of these "ANY" requests coming in at once. The amplified traffic is enough to take the site offline.

Where the attack comes from:

Similar to a DNS hijacking attack, the relatively primitive nature of the attack means it can originate from anywhere in the world, be it nation-state hackers or a lone wolf.

DNS Hijacking

In late 2022, Celer Network — an interoperability protocol and cross-chain bridge — was the victim of a DNS hijacking attack. The hijack of their cBridge UI redirected users to phishing smart contracts on Avalanche, Ethereum and Polygon, eventually draining their account balance.

DNS Hijacking

What you need to know:

DNS is often called the Achilles heel of the internet, or the internet's phonebook, because it plays a critical role in routing web traffic. The DNS is the protocol used to map domain names to IP addresses. It has been proven to work well for its intended function. But DNS is notoriously vulnerable to attack, attributed in part to its distributed nature. DNS relies on unstructured connections between millions of clients and servers over inherently insecure protocols.

The gravity and extent of the importance of securing DNS from attacks is undeniable. The fallout of compromised DNS can be disastrous. Not only can hackers bring down an entire business, they can intercept confidential information, emails and login credentials as well.

How the attack happens:

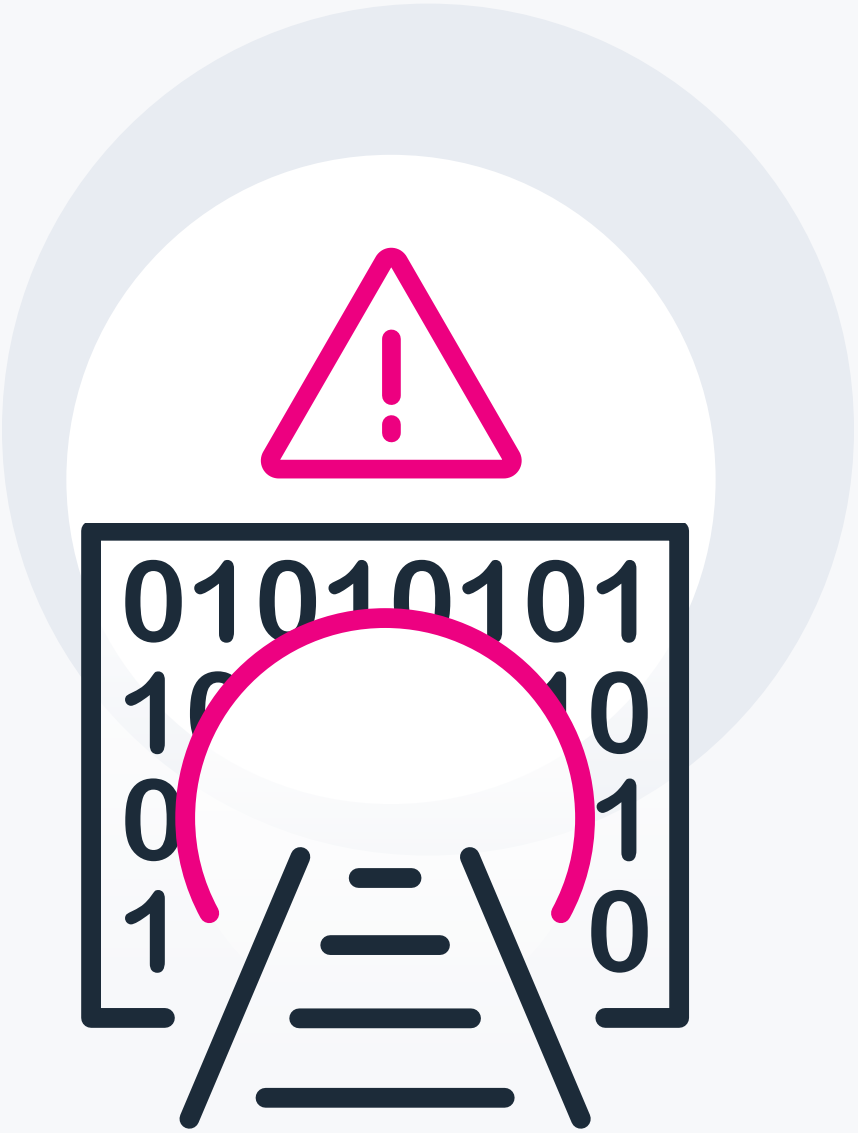
The attack works when hackers exploit the way DNS communicates with an internet browser. The system acts as a phone book, translating a domain — like NYTimes.com — into an IP address. The DNS then looks up and finds which global server is hosting that site and then directs traffic to it. The attack happens when a hacker is able to disrupt the DNS lookup and then either push the site offline or redirect traffic to a site that the hacker controls.

Where the attack comes from:

There is no one singular profile of a DNS hijacker, largely because the attack can occur as easily as a social engineering attack in which someone calls a domain provider and tricks them into changing a DNS entry.

DNS Tunneling

A hacker group known as OilRig has made regular attacks on various governments and businesses in the Middle East using a variety of tools and methods over the past several years. An essential element of its efforts to disrupt daily operations and exfiltrate data is maintaining a connection between its command-and-control server and the system it's attacking using DNS tunneling.



DNS Tunneling

What you need to know:

The protocol that translates the URLs we enter in web browsers into their numerical IP addresses is called the Domain Name System (DNS) — think of it as the phone book for the internet. The traffic passing through DNS often goes unmonitored, since it's not designed for data transfer, leaving it vulnerable to several kinds of attacks, including DNS tunneling, which happens when an attacker encodes malicious data into a DNS query: a complex string of characters at the front of a URL.

There are valid uses for DNS tunneling — anti-virus software providers use it to send updated malware profiles to customers in the background, for example. Because of the possibility of legitimate use, it's important for organizations to monitor their DNS traffic thoroughly, allowing only trustworthy traffic to continue flowing through the network.

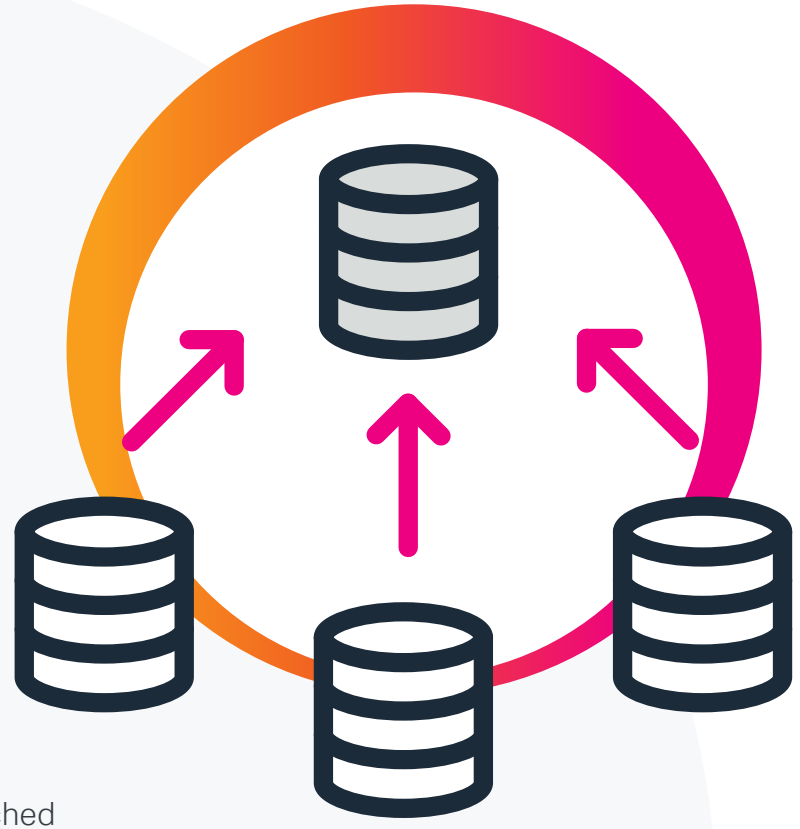
How the attack happens:

With DNS tunneling, an attacker can bypass security systems (tunneling under or around them, so to speak) by redirecting traffic to their own server, setting up a connection to an organization's network. Once that connection is active, command and control, data exfiltration and a number of other attacks are possible.

Where the attack comes from:

While there are DNS tunneling tools readily available for download, attackers wishing to do more than bypass a hotel or airline's paywall for internet access require more sophisticated knowledge. In addition, because DNS was designed only to resolve web addresses, it's a very slow system for data transfer.

DoS Attack



Almost two decades ago, a 16-year-old hacker known as Mafiaboy launched one of the most famous denial-of-service (DoS) attacks that took several major sites offline, including CNN, eBay, Amazon and Yahoo. According to reports, Mafiaboy broke into dozens of networks to install malware designed to flood targets with attack traffic. Because many sites were underprepared for such an assault, the attack lasted about a week as the targeted organizations struggled to figure out what happened and how to get back online. Mafiaboy was eventually arrested and sentenced to juvenile detention.

Twenty years later, DoS attacks — many of which are distributed denial-of-service attacks (DDoS) masterminded by hackers, hacktivists or cyber spies to take down websites and online services — are on the rise, and one of the most common attacks faced by organizations, with DDoS attacks growing by 150% on a global basis in 2022.

DoS Attack

What you need to know:

A DoS attack is where cyberattackers make a machine or network inaccessible for its intended users. DoS attacks can be executed by either flooding networks with traffic or by sending information that triggers a system slowdown or complete crash. As with DDoS attacks, DoS attacks tend to focus on high-profile organizations or ones with popular, public-facing websites such as banking, ecommerce, media or government institutions. DoS attacks deprive legitimate users of the service they want to access and cause extensive damage to the victim, due to security and cleanup costs, loss of reputation, loss of revenue and customer attrition.

How the attack happens:

DoS attacks occur in one of two ways: by flooding or crashing a targeted network. In flood attacks, cybercriminals bombard victim computers with more traffic than they can handle, causing them to slow or shut down altogether. Various flood attacks include buffer overflow attacks, ICMP flood and SYN flood attacks.

