splunk>
turn data into doing™

TOP 50 Security Threats

Table of Contents

Data Security Is Essential to Our Future

In the most obvious sense, effective data security assures the safety of our financial assets, protects individual privacy, and guards the integrity of our systems and infrastructure — from democratic elections to basic municipal functionality. In a broader and less direct sense, though, security is the essential first ingredient to our evolution as a global society

At Splunk, we're very excited about the possibilities of a data-enabled future. Augmented reality that puts essential information and compelling entertainment right in front of us. Faster, more transparent ways to interact with governments. More compelling and personal retail experiences. Opportunities for lifelong learning. And on the backend, data will reveal better ways to harness and share resources and solve societal and environmental problems. We're already working with nonprofits that use data to reduce global hunger and improve crisis response to devastating hurricanes, brutal war and more.

None of this can happen if we don't trust the data, and the systems that house, analyze and act on that data. Data security is more than a mission to protect our individual organizations, as important as that is. Every step forward in data security moves us closer to a world in which the full, positive potential of data technologies can be unleashed.

We put this book together to look at the threat landscape we're facing today, because it's essential that we understand the specific (and evolving) challenges that threaten our data security. But we see this as more than the ever-escalating whack-a-mole that can dominate daily security concerns. The everyday battles to improve data security are about building a better world.

Doug Merrit

Like you, cybercriminals are on their own digital transformation journey. Connected Internet of Things (IoT) devices, bring-your-own-device (BYOD) trends and cloud initiatives have given them new ways to infiltrate your organization by exponentially expanding the attack surface. Technologies like artificial intelligence and machine learning have given these miscreants new tools with which to distribute malware, vector in on high-end targets, and reach bigger and more diverse audiences. And as these technologies evolve, cybercriminals are becoming increasingly stealthy, sophisticated and evasive.

These days, cybercriminals are creative, ambitious and intelligent, with no shortage of resources at their disposal. They're constantly reaching into their arsenal of tools to help them gain a competitive edge — only they're competing to break into your systems and abscond with your IP address, personally identifiable information (PII) and other critical data before you even notice it's gone.

While their financial motivations have remained the same for decades, their methods have significantly evolved over the years. For example:

- Phishing attacks have progressed from crafty personal emails to attacks that hijack business conversations or target business SaaS applications.
- Ransomware not only encrypts and holds files in exchange for money, but now punishes victims who fail to pay in a timely manner.
- Botnets contain adaptable variants that mutate to infect different kinds of IoT devices and incorporate them into a bot army that launches global distributed denial-of-service (DDoS) attacks.
- Malicious exploits now often include cryptocurrency miners — malware that exploits computer processing power to create valuable cryptocurrency on your dime.
- And DDoS attacks can now bombard victims with terabytes of traffic per second.

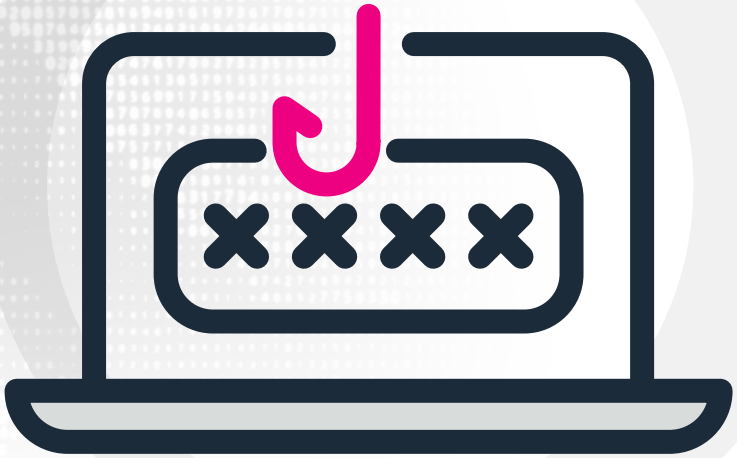
These advanced threats are not slowing down any time soon. In fact, known malware samples have already surpassed the one billion mark. So, even if you strive daily to protect your data and keep the cybercriminals at bay, you might have a few strikes against you.

But before you go to battle with any cyber attacker, you first need to know what you're up against. Our anthology of security threats equips you with a comprehensive inventory of threats that you're sure to face in the digital age — from "account takeover" to "zero-day attacks" and everything in between. We also arm you with insights into who is behind them, how they occur and where they are sourced.