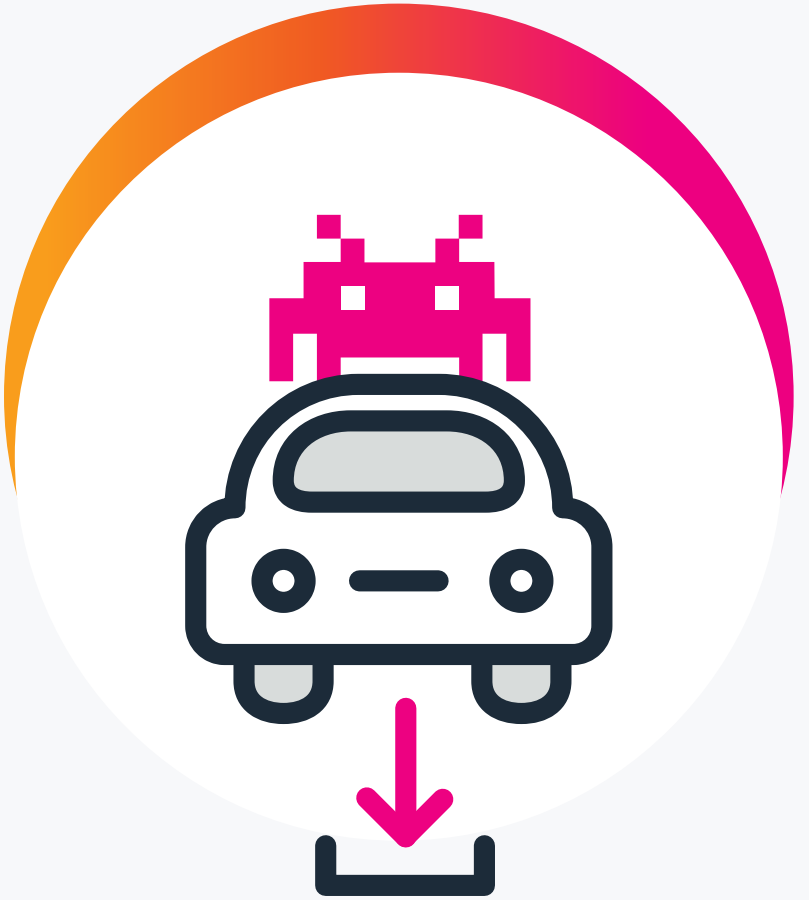
The malicious actors behind DDoS attacks aim to wreak havoc on their targets, sabotage web properties, damage brand reputation and prompt financial losses by preventing users from accessing a website or network resource. DDoS leverages hundreds or thousands of infected “bot” computers located all over the world. Known as botnets, these armies of compromised computers will execute the attack at the same time for full effectiveness.

Where the attack comes from:

DoS attacks can originate from anywhere in the world. Attackers can easily mask their whereabouts so they can overwhelm victim computers, execute malware or conduct other nefarious deeds with the peace of mind that they won’t be detected.

As their name implies, DDoS attacks are distributed, meaning that the incoming flood of traffic targeting the victim’s network originates from numerous sources. Thus, the hackers behind these attacks can literally be from anywhere in the world. What’s more, their distributed nature makes it impossible to stop these attacks simply by securing or blocking a single source.

Drive-by Download Attack



In January 2020, visitors to the legendary zine and blog site Boing Boing saw a fake Google Play Protect overlay prompting them to download what was actually a malicious APK that installed a banking Trojan on Android devices. For Windows users, it appeared as a (fake) Adobe Flash installation page that distributed other malicious programs. Boing Boing's content management system had been hacked. Even if the visitor didn't take the bait, the drive-by-downloads were automatically initiated by JavaScript embedded into the page. While Boing Boing was able to detect the attack and remove the script relatively quickly, given the site's five million unique users — former President Barack Obama among them — the impact could have been disastrous.

Drive-by Download Attack

What you need to know:

A drive-by download refers to the unintentional download of malicious code onto a computer or mobile device that exposes users to different types of threats. Cybercriminals use drive-by downloads to steal and collect personal information, inject banking Trojans or introduce exploit kits or other malware to user devices. To be protected against drive-by downloads, regularly update or patch systems with the latest versions of apps, software, browsers and operating systems. It's also recommended to stay away from insecure or potentially malicious websites.

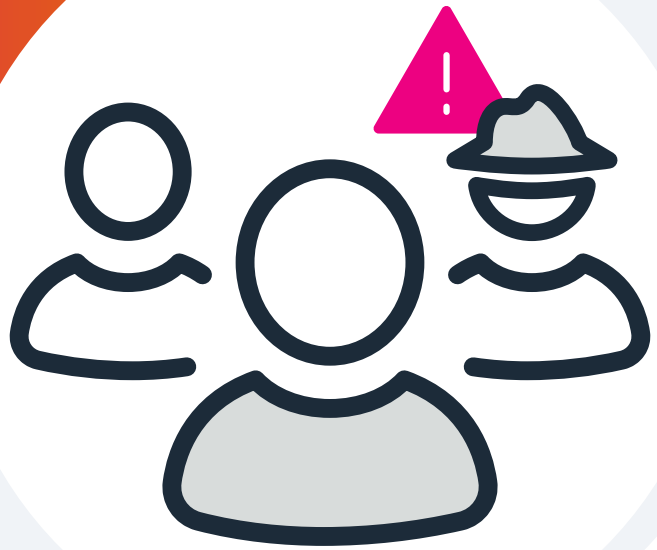
How the attack happens:

What makes drive-by downloads different is that users do not need to click on anything to initiate the download. Simply accessing or browsing a website can activate the download. The malicious code is designed to download malicious files onto the victim's device without the user's knowledge. A drive-by download abuses insecure, vulnerable or outdated apps, browsers or even operating systems.

Where the attack comes from:

The rise of prepackaged drive-by download kits allows hackers of any skill level to launch these kinds of attacks. In fact, these kits can be purchased and deployed without the hacker writing their own code or establishing their own infrastructure for data exfiltration or other abuses. The ease with which these attacks can be executed means that they can come from virtually anywhere.

Insider Threat



Revenge. It's a tale as old as time. In 2022, an IT specialist was charged for allegedly hacking the server of a Chicago healthcare organization. He'd had access to the server because he'd been a contractor, and he had motive. He'd been denied a job at the organization, and a few months later, he was fired by the contracting IT firm. This act of individual retaliation resulted in a cyberattack that dramatically disrupted medical examinations, treatments and diagnoses for many patients. The attacker could face up to 10 years in federal prison if convicted.

Insider Threat

What you need to know:

An insider threat attack is a malicious assault carried out by insiders with authorized access to your bank's computer system, network and resources. In this assault, attackers often aim to pilfer classified, proprietary or otherwise sensitive information and assets, either for personal gain or to provide information to competitors. They might also try to sabotage your organization with system disruptions that mean loss of productivity, profitability and reputation.

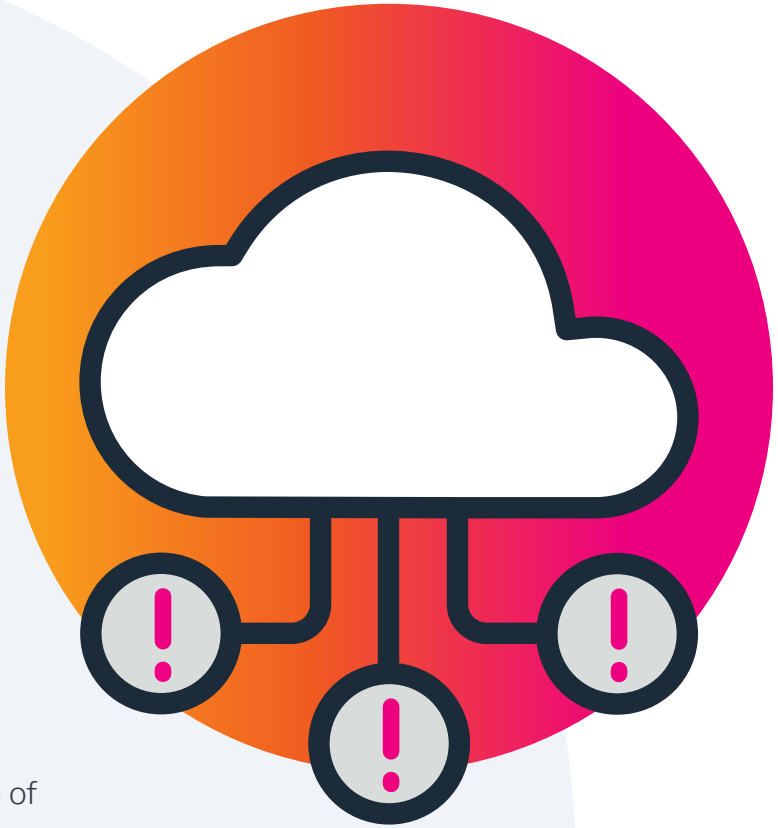
How the attack happens:

Malicious insiders have a distinct advantage in that they already have authorized access to your company's network, information and assets. They may have accounts that give them access to critical systems or data, making it easy for them to locate it, circumvent security controls and send it outside of the organization.

Where the attack comes from:

Inside attackers can be employees in the organization with bad intentions or cyberspies impersonating contractors, third parties or remote workers. They may work autonomously, or as part of nation-states, crime rings or competing organizations. While they might also be remote third-party suppliers or contractors located all over the world, they usually have some level of legitimate access to the organization's systems and data.

IoT Threats



After a data leak exposed the personal information of over 3,000 users of Ring, a home security provider owned by Amazon, hackers took advantage of the leak and hijacked video doorbells and smart cameras in people's homes. Thousands of organizations remain at risk thanks to their Ring devices, which researchers say these documented attacks are just the tip of the iceberg. Ring has since introduced end-to-end video encryption to help protect against future hacks, but with the increasing ubiquity of IoT devices, this won't be the last of these kinds of attacks.

What you need to know:

There are an estimated 15.14 billion connected IoT devices globally — a number that is projected to increase to 30 billion by 2030. These devices often lack security infrastructure, creating glaring vulnerabilities in the network that exponentially grow the attack surface and leave it susceptible to malware. Attacks delivered over IoT devices can include DDoS, ransomware and social engineering threats.

How the attack happens:

Hackers and malicious nation-states can exploit vulnerabilities in connected IoT devices with sophisticated malware to gain access to a network so they can monitor users or steal intellectual property, classified or personally identifying data and other critical information. Once they infiltrate an IoT system, hackers can also use their newly gained access for lateral movement to other connected devices or to gain entry to a greater network for various malicious purposes

Where the attack comes from:

Attacks can come from anywhere in the world. But because many verticals such as government, manufacturing and healthcare are deploying IoT infrastructure without proper security protections, these systems are targets for attacks by hostile nation-states and sophisticated cybercrime organizations. Unlike attacks against technology infrastructure, attacks against connected civic or healthcare systems could lead to widespread disruption, panic and human endangerment.

Macro Viruses

One of the most infamous virus incidents of all time, the Melissa virus of the late '90s, was none other than a macro virus. A Melissa-infected PC would hijack the user's Microsoft Outlook email system and send virus-laden messages to the first 50 addresses in their mailing lists. The virus propagated at an incredible speed, and caused astounding damage worldwide: an estimated $80 million for cleaning and repairing affected systems and networks. Though the heyday of the macro virus may have passed, these attacks still persist, and they're not just targeting Microsoft Windows now — recent attacks are targeting Mac users as well.

Macro Viruses

What you need to know:

A macro virus is a computer virus written in the same macro language that is used for software applications. Some applications, like Microsoft Office, Excel and PowerPoint allow macro programs to be embedded in documents such that the macros are run automatically when the document is opened, and this provides a distinct mechanism by which malicious computer instructions can spread. This is one reason it can be dangerous to open unexpected attachments in emails, or emails from unrecognized senders. Many antivirus programs can detect macro viruses, however the macro virus' behavior can still be difficult to detect.

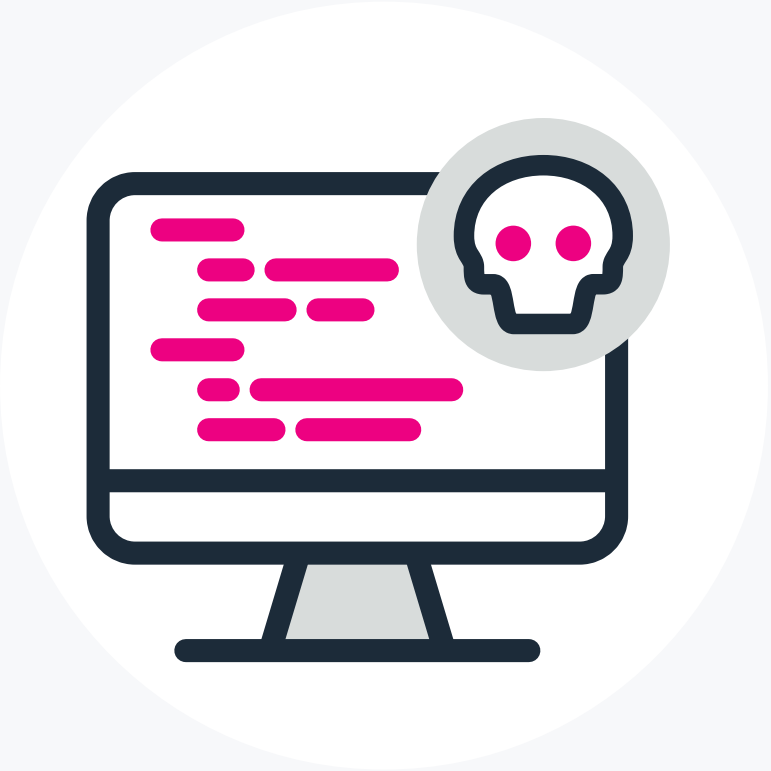
How the attack happens:

Macro viruses are often spread through phishing emails containing attachments that have been embedded with the virus. Because the email looks like it came from a credible source, many recipients open it. Once an infected macro is executed, it can jump to every other document on the user's computer and infect them. Macro viruses spread whenever a user opens or closes an infected document. They run on applications and not on operating systems. The most common methods of spreading macro viruses are sharing files on a disk or network and opening a file attached to an email.

Where the attack comes from:

While macro viruses have fallen out of vogue for malicious attacks — primarily because antivirus software is better able to detect and disable them — they still represent a major threat. A cursory Google search for "macro virus" yields instructions for creating macro viruses and tools that assist non-coders in creating these viruses. In theory, anyone with internet access can create a macro virus with ease.

Malicious Powershell



Attack sequences that exploit the ever-popular PowerShell are broadly attractive to top cybercriminals and cyberespionage groups because they make it easy to propagate viruses across a network. Notorious bad actors such as APT29 (aka Cozy Bear) use PowerShell scripts to gather critical intelligence to inform even more sophisticated cyberattacks. In 2020, the notorious threat group APT35 (aka “Charming Kitten”) abused Powershell in a ransomware attack on a charity organization and to harvest and exfiltrate data from a U.S. local government.

Malicious Powershell

What you need to know:

PowerShell is a command-line and scripting tool developed by Microsoft and built on .NET (pronounced “dot net”), that allows administrators and users to change system settings as well as to automate tasks. The command-line interface (CLI) offers a range of tools and flexibility, making it a popular shell and scripting language. Bad actors have also recognized the perks of PowerShell — namely, how to operate undetected on a system as a code endpoint, performing actions behind the scenes.

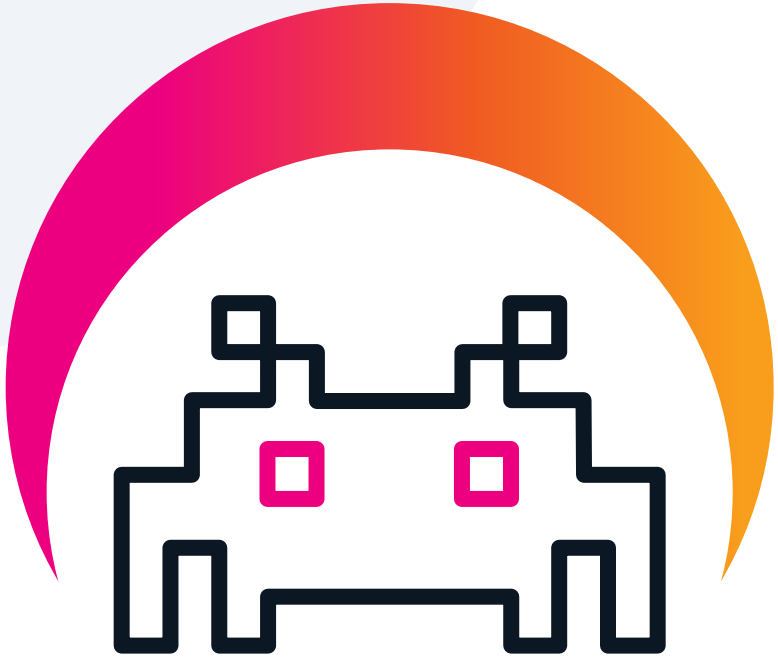
How the attack happens:

Since PowerShell is a scripting language that runs on the majority of enterprise machines — and since most companies don’t monitor code endpoints — the logic behind this type of attack is abundantly clear. It’s easy to gain access, and even easier for attackers to take root in the system. Malware doesn’t need to be installed in order to run or execute the malicious script. This means the hacker can effortlessly bypass detection — circumventing the analysis of executable files to wreak havoc at their leisure.

Where the attack comes from:

This type of attack is more sophisticated than other methods, and is usually executed by a power hacker who knows exactly what they’re doing (versus an amateur who might resort to brute force attacks). Ever stealth in their approach, they’re adept at covering their tracks, and know how to move laterally across a network.

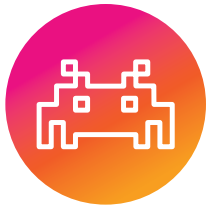
Malware



First identified in 2014 as a banking trojan targeting consumers, Emotet is a type of malware that has reinvented itself as a persistent and pervasive threat to *both* the private and public sector. The Department of Homeland Security reported that Emotet is one of the most costly and destructive types of malware, costing upwards of $1M per incident.

Emotet has attacked government agencies across France, Japan, Canada and New Zealand, as well as companies in the private sector, including pharmaceutical, manufacturing, technology and financial services. U.S. and European law enforcement agencies disrupted the Emotet network in February 2021, halting communications and its ability to spread. Emotet returned in 2023, with the botnet once again resuming its shady practices.

Malware



What you need to know:

Various types of malware allow for spying, backdoor administrative control and unfettered, unauthorized remote access to a target's device. Once the attackers gain control of the machine or machines in question, they can install and remove programs, hijack webcams, manipulate files, and harvest login credentials and other sensitive data. Hackers can also impersonate legitimate users in order to easily download additional malware, compromising other computers and devices across the network.

How the attack happens:

Malware, distributed through advanced phishing tactics, is designed to steal sensitive information — which includes user credentials, screenshots, webcam access, audio, geolocation and keylogging data. One of their most common phishing tactics is to lure users into opening a file packaged up as Microsoft Office documents — primarily PowerPoint and Word. Attackers can also deploy malware to enterprises through spearphishing campaigns and drive-by downloads, as well as through traditional remote service-based exploitation.

Where the attack comes from:

Given the popularity and pervasiveness of malware, this tactic is as insidious as it is common. If you see a suspicious email in your inbox with a file extension, be sure to check that it's from a trusted sender before you open, and possibly unleash what could be malware onto your network.