Some of the most treacherous threats you'll face are invisible, conducted by malicious actors who can enter your network in the blink of an eye from across oceans. Their digital transformation strategy includes technology that can employ economies of scale, mobilize hostile nation-states and quickly adapt methods to stay under the radar.

But knowing who they are and what to look for will give you a few tools to understand their motivation, shine a light on their tactics and help you stay one step ahead of an increasingly cunning adversary.

Account Takeover



Account takeover is considered one of the more harmful and nefarious 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. Scarier yet, user credentials can be sourced from the deep web and matched against e-commerce sites with the help of bots and other automated tools for quick and easy entry.

FitBit even fell victim to this type of attack in 2015. Hackers employed a two-pronged approach, exposing log-in details to customers' FitBit accounts, changing the email they registered with, and then calling up customer support with a complaint about the device so that they could get a replacement under their warranty.

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 type of attack.

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.

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. As such, these kinds of attacks can originate anywhere in the world.

Advanced Persistent Threat

In 2015, security experts connected state-sponsored attackers working for the Chinese government to one of the most notable data breaches in U.S. history — the attack on the U.S. Office of Personnel Management (OPM).

The attack on OPM compromised over 4 million records, including information on current, former and prospective federal government employees, as well as their family members, foreign contacts and even psychological information.

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). Regardless, various methodologies are used to reach and compromise the target in question 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 said accounts 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.

Application Access Token

Pawn Storm — an active and aggressive espionage group that's been operating since 2004 — uses different strategies to gain information from their targets. One method in particular was to abuse Open Authentication (OAuth) in advanced social engineering schemes, targeting high profile users of free webmail between 2015 and 2016.

The group also set up aggressive credential phishing attacks against the Democratic National Convention (DNC), the Christian Democratic Union of Germany (CDU), the parliament and government of Turkey, the parliament of Montenegro, the World Anti-Doping Agency (WADA), Al Jazeera and many other organizations.

They continue to use several malicious applications that abuse OAuth access tokens to gain access to target email accounts, including Gmail and Yahoo Mail.

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

Zelle is a financial service that allows customers to easily send money to friends and family. Yet the very same features that make Zelle so quick and efficient for transferring funds are also being exploited by cyberthieves for monetary gain. Hackers and scammers used 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 the most recent data from the FTC, consumers reported losing about $1.48 billion related to fraud complaints in 2018, an increase of $406 million from 2017.

How the attack happens:

This attack aims to trick 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.

Business Invoice Fraud

Even the largest technology firms in the world aren't immune to invoice fraud. According to an investigation by Fortune Magazine, both Facebook and Google unwittingly fell victim to a massive business invoice fraud scheme back in 2013. The fraudster, a Lithuanian man known as Evaldas Rimasauskas, created invoices impersonating a large Asian-based manufacturer that frequently did business with the two companies to trick them into paying for bogus computer supplies. Over two years, the fraudster duped the two tech giants into shelling out tens of millions of dollars. By the time the firms figured out what was going on, Rimasauskas had absconded with more than $100 million.

Business Invoice Fraud

What you need to know:

Business invoice fraud attempts to trick you into paying out on a fraudulent (but convincing) bill addressed to your organization. In reality, the funds you pay will go to imposters mimicking your suppliers. These hackers are often willing to bill you an amount that appears reasonable so as not to draw suspicion — like $1,500. But executing these scams hundreds or thousands of times quickly adds up.

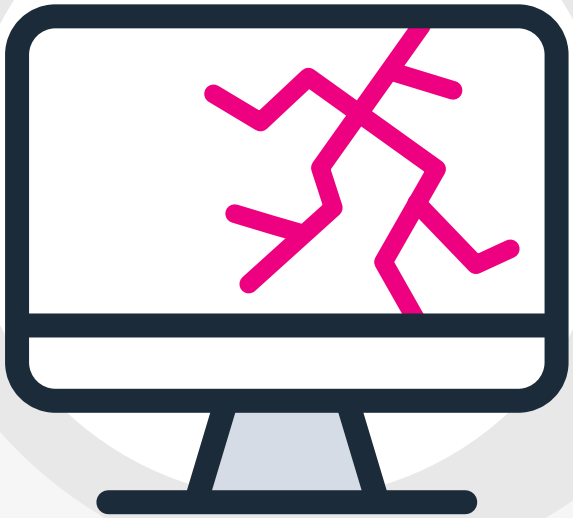
How the attack happens:

In this attack, you'll be sent fake invoices attempting to steal your money in the hopes that you're not paying attention to your accounts payable processes. Hackers will target you based on the size of your business, location and the suppliers you use and create phony invoices that appear legitimate. With the hopes that your 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 your banking institution and create a billing experience that feels real. Fraud rings conducting invoice scams can be found all over the world. Invoice fraud costs UK businesses £93 million ($122.8 million USD) with 3,280 invoice and mandate scam cases last year, according to a recent report. There are also thousands of fraud rings in the U.S. located coast to coast — with Florida, Michigan and Nevada having the highest number of fraud reports in 2018, according to the U.S. Federal Trade Commission.