Man-in-the-Middle Attack

In early 2022, Microsoft discovered a phishing campaign targeting Office365 users. The attackers spoofed a phony 365 login page, gathering credentials for later abuse and misuse. To do this, the attackers used a Evilginx2 phishing kit — a man-in-the-middle (MITM) attack framework used for phishing login credentials along with session cookies, allowing bad actors to bypass two-factor authentication — in order to hijack the authentication process. Microsoft added in its blog post, "Note that this is not a vulnerability in MFA; since AiTM phishing steals the session cookie, the attacker gets authenticated to a session on the user's behalf, regardless of the sign-in method the latter uses."

Man-in-the-Middle Attack

What you need to know:

The MITM attack, also known as adversary-in-the-middle (AiTM), sets up a proxy server that intercepts the victim's log-in session, so that the malicious actor can act as a relay between the two parties or systems — thereby gaining access to and/or pilfering sensitive information. This type of attack allows a malicious actor to intercept, send and receive data intended for somebody else — or that's not meant to be sent at all — without either outside party knowing, until it is too late.

How the attack happens:

Virtually anyone could execute a man-in-the-middle attack. Since the implementation of HTTPS Everywhere, however, these kinds of attacks are more difficult to execute, and are therefore more rare. In an MITM attack, the hacker sits between the user and the real website (or other user) and passes the data between them, exfiltrating whatever data they like from the interaction.

Where the attack comes from:

Because improvements in security technologies have made MITM attacks more difficult to execute, the only groups attempting them are sophisticated hackers or state actors. In 2018, the Dutch police found four members of the Russian hacking group Fancy Bear parked outside of the Organization for the Prohibition of Chemical Weapons in Holland, attempting an MITM infiltration to steal employee credentials. Later that year, the U.S. and UK governments released warnings that Russian state-sponsored actors were actively targeting routers in homes and enterprises for the purpose of MITM exfiltration.

Masquerade Attack

Scammers often masquerade as representatives from software companies in order to dupe unsuspecting users into downloading malware disguised as email attachments. One recent trend involved Microsoft and Adobe. “Scammers send out Microsoft OneNote files as email attachments to victims, triggering malware downloads when someone opens the attachment,” Avast, a well-known antivirus and security company, reported in early 2023. Since then, masquerade attacks continue to be on the rise.

Masquerade Attack

What you need to know:

A masquerade attack happens when a bad actor uses a forged or legitimate (but stolen) identity to gain unauthorized access to someone's machine or an organization's network via legitimate access identification. Depending on the level of access the permissions provide, masquerade attacks could give attackers access to an entire network.

How the attack happens:

A masquerade attack can happen after users' credentials are stolen, or through authenticating on unguarded machines and devices which have access to the target network.

Where the attack comes from:

From an insider angle, attackers can get access by spoofing login domains or using keyloggers to steal legitimate authentication credentials. The attacks can also happen physically by taking advantage of targets who leave machines unguarded — like a coworker accessing someone's laptop while they're away. Generally speaking, weak authentication methods that can be duped by external parties are usually the source of the problem.

Meltdown and Spectre Attack

Most cybersecurity attacks exploit a vulnerability, such as a coding mistake or bad design. But not all attacks are created equal. Two Google researchers discovered a new type of attack that affected all computer chip makers and potentially exposed billions to the meltdown and spectre attack.

Meltdown and Spectre Attack

What you need to know:

The meltdown and spectre attack exploits vulnerabilities in computer processors. These vulnerabilities allow attackers to steal almost any data that is being processed on the computer. This is an attack that strikes at the core of computer security, which relies on the isolation of memory to protect a user's information. A "meltdown" refers to the breakdown of any protective barrier between an operating system and a program, while "spectre" indicates the breakdown between two applications that keep information from each other.

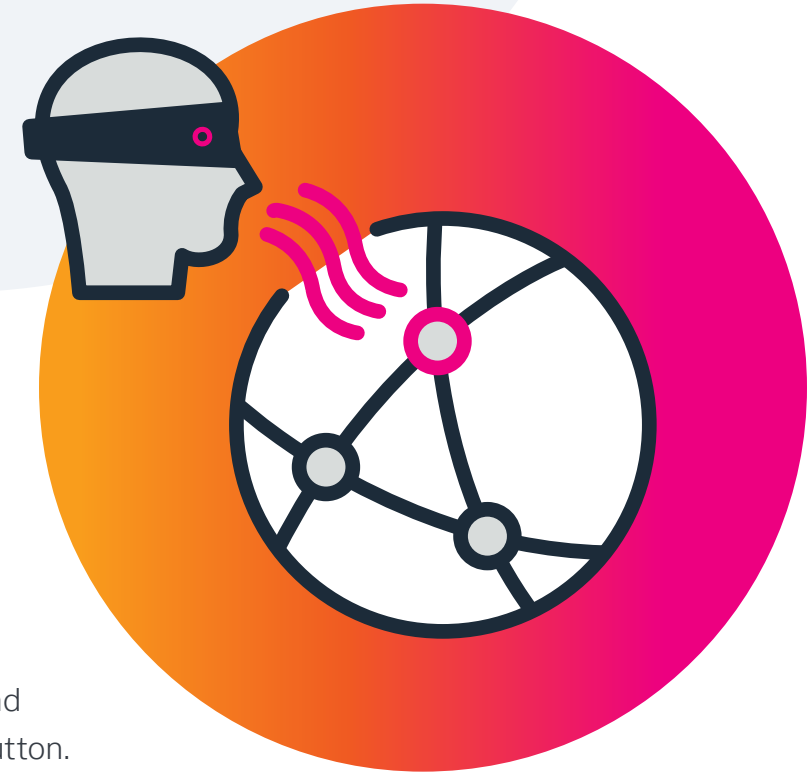
How the attack happens:

A meltdown and spectre attack exploits critical vulnerabilities in modern CPUs that allow unintended access to data in memory storage. The attack breaks the norm of computing where programs are not allowed to read data from other programs. The type of information that attackers typically target are passwords stored in a password manager or browser as well as emails, financial records and personal information such as photos and instant messages. But this attack is not limited to personal computers. It can target almost any device with a processor, such as a mobile phone or tablet.

Where the attack comes from:

The spectre and meltdown attack can originate from nearly anywhere, and much of the research thus far has focused on this attack's unique nature instead of who's behind it.

Network Sniffing



Smart locks are a new type of device intended to protect your home and make it easier to enter with the click (or, more appropriately, tap) of a button. But taking a more futuristic approach to fortifying your house can have serious consequences, security researchers have found. One smart lock, not-so-aptly marketed as the “smartest lock ever,” could be intercepted via network traffic between the mobile app and the lock itself. Scarier yet, this can be done through inexpensive, readily available network-sniffing devices.

Network Sniffing

What you need to know:

Network sniffing, also known as packet sniffing, is the real-time capturing, monitoring and analysis of data flowing within a network. Whether it's via hardware, software or a combination of both, bad actors use sniffing tools to eavesdrop on unencrypted data from network packets, such as credentials, emails, passwords, messages and other sensitive information.

How the attack happens:

Much like wiretapping scenarios in which someone listens in on phone calls for sensitive details, network sniffing works in the background, silently listening in as information is exchanged between entities on a network. This happens when attackers place a sniffer on a network via the installation of software or hardware plugged into a device that allows it to intercept and log traffic over the wired or wireless network the host device has access to. Due to the complexity inherent in most networks, sniffers can sit on the network for a long time before being detected.

Where the attack comes from:

Network sniffing is often conducted legally by organizations like ISPs, advertising agencies, government agencies and others who need to verify network traffic.

But it can also be launched by hackers doing it for the "lulz" or nation-states looking to pilfer intellectual property. Like ransomware, network sniffers can be injected into the network by getting the right person to click on the right link. Insider threats with access to sensitive hardware could also be a vector for attack.

Open Redirection

In 2022, yet another phishing campaign targeting Facebook users was discovered to have netted hundreds of millions of credentials. The technique used was a common one: A link is sent via DM from a compromised Facebook account, then that link performs a series of redirects, often through malvertising pages to rack up views and clicks (and revenue for the attacker), ultimately landing on a fake page. Though the technique of host redirection, also known as open redirect, isn't new, the sheer scale of this campaign is remarkable. Researchers found that just one phishing landing page out of around 400 had 2.7 million visitors in 2021, and 8.5 by June of 2022. In an interview with researchers, the attacker boasted of making $150 for every thousand visits from US Facebook users, which would put the bad actor's total earnings at $59 million.

Open Redirection

What you need to know:

Host redirection attacks are very common and increasingly subversive, as hackers become more creative about how they lure their targets. Attackers use URL redirection to gain a user's trust before they inevitably strike. They'll typically use embedded URLs, an .htaccess file or employ phishing tactics in order to redirect traffic to a malicious website.

How the attack happens:

The hacker might send a phishing email that includes a copycat of the website's URL to the unsuspecting victim. If the website appears legitimate, users might inadvertently share personal information by filling out any prompts or forms that appear. Attackers can take this to the next level by embedding faux command-and-control domains in malware, and hosting malicious content on domains that closely mimic corporate servers.

Where the attack comes from:

The origins of this attack are not as important as the target. This attack is usually aimed at unsophisticated internet users who won't notice that the URL of their favorite domain is a letter or two off. And because this attack prides itself on simplicity (it can be as easy as registering a domain name), it can originate from almost anywhere.

Pass the Hash

The infamous breach of over 40 million Target customer accounts was successful partly due to the well-known attack technique called pass the hash (PtH). The hackers used PtH to gain access to an NT hash token that would allow them to log-in to the Active Directory administrator's account without the plaintext password — thereby giving them the necessary privileges to create a new domain admin account, later adding it to the Domain Admins group. This root in the system gave them the opportunity to steal personal information and payment card details from Target's customers.

Pass the Hash

What you need to know:

Pass the hash allows an attacker to authenticate a user's password with the underlying NTLM or LanMan hash instead of the associated plaintext password. Once the hacker has a valid username along with their password's hash values, they can get into the user's account without issue, and perform actions on local or remote systems. Essentially, hashes replace the original passwords that they were generated from.

How the attack happens:

On systems using NTLM authentication, a user's password or passphrase is never submitted in cleartext. Instead, it's sent as a hash in response to a challenge-response authentication scheme. When this happens, valid password hashes for the account being used are captured using a credential access technique.

Where the attack comes from:

This type of attack is more sophisticated than other methods, and is usually executed by highly organized, motivated threat groups with their sights set on a specific organization or person, and with a mind to political or financial gain.

Phishing

In June 2022, Twilio — a customer engagement platform — experienced their second major breach. The “0ktapus” hackers, responsible for both incidents, successfully accessed customer data by utilizing voice phishing — i.e., impersonating Twilio’s IT department over a phone call — in order to deceive an employee. Thinking they were speaking to a legitimate representative, the employee provided the theat group with corporate login details. This breach led to unauthorized access to a limited number of customer contact details.

Phishing

What you need to know:

A phishing attack tricks everyday consumers, users or employees into clicking on a malicious link, often driving them to a bogus site to provide personally identifiable information such as banking account numbers, credit card information or passwords, delivered via email, direct message or other communication. Be wary — while these bogus sites may look convincing, attackers will harvest any information you submit to them. Or they may launch malware aimed at stealing funds from your accounts, personally identifiable customer information or other critical assets.

How the attack happens:

Typically you'll be lured by an email impersonating someone you know — a message that appears to be from a manager or coworker, for example — compelling you to open malicious attachments or click links that lead you to webpages practically identical to legitimate sites.

Where the attack comes from:

Just a few decades ago, a large number of phishing attacks were sourced to Nigeria in what were known as 419 scams, due to their fraud designation in the Nigerian criminal code. Today, phishing attacks originate from all over the world, with many occurring in BRIC countries (Brazil, Russia, India and China), according to the InfoSec Institute. Because of the ease and availability of phishing toolkits, even hackers with minimal technical skills can launch phishing campaigns. The people behind these campaigns run the gamut from individual hackers to organized cybercriminals.

Phishing Payloads

A unique phishing attack has emerged and attributed to the threat group TA866, where a preliminary malware payload takes screenshots of victims' devices. This allows the attackers to evaluate the potential value of the victim and decide if more malware should be deployed. To date, this campaign has targeted over 1,000 organizations in the U.S. and Germany.

Phishing Payloads

What you need to know:

Despite its simplicity, phishing remains the most pervasive and dangerous cyberthreat. In fact, research shows that as many as 91% of all successful attacks are initiated via a phishing email.

These emails use fraudulent domains, email scraping techniques, familiar contact names inserted as senders, and other tactics to lure targets into clicking a malicious link, opening an attachment with a nefarious payload, or entering sensitive personal information that perpetrators may intercept. The “payload” refers to the transmitted data that is the intended message. Headers and metadata are only sent to enable the delivery of the payload to the correct person.

How the attack happens:

This attack has a typical attack pattern: First, the attacker sends a phishing email and the recipient downloads the attached file, which is typically a .docx or .zip file with an embedded .lnk file. Second, the .lnk file executes a PowerShell script and lastly the Powershell script executes a reverse shell, rendering the exploit successful.

Where the attack comes from:

Because this attack doesn’t require a high level of sophistication, and because phishing is at the center of most attack cyberattacks, it can originate from anywhere in the world.

Spear Phishing

These days spear phishers are not only targeting bigger fish, they're taking a page from the book of romance scams, luring victims with attractive fake profiles to get them to download malware onto their computers. Researchers identified a years-long social engineering and targeted malware attack sourced to the renowned Iranian-state aligned threat actor TA456. Using a fake social media profile "Marcella Flores," TA456 built a romantic relationship with an employee of a small aerospace defense contractor subsidiary. The attacker cashed in a few months later by sending out a large malware file via an ongoing corporate email communication chain with the aim of conducting reconnaissance. Once the malware, dubbed LEMPO, infiltrated the machine, it exfiltrated data and sent highly sensitive information back to the attacker, while obfuscating its whereabouts to evade detection.

Spear Phishing

What you need to know:

A subset of phishing, spear phishing occurs when cybercriminals selectively target you with a specific, personalized email message to trick targets or a target company's employees into giving away financial or proprietary data, or unlocking access to the network. Spear phishers target individuals who either have access to sensitive information or are weak links to the network. High-value targets, such as C-level executives, company board members or administrators with elevated privileges, are especially vulnerable, since they have access to critical systems and proprietary information.

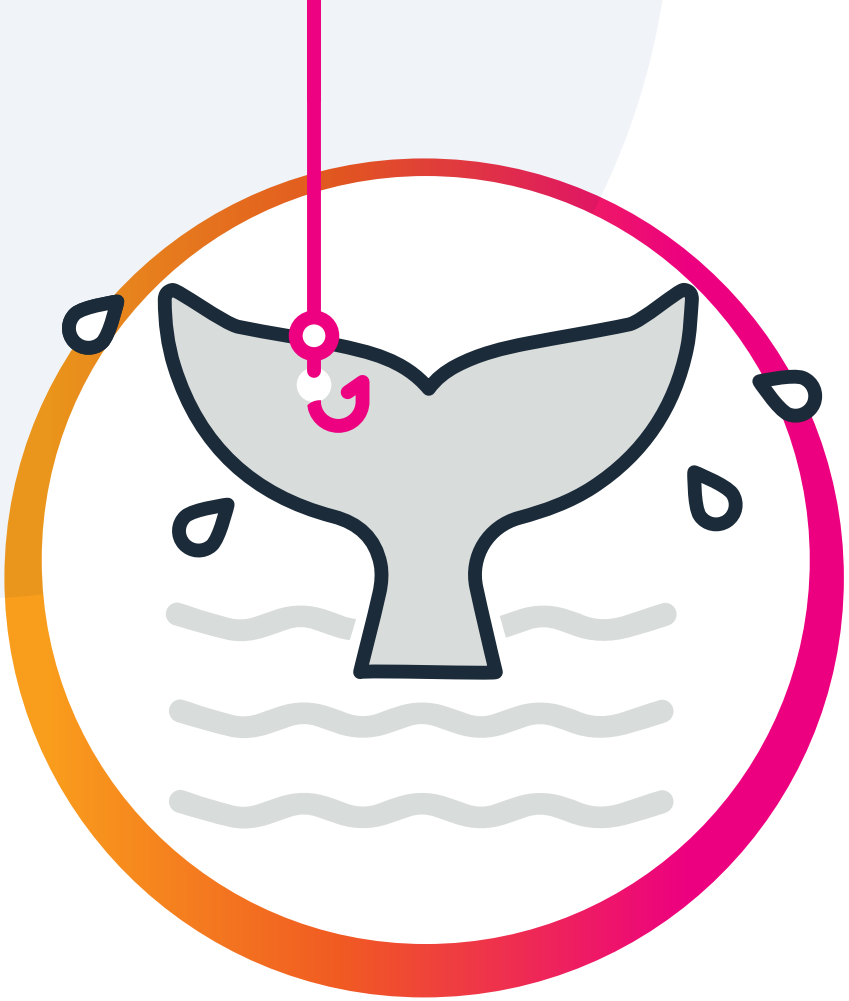
How the attack happens:

Spear phishers do their research to identify targets and their professional positions using social media sites like LinkedIn. From there, they spoof addresses to send highly personalized, authentic-looking messages to infiltrate the target's infrastructure and systems. Once hackers gain access to the environment, they attempt to carry out even more elaborate schemes.

Where the attack comes from:

Individuals and organizations alike are behind this attack. However, many high-profile spear phishing attempts are sourced to state-sponsored cybercrime organizations, which have the resources to research their targets and bypass strong security filters.

Whale Phishing (Whaling)



Why go after little phish when you can phish a whale? Australian hedge fund Levitas Capital found that out the hard way when attackers launched a stealthy whaling attack aimed directly at one of the founders. The bad actors gained entry to the hedge fund's network after sending the executive a fake Zoom link that installed malware once it was clicked. The malicious code allowed the attackers to infiltrate the targeted email account and subsequently create bogus invoices to the fund's trustee and third party administrator, which initiated and approved cash transfer requests resulting in $8.7 million in theft. The bogus invoices also included a request for a $1.2 million payment to suspicious private equity firm Unique Star Trading. The losses were so damaging and extensive that the firm was eventually forced to permanently close.

Whale Phishing (Whaling)

What you need to know:

Whaling is when hackers go after one single, high-value target, such as a CEO of a financial services firm. The target is always someone specific, whereas a phishing email may go after anyone at a company. The hackers also usually go after high-profile targets because they may possess important or sensitive information.

How the attack happens:

The technique used in a whaling attack is a classic phishing practice. The target receives an authentic-looking email, usually asking him or her to click on a link that contains malicious code or leads to a website that asks for sensitive information, such as a password.

Where the attack comes from:

Phishing is the most common entry point for a cyberattack, which means a whaling attack can originate from anywhere in the world.

The Levitas Capital attack, for example, was sourced to a collective of cybercriminals from various regions, with payments sent to Bank of China and United Overseas Bank in Singapore.

Privileged User Compromise

In 2022, the criminal hacking group Lapsus$, allegedly run by a teenager from Oxford, England, boasted publically that it had successfully hacked Okta, a single sign-on provider used by thousands of organizations and governments worldwide. Lapsus$ gained access to a “super user” administrative account for Okta via a third-party support engineer and had access to the employee’s laptop for five days, including privileged access to some Okta systems. The cybercrime group posted about the attack on its Telegram channel, even going so far as to post screenshots showing it was inside Okta’s systems. But it wasn’t after Okta, exactly — the real targets were Okta’s 15,000 customers. A week later, the hacking group added 15 thousand followers to their Telegram channel, raising fears that more attacks are imminent.

Privileged User Compromise

What you need to know:

It's widely accepted that many serious data breaches can be traced back to the abuse of privileged credentials. These are accounts with elevated privileges, such as users with domain administrator rights or root privileges. Attackers are increasingly using privileged user credentials to access an organization's resources and information and exfiltrate sensitive data. An attacker that gains access to privileged user credentials can take control of an organization's infrastructure to modify security settings, exfiltrate data, create user accounts and more, all the while appearing legitimate — and therefore harder to detect.