Brute Force Attack



In a now infamous brute force attack, over 90,000 PlayStation and Sony Online Entertainment accounts were compromised in 2011. Hackers attempted countless username and password combinations from an unidentified third party, eventually ransacking members' accounts for personal information.

The now-discontinued Club Nintendo also fell victim to the same type of attack in 2013, when hackers executed a coordinated attack on over 15 million members, eventually breaking into over 25,000 forum members' accounts. All compromised accounts were suspended until access had been restored to the rightful owners — but the damage to brand reputation had already been done.

Brute Force Attack

What you need to know:

A brute force attack aims to take your personal information, specifically your username and password, 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.

Compromised Credentials

Former internet giant Yahoo inevitably comes to mind when talk of compromised credentials come up. An attack in 2016 resulted in a serious breach of half a billion users' personal information, including their dates of birth and telephone numbers. But it only gets better: Later that year, Yahoo announced that a breach in 2013 had compromised 1 billion accounts (eventually revealed to be 3 billion), along with their passwords, unencrypted security questions and answers. Unsurprisingly, Yahoo's sale price went down about $350 million shortly after.

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 and 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

Disney+ signed up 10 million users and its stock hit a record high shortly after. But that shine quickly faded when many of those eager subscribers began complaining about being locked out of their accounts. Within days of the launch, Disney+ credentials were up for grabs for as little as $3.

Disney said the site wasn't actually breached — allegedly, users who found their credentials online likely fell victim to a common (but notoriously bad) practice: using the same password across multiple sites that were later hit by a credential dumping attack.

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. Think about the aforementioned command and control attack and moving laterally through a network. But 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.

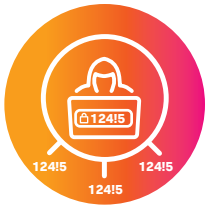
Where the attack comes from:

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 of the more notable credential reuse attacks is the 2019 Dunkin Donuts breach — which, unluckily for the east coast chain, happened to be their second hack in two months. This time around, the threat actors went so far as to sell thousands of accounts on the dark web. They sold users' credentials — including usernames and passwords — to the highest bidders, who could then try them across other consumer websites until they got a hit.

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 users 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.

Credential Stuffing

2019 was not the year for Fort Lauderdale-based Citrix Systems, which found itself neck deep investigating a major network breach that had occurred the previous year, resulting in stolen business documents by hackers. The FBI believed the breach was sourced for “password spraying,” otherwise known as credential stuffing — an attempt by hackers to remotely access a large number of accounts at once. According to a form 10-K filing to the U.S. Securities and Exchange Commission, Citrix believed the perpetrators tried to infiltrate company systems to access content collaboration customer accounts.

Credential Stuffing

What you need to know:

With credential stuffing, cybercriminals will use stolen account credentials — often usernames and passwords procured from a data breach — to access additional accounts by automating thousands or millions of login requests directed against your web application. They want to access your sensitive accounts the easy way — by simply logging in. It works because they rely on you or your colleagues reusing the same usernames and passwords across multiple services. If they're successful, one credential can unlock accounts that house financial and proprietary information, giving them the keys to almost everything.

How the attack happens:

Hackers only need access to login credentials, an automated tool and proxies to carry out a credential stuffing attack. Attackers will take a cache of usernames and passwords, gleaned from massive corporate breaches, and by using automated tools, essentially "stuffing" those credentials into the logins of other sites.

Where the attack comes from:

Proxies mask the location of credential stuffing attackers, making it challenging to detect their location. But you'll find them all over the world, especially in organized cybercrime hotspots. Often, attackers will be individual and organized hackers with access to dedicated account-checking tools and numerous proxies that prevent their IP addresses from being blacklisted. Less sophisticated perpetrators may end up giving themselves away by attempting to infiltrate a large number of accounts via bots, which results in an unexpected denial-of-service-attack (DDoS) scenario.

Cloud Access Management

Moving to the cloud has countless advantages, from fostering collaboration to allowing employees to work from almost anywhere in the world. But switching to a cloud-based service can carry a fair amount of risk — oftentimes due to human error.

Wyze Labs, a company that specializes in low-cost smart home products, experienced this firsthand. An almost-prolific breach in 2019 occurred at the startup when an employee built a database for user analytics, only to accidentally remove the necessary security protocols. As a result, a database-worth of customers' personal information was exposed.

Cloud Access Management

What you need to know:

Managing permissions for your organization has become increasingly important in order to avoid a cloud-based breach. Lax or nonexistent security — and in this case, incorrectly configured security controls — can easily jeopardize the security of your data, exposing your organization to an unnecessary amount of risk, including significant damage to brand reputation.

How the attack happens:

This type of attack usually happens because of poor communication, lack of protocol, insecure default configuration and poor documentation. Once the attacker exploits the vulnerability and gains a foothold in your cloud environment, they can leverage privileges to access other remote entry points, looking for insecure applications and databases, or weak network controls. They can then exfiltrate your data while remaining undetected.

Where the attack comes from:

Mismanagement and misconfiguration of a cloud environment isn't considered a malicious act in and of itself, and as mentioned, typically occurs due to mere human error.

Cloud Cryptomining

Cloud cryptomining doesn't need gas to go. Look no further than Tesla for evidence. In 2018, the electric carmaker fell victim to a cloud cryptomining attack when hackers took advantage of an insecure Kubernetes console, stealing computer processing power from Tesla's cloud environment to mine for cryptocurrencies.

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:

Cryptojacking 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 (AWS), Google Cloud Platform (GCP) and Microsoft Azure.

It's difficult to determine exactly how widespread the practice has become, since bad actors 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 malicious miners appropriate a cloud instance, often spinning up hundreds of new instances, the costs can become astronomical for the account holder. So it is critical to monitor your systems for suspicious activities that could indicate that your 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 is 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

The first known take down of a country's power grid due to a cyberattack happened on December 23, 2015. The details of the hack is summarized in vivid detail by Wired. At about 3:30 p.m. local time, a worker inside the Prykarpattyaoblenergo control center saw his mouse's cursor move across the screen.

The ghostly cursor floated toward the digital controls of the circuit breakers at a substation, and began taking them offline. Almost 30 substations subsequently went down, and 230,000 residents were forced to spend a cold evening in the dark in Western Ukraine, with a blistering low of 30 degrees Fahrenheit.

Command and Control

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.

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 as well.

How the attack happens:

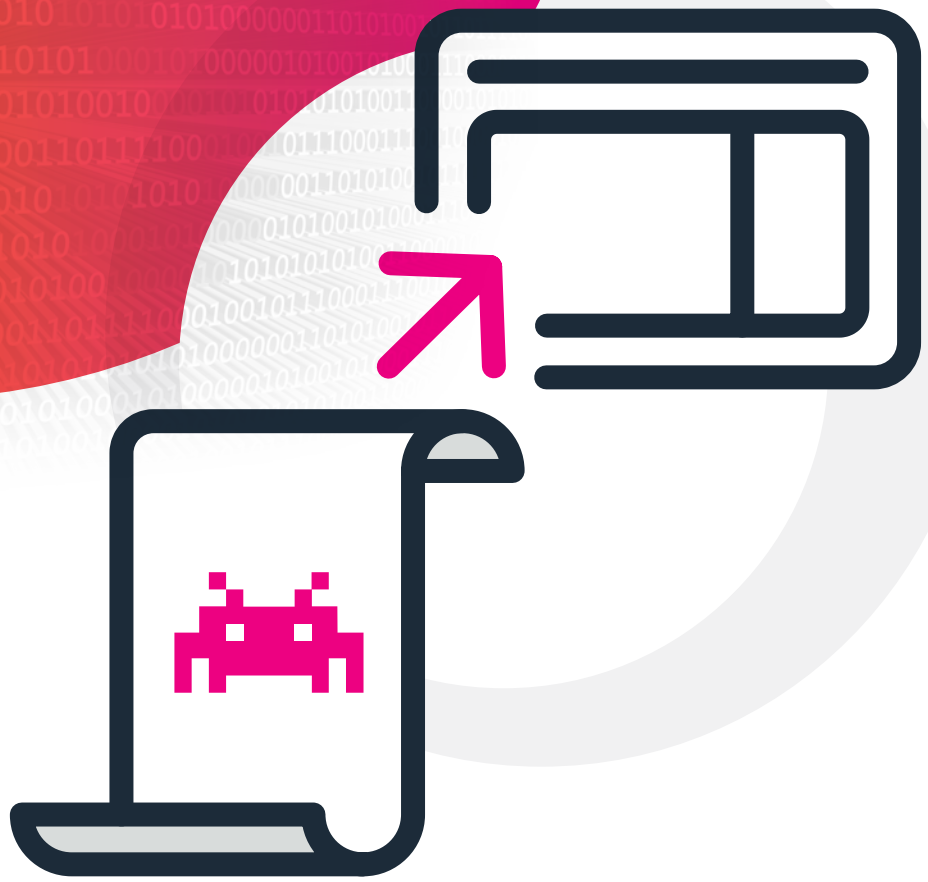
Most bad actors will get a foothold in the system through phishing emails and the installation of malware. This establishes a command and control channel that's used to proxy data between the compromised endpoint and the attacker. These channels relay commands to the compromised endpoint and the output 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.