How the attack happens:

Attackers attempt to gain access to privileged accounts by using social engineering techniques, sending spear-phishing messages, using malware, or "pass the hash" attacks. Organizations have opened their networks to cope with an increasingly mobile, remote workforce, and enable a complex web of remote access used by suppliers and service providers. Many of those connections, including to the cloud, are accessed through powerful privileged account credentials, and finding, controlling and monitoring access to them all is challenging, giving bad actors plenty of openings.

Once armed with the credentials, attackers get in and grab what they can, such as SSH keys, certificates and domain administration hashes. And it takes only one successful account hit to cause a major data breach that can bring an organization to its knees.

Where the attack comes from:

Because it provides attackers with hard to detect, wide access to all kinds of data privilege, user compromise is widely appealing and commonly used in cyber attacks of various kinds, whether nation-state cyber espionage motivated by political ideology or sophisticated, financially-motivated cybercrime groups like Lapsus$.

Ransomware

According to cybersecurity company Emsisoft, ransomware attacks affected at least 948 government agencies, educational establishments and healthcare providers in the United States in 2019, at a potential cost exceeding $7.5 billion.

In the medical sector, the potential effects of these kinds of attacks include patients being redirected to other hospitals, medical records being made inaccessible (or permanently lost) and emergency dispatch centers relying on printed maps and paper logs to keep track of emergency responders in the field. In government, local 911 services can be disrupted. And according to Manhattan D.A. Cyrus Vance Jr., the effect of ransomware could be as devastating and costly as a natural disaster like Hurricane Sandy.

Ransomware

What you need to know:

Ransomware is an attack where an infected host encrypts a victim's data, holding it hostage until they pay the attacker a fee. Recent ransomware attacks have demonstrated that hackers have begun threatening to leak or sell the stolen data, increasing the potential damage of these kinds of attacks by orders of magnitude.

There are countless types of ransomware, but certain groups are especially nefarious. One well-known gang, Blackmatter, has targeted a number of organizations critical to the U.S. economy and infrastructure, including the food and agriculture industry. Ryuk is another type of ransomware to watch out for. As of 2019, Ryuk had the highest ransom on record at $12.5 million.

How the attack happens:

Attackers can deploy ransomware to businesses and individuals through spear phishing campaigns and drive-by downloads, as well as through traditional remote service-based exploitation. Once the malware is installed on the victim's machine, it either prompts the user with a pop-up or directs them to a website, where they're informed that their files are encrypted and can be released if they pay the ransom.

Ransomware as a Service (RaaS), on the other hand, is a business model between ransomware operators and affiliates in which affiliates pay to launch ransomware attacks developed by operators. RaaS kits allow affiliates lacking the skill or time to develop their own ransomware variant to be up and running quickly and affordably. A RaaS kit may include 24/7 support, bundled offers, user reviews, forums and other features identical to those offered by legitimate SaaS providers.

Where the attack comes from:

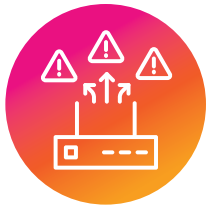
Ransomware has typically been the work of advanced cybercriminal groups — who remain anonymous after extorting governments or major enterprises requires technological sophistication. However, since the arrival of cryptocurrencies, which simplify anonymous transactions, the general population is at greater risk of ransomware attack.

Because RaaS kits are relatively easy to use and very easy to find on the dark web, where they are widely advertised, this attack could come from any beginning hacker with the money to buy a kit.

Router and Infrastructure Attacks

Cisco was the victim of a router and infrastructure attack in which a router "implant," dubbed SYNful Knock, was reportedly found in 14 routers in four different countries. SYNful Knock is a type of persistent malware that allows an attacker to gain control of an affected device and compromise its integrity with a modified Cisco IOS software image. Mandiant describes it as having different modules enabled via the HTTP protocol and triggered by crafted TCP packets sent to the device.

Router and Infrastructure Attacks



What you need to know:

Router implants have been rare, and are largely believed to be theoretical in nature and use. However, recent vendor advisories indicate that these have been seen in the wild. Attackers probably access these devices by identifying known vulnerabilities or by targeting devices with default or weak passwords that are simple to guess. The router's position in the network makes it an ideal target for re-entry or further infection.

How the attack happens:

Networking devices, such as routers and switches, are often overlooked as resources that attackers will leverage to subvert an enterprise. Attackers compromise network devices and can then obtain direct access to the company's internal infrastructure — effectively increasing the attack surface and accessing private services/data.

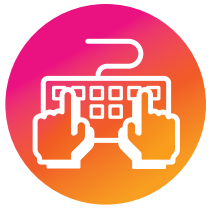
Where the attack comes from:

Advanced threats actors have shown a proclivity to target these critical assets as a means to siphon and redirect network traffic, flash backdoored operating systems and implement cryptographic weakened algorithms to more easily decrypt network traffic.

Shadow IT

As software as a service (SaaS) applications have become increasingly quick and easy to use, employees can now download solutions onto their workstations to help them get the job done. However, many are using these applications with little regard for security. It's not surprising then that a Forbes Insights survey titled "Cyber Resilience Perception Gaps: What Could Go Wrong?" found that more than one in five organizations experienced a cyber incident originating from an unauthorized — or "shadow" — IT resource.

Shadow IT



What you need to know:

Shadow IT refers to IT applications and infrastructure that employees use without the knowledge and/or consent of their organization's IT department. These can include hardware, software, web services, cloud applications and other programs. In general, well-intentioned employees innocently download and use these applications to make their work easier or more efficient. It's a phenomenon so pervasive that Gartner had estimated that a third of all enterprise cybersecurity attacks would be from shadow IT. Because users are accessing these applications largely under the radar, they are often unintentionally opening the floodgate for insider threats, data breaches and compliance violations.

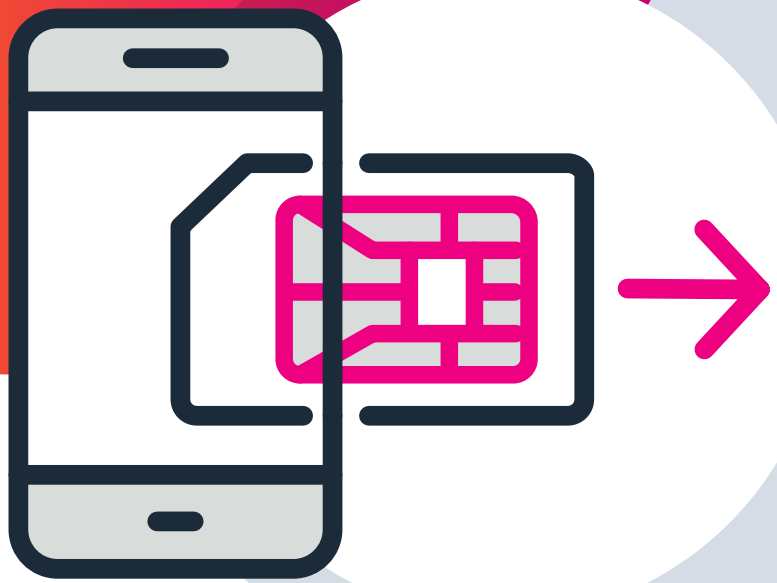
How the attack happens:

As the name suggests, the secretive nature of shadow IT is due to employees sharing or storing data on unauthorized cloud services, setting the stage for a host of security and compliance risks. Breaches can occur when employees upload, share or store critical or regulated data into shadow IT apps without appropriate security and data loss prevention (DLP) solutions. The exposed information then provides an easy target for insider threats and data theft, and can also lead to costly compliance violations. In addition, the applications themselves might be fraught with endpoint vulnerabilities and security gaps.

Where the attack comes from:

In this case, the threat originates from within an organization. Employees using shadow IT apps often do so to get around a prohibitive policy or to get work done faster — not necessarily to put their employers and coworkers at risk. However, they ultimately leave the door wide open for malicious insiders or external hackers looking to exploit security holes in these systems.

Simjacking



On August 30, 2019, Twitter CEO Jack Dorsey's 4.2 million followers were subjected to a stream of deeply offensive messages, courtesy of a group of hackers called the "Chuckling Squad." The group used simjacking to gain control of Dorsey's phone number, then used a text-to-tweet service acquired by Twitter to post the messages. Despite the messages being visible online for fewer than ten minutes, millions of people were exposed to the offensive tweets.

Simjacking

What you need to know:

SIMjacking (also known as a SIM swap scam, port-out scam, SIM splitting and SIM swapping) is a type of account takeover that generally targets a weakness in two-factor authentication and two-step verification in which the second factor is a text message (SMS) or call placed to a mobile telephone. Simply put, simjacking is when an attacker impersonates a target to a cellular provider in order to steal their cell phone number by having it transferred to a different SIM card (which is already in the hacker's possession).

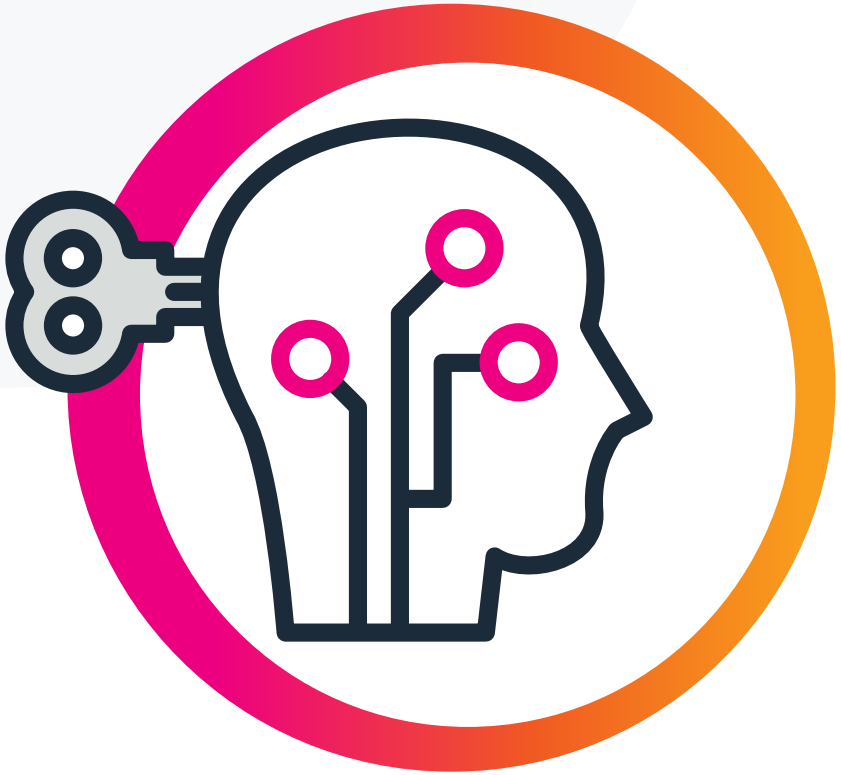
How the attack happens:

A hacker calls the support line for a mobile service provider, pretending to be the target, saying they've lost their SIM card. They can verify their identity because they have acquired some amount of the target's personal information (address, passwords or SSN) through one of the many database hacks in the last decade. The service provider's employee, having no way of knowing that the person on the other end of the line is not who they say they are, makes the switch. Instantly, that phone number — the key associated with so much of digital life — is under the attacker's control.

Where the attack comes from:

Simjackers are typically looking to extort victims for something of great value — like Bitcoin or other cryptocurrency wallets or high-value social media accounts — or to cause harm to their reputations, as Chuckling Squad did with Jack Dorsey. These hackers can come from anywhere in the world, and can be members of organized groups or solitary actors.

Social Engineering Attack



In July 2022, CoinsPaid — a cryptocurrency payment system — lost $37 million due to a social engineering attack. The threat actors presented a fake job offer to an existing employee, but not before tricking them into installing malicious software on their company computer. “Although you may think that such an attempt to install malicious software on the employee’s computer is obvious,” the company revealed, “the hackers had spent six months learning all possible details about CoinsPaid, our team members, our company’s structure and so on.”

Social Engineering Attack

What you need to know:

Social engineering is the term used for a broad range of malicious activities accomplished through psychological manipulation to trick users into making security mistakes or giving away sensitive information. What makes social engineering especially dangerous is that it relies on human error, rather than vulnerabilities in software and operating systems. Mistakes made by legitimate users are much less predictable, making them harder to identify and thwart than a malware-based intrusion.

How the attack happens:

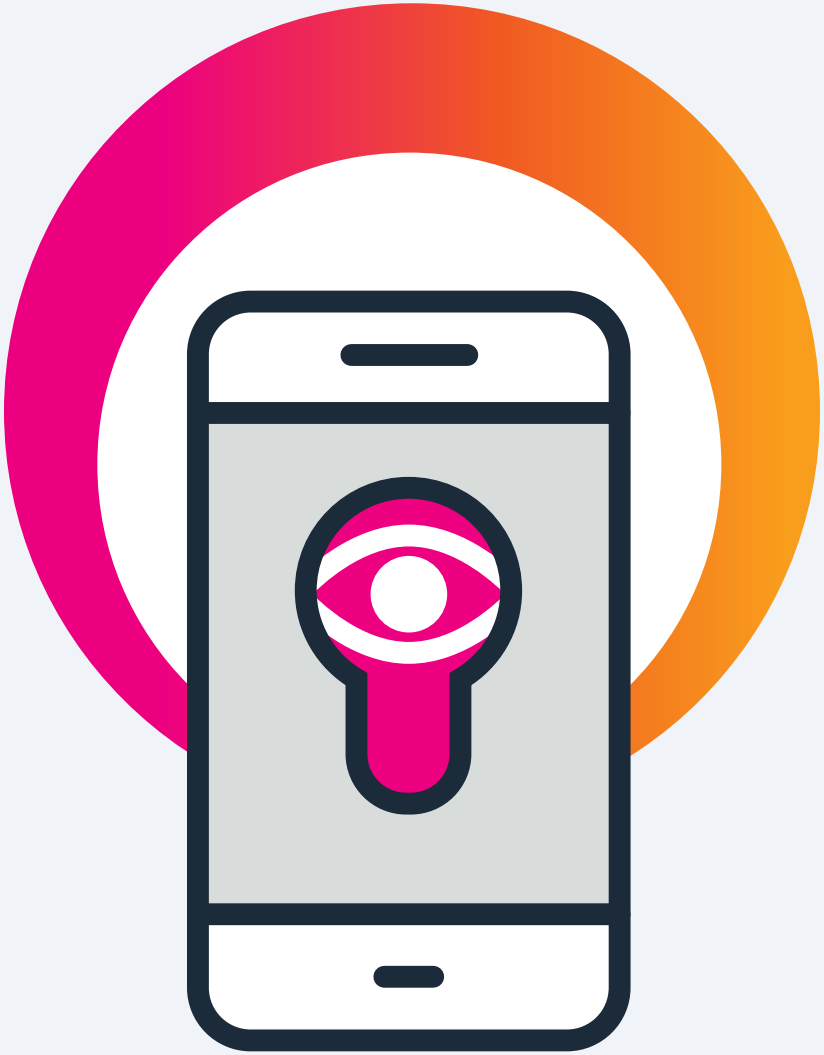
Social engineering attacks come in many different forms and can be performed anywhere where human interaction is involved. The following are five common forms of digital social engineering assaults. A perpetrator first investigates the intended victim to gather the necessary background information — such as potential points of entry and weak security protocols — needed to proceed with the attack. Then, the attacker gains the victim's trust and provides stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.

Where the attack comes from:

Social engineering can take many forms and come from many sources and motivations. Most commonly, it comes in the form of phishing emails. Other forms include pretexting, where the attacker creates a good pretext to steal important data; baiting and quid pro quo, in which the attacker offers the victim something desirable in exchange for providing login credentials; and tailgating or piggybacking, in which an attacker gains access to a restricted area of a business by following an authenticated employee through secure doors.

Spyware

It's no secret that spyware attacks continue to occur with alarming frequency. But if you're a high-profile figure, you're likely a bigger target. Officials announced that bad actors had targeted the cellphones of Spanish Prime Minister Pedro Sánchez and Defense Minister Margarita Robles in several attacks using the Pegasus spyware, resulting in significant data theft from both devices while wreaking havoc on Spain's administrators and government systems.



Spyware

What you need to know:

Spyware is a type of malware that aims to gather personal or organizational data, track or sell a victim's web activity (e.g., searches, history and downloads), capture bank account information and even steal a target's identity. Multiple types of spyware exist, and each one employs a unique tactic to track the victim. Ultimately, spyware can take over a device, exfiltrating data or sending personal information to another unknown entity without prior knowledge or consent.

How the attack happens:

Spyware can install itself on a victim's device through various means, but will commonly get a foothold in a system by duping the target or exploiting existing vulnerabilities. This can happen when a user carelessly accepts a random prompt or pop-up, downloads software or upgrades from an unreliable source, opens email attachments from unknown senders, or pirates movies and music.

Where the attack comes from:

Thanks to crimeware kits that are now readily available, this type of attack can come from anyone and anywhere. But more often than not, they'll originate from nefarious organizations looking to sell a victim's information to a third-party.

SQL Injection

Structured Query Language, or SQL (sometimes pronounced “sequel”), is the standard programming language used to communicate with relational databases — systems that support every data-driven website and application on the internet. An attacker can take advantage of this (very common) system by entering a specific SQL query into the form (injecting it into the database), at which point the hacker can access the database, network and servers. And SQL injection attacks continue to be a popular attack method. As recently as August of 2020, the Freepik Company disclosed a data breach impacting the logins of more than eight million users resulting from an SQL injection in a global database of customizable icons, which allowed the miscreants to access and ultimately steal user login and personal information.

SQL Injection

What you need to know:

SQL injection is a type of injection attack used to manipulate or destroy databases using malicious SQL statements. SQL statements control the database of your web application and can be used to bypass security measures if user inputs are not properly sanitized.

How the attack happens:

A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data, execute administration operations on the database, recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system.

Where the attack comes from:

Because so much of the internet is built on relational databases, SQL injection attacks are exceedingly common. Searching the Common Vulnerabilities and Exposures database for "injection" returns 15,000 results.

Supply Chain Attack

The SolarWinds attacks, which some experts have called the worst series of cybersecurity attacks in history, are a prime example of the damage a supply chain attack can inflict. In 2020, sophisticated attackers believed to have been directed by the Russian intelligence service compromised SolarWinds software. They embedded it with malware that was then deployed through a product update, giving them backdoor access to all of SolarWinds Orion Platform customers' networks. Up to 18,000 customers installed updates that left them vulnerable to hackers, including Fortune 500 companies and multiple agencies in the U.S. government. As Tim Brown, vice president of security at SolarWinds, said, "it's really your worst nightmare."

Supply Chain Attack

What you need to know:

A supply chain attack is a powerful cyberattack that can breach even the most sophisticated security defenses through legitimate third-party vendors. Because vendors need access to sensitive data in order to integrate with their customers' internal systems, when they are compromised in a cyberattack, often their customers' data is too. And because vendors store sensitive data for numerous customers, a single supply chain attack gives hackers access to the sensitive data of many organizations, across many industries. The severity of supply chain attacks cannot be overstated. And the recent spate of these attacks suggests this method is now the state actors' attack du jour.

How the attack happens:

A supply chain attack uses legitimate, trusted processes to gain full access to organizations' data by targeting the vendor's software source code, updates or build processes. They are difficult to detect because they happen at an offset to the attack surface. Compromised vendors then unwittingly transmit malware to their customer network. Victims can be breached through third-party software updates, application installers and through malware on connected devices. One software update can infect thousands of organizations, with minimal effort from the hacker, who now has "legitimate" access to move laterally across thousands of organizations.