Cross-Site Scripting



In January of 2019, an XSS vulnerability was discovered in the Steam Chat client operated by Valve, a computer gaming company with more than 90 million active users, any number of whom could have been attacked until the bug was disclosed.

Cross-Site Scripting (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 — in which 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.

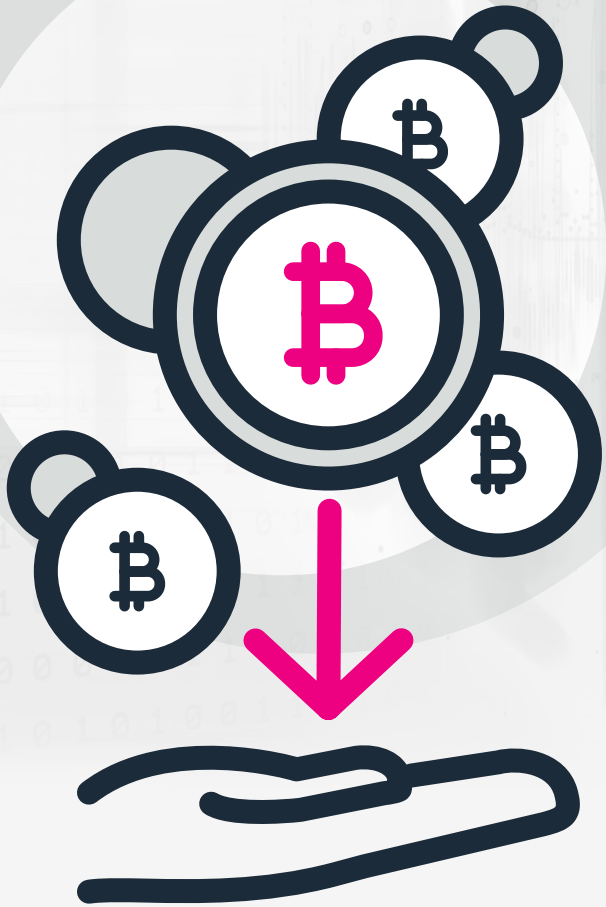
How the attack happens:

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 are 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



Sadly, no websites are sacred when it comes to hackers' desire to exploit them for profitability — not even Australia's parliament. In early 2018, cyberhackers compromised numerous Australian government websites with malware that forced visitors' computers to secretly mine cryptocurrency without their permission. The cryptojacking attack was initiated when hackers exploited a vulnerability in a popular browser plugin as part of a larger global security breach. The attack affected the official website of the Victorian parliament, the Queensland Civil and Administrative Tribunal, and the Queensland Community Legal Centre homepage, among others, as well as the UK's National Health Service, and the UK's own data protection watchdog site.

Cryptojacking Attack

What you need to know:

Cryptojacking is an attack where a hacker targets and hijacks your computer systems with malware that hides on your device and then exploits its processing power to mine for cryptocurrency — such as Bitcoin or Ethereum — all on your dime. Their mission is to create valuable cryptocurrency with your computing resources.

How the attack happens:

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

Where the attack comes from:

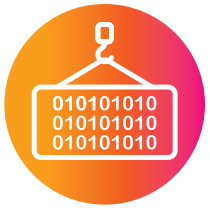
These attacks come from all over the world. These days, cryptojacking doesn't require significant technical skills. Cryptojacking kits are available on the deep web for as little as $30. It's a low bar for entry for hackers that want to make a quick buck for relatively little risk. In one attack, a European bank experienced some unusual traffic patterns on its servers, slower than average night processes and unexplained online servers — all attributed to a rogue staffer who installed a cryptomining system.