Where the attack comes from:

Supply chain attacks are large-scale, sophisticated attacks perpetrated by sophisticated threat actors, often nation-state sponsored and ideologically motivated, though financial gain is also a big motivation.

Suspicious Cloud Storage Activities

According to the 2022 Verizon Data Breach Investigations Report (DBIR), a staggering 82% of breaches involve a "human element," with "miscellaneous errors" on the rise due to misconfigured cloud storage. The Sensitive Data in the Cloud report also found that the majority of security and IT professionals (67%) are storing sensitive data in public cloud environments, with a third of respondents saying that they weren't confident — or only slightly confident — about their ability to protect sensitive data in the cloud.

This type of technical and professional oversight — whether it involves a misconfigured database or security teams lacking the necessary know-how — is exactly why cloud accounts have become a prime target in this era of remote work.

Suspicious Cloud Storage Activities

What you need to know:

Now that data is widely (and all too often, haphazardly) dispersed across the cloud, attackers have ample opportunity to find and exploit both known and unknown vulnerabilities. This is especially true as organizations hurriedly migrate to the cloud, potentially compromising or misconfiguring certain security controls.

To complicate matters further, assets and applications need to be secured per the shared responsibility model, where cloud service providers (CSPs) will cover certain elements, processes and functions, but then the customer is responsible for securing its proprietary data, code and any other assets of note, per the cloud security alliance (CSA). But when that responsibility is shirked, hackers inevitably abound.

How the attack happens:

An attack on cloud storage happens when a bad actor gets a foothold within the organization's cloud infrastructure due to incorrect, lax or nonexistent security settings. Once inside, they'll start disabling certain controls, like access monitoring. They may create new accounts for continued access, while executing commands that aren't typical for the type of user or system in question. They could also change the policies of certain storage buckets, so that an organization's files are accessible to the public, leading to data exfiltration. Fortunately, these are all notable events, and will be easy to track and identify in the CSP's audit logs.

Where the attack comes from:

One example of how this can happen is if a developer runs an outdated instance of a cloud function or application. This could contain known vulnerabilities that were eventually patched in a later version. But since an older program is running, attackers can use this as an entry point before they move laterally across the cloud environment.

Typosquatting

Noblox.js is a wrapper for the Roblox API, a function widely used by many gamers to automate interactions with the popular Roblox gaming platform. The software also appears to be attracting a new crowd. In 2021, hackers launched typosquatting attacks via the noblox.js package by uploading confusingly similar packages laden with ransomware to a registry for open source JavaScript libraries, and then distributing the infected files via a chat service. However, since September of 2021, gamer Josh Muir along with several others have actively been cracking down on the attackers, attempting to prevent the proliferation of ransomware through the noblox.js package and other code libraries, and thwart further attacks on the gaming community.

Typosquatting

What you need to know:

Typosquatting is a phishing attack where attackers take advantage of commonly misspelled domain names. Oftentimes, the guilty party isn't actually looking to carry out an attack, but instead is holding out hope that a company, brand or person will buy the domain off them. But in other cases, thieves create malicious domains that closely resemble those of legitimate brands.

How the attack happens:

This is not a sophisticated attack. It can be as simple as a 14-year-old registering a domain and then installing malicious code on said domain. The malicious form of this attack usually involves a hacker using faux domains to mislead users into interacting with malicious infrastructure.

Even for users familiar with these risks, human error is a fact of life, and most adversaries are all too aware of this reality and will take advantage of it whenever possible — like phishing with look-alike addresses, embedding fake command-and-control domains in malware, and hosting malicious content on domains that closely mimic corporate servers.

Where the attack comes from:

The origins of this attack are not as important as the target. This attack is usually aimed at unsophisticated internet users who won't notice that the URL of their favorite domain is a letter or two off. And because this attack is so simple (it can be as easy as registering a domain name), it can originate from almost anywhere.

Watering Hole Attack

In what became a classic watering hole attack, a Florida water and wastewater treatment facility contractor inadvertently hosted malicious code on its website, leading to the reported Oldsmar water plant hack in 2021. The cybercriminals behind the attack seemed to have a distinct audience in mind — the malicious code found on the contractor's site also appeared to target other Florida water utilities, and perhaps not surprisingly, was visited by a browser sourced to the city of Oldsmar on the same day of the hack. While the website didn't launch exploit code, it instead injected malware that functioned as a browser enumeration and fingerprinting script designed to glean information from site visitors, including operating system, browser type, time zone and presence of camera and microphone, which it then sent to a remote database hosted on a Heroku app site that also stored the script.

Watering Hole Attack

What you need to know:

Like a literal watering hole, a watering hole attack is one in which the user's computer is compromised by visiting an infected website with malware designed to infiltrate their network and steal data or financial assets. The specific technique is essentially a zero-day attack — the goal being to infect the computer system with to gain access to a network for financial gain or proprietary information.

How the attack happens:

The attackers will first profile their target to determine the websites they frequently visit, and from there, will look for vulnerabilities. By exploiting identified flaws, the attacker compromises these websites and then waits, knowing it's only a matter of time before the user in question visits. The compromised website will, in turn, infect their network, allowing attackers to gain entry into their entire system and then move laterally to other systems.

Where the attack comes from:

While they come from all over, many of the cybercriminals behind this attack originate where organized threat groups flourish, such as Russia, Eastern Europe and China. In 2018, a country-level watering hole attack was sourced to the Chinese threat group known as LuckyMouse" (aka Iron Tiger, 'EmissaryPanda," "APT 27" and "Threat Group 3390"), known for targeting government, energy and manufacturing sectors with numerous types of attacks, including watering hole assaults.

Web Session Cookie Theft

Almost every web application we use, from social media and streaming platforms to cloud services and financial applications, runs on authentication cookies. Though cookies make our experience on the web much more convenient, they also create a vulnerability that can be abused to great effect. In late 2019, a group of loosely connected hackers made a name for themselves by executing cookie theft malware to hijack various YouTube channels, then lure unsuspecting owners with bogus offers to broadcast cryptocurrency scams or sell the accounts to the highest bidder.

Web Session Cookie Theft

What you need to know:

When an attacker successfully steals a session cookie, they can perform any actions the original user is authorized to take. A danger for organizations is that cookies can be used to identify authenticated users in single sign-on systems, potentially giving the attacker access to all of the web applications the victim can use, like financial systems, customer records or line-of-business systems potentially containing confidential intellectual property.

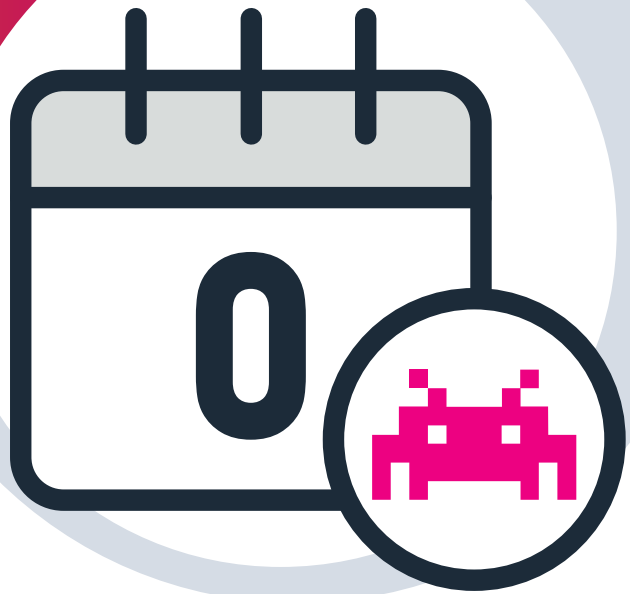
How the attack happens:

After a user accesses a service and validates their identity, a cookie is stored on their machine for an extended period of time so that they don't have to log in over and over. Malicious actors can steal web session cookies through malware, then import the cookie into a browser they control, allowing them to use the site or application as the user for as long as the session cookie is active. Once logged into the site, an adversary can access sensitive information, read email or perform actions that the victim's account has permissions to perform.

Where the attack comes from:

Cookie theft is commonly accomplished through malware that copies the victim's cookies and sends them directly to the attacker. The malware can land on the victim's machine in any number of ways covered in this book, like phishing, macro viruses, cross-site scripting and more. Many hackers engaging in cookie theft belong to larger networks based in Russia and China. The actors behind the YouTube attack, for example, were found to have been part of a group of hackers connected via a Russian-speaking forum.

Zero-Day Exploit



It's hardly surprising that the number of zero day flaws continues on an upward trajectory. But 2021 blew all other years out of the water as malicious actors exploited a total of 58 new zero day threats, compared to 25 flaws in 2020 and 21 vulnerabilities in 2019. And no doubt the stakes are getting higher as critical systems become more connected. In recent years, hackers have used zero day attack threats to compromise Microsoft servers and install advanced spyware on smartphones for espionage activities targeting journalists, politicians and human rights activists.

Zero-Day Exploit

What you need to know:

A zero-day vulnerability, at its core, is a flaw. It is a weakness within a piece of software or a computer network that hackers take advantage of soon (or immediately) after it becomes available for general use — the term “zero” refers to the same-day window in which these vulnerabilities are abused.

How the attack happens:

A zero-day attack happens once the vulnerability is exploited. The nature of the vulnerability will affect how the attack is implemented, but zero-day attacks follow a pattern. First, the hacker (or groups of hackers working together) scan the code base for vulnerabilities. Once they find the flaw, they create code that exploits the vulnerability. They infiltrate the system (using one or more of the methods described in this book) and infect it with their malicious code, then launch the exploit.

Where the attack comes from:

The prevalence of technology has led to explosive growth in zero-day attacks. While these attacks can ostensibly be launched from anywhere, they often are proliferated via nation-states or regions with extensive cyber underworld networks and infrastructure.

Learn More.

Discover how your organization can thwart countless threats and **modernize your SOC** using **Splunk's analytics-driven security**.

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2023 Splunk Inc. All rights reserved.

23-337536-Splunk-Top 50 Cybersecurity Threats-EB-110

splunk>