Data From Information Repositories

In 2016, the threat group APT28 reportedly compromised the Hillary Clinton campaign, the Democratic National Committee (DNC) and the Democratic Congressional Campaign Committee (DCCC). They've also targeted Eastern European governments, military and security-related organizations, including the North Atlantic Treaty Organization (NATO).

The group uses a complex set of tools and strategies, surreptitiously accessing information repositories to control and steal data. APT28 has collected information from Microsoft SharePoint services within target networks.

Data From Information Repositories



What you need to know:

Information repositories are tools that allow for the storage of information — tools like Microsoft SharePoint and Atlassian Confluence. Information repositories typically facilitate collaboration or information sharing between users and they store a wide variety of data that may tempt attackers. Hackers may leverage information repositories to access and mine valuable information.

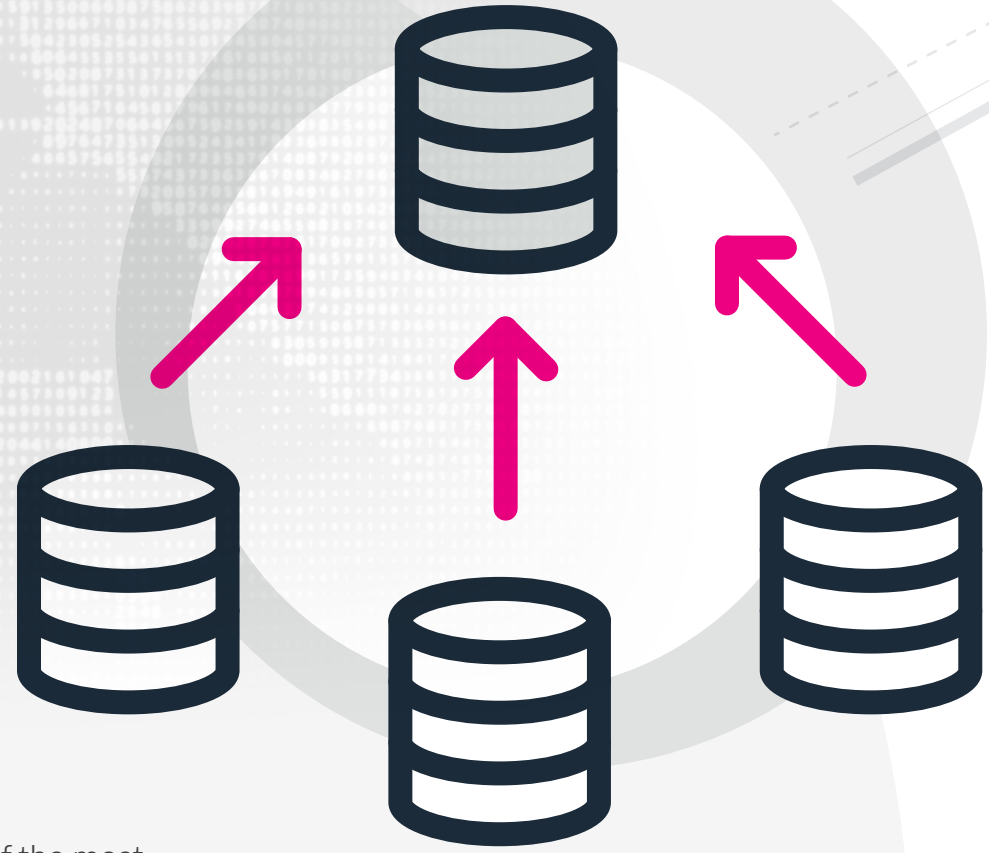
How the attack happens:

Information repositories often have a large user base, and the detection of breaches can be difficult. Attackers may collect information from shared storage repositories hosted on cloud infrastructure or in software-as-a-service (SaaS) applications.

Where the attack comes from:

Attackers like APT28 target government agencies, hotel booking websites, telecoms and IT companies. At a minimum, access to information repositories performed by privileged users (for example, Active Directory Domain, Enterprise or Schema Administrators) should be closely monitored and alerted upon, as these types of accounts should not generally be used to access information repositories. Additional log storage and analysis infrastructure will likely be required for more robust detection capabilities.

DoS Attack



In 2000, a 16-year-old hacker known as Mafiaboy launched one of the most famous denial-of-service (DoS) attacks that took a host of major players 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 in April 2000 and sentenced to juvenile detention.

Twenty years later, DoS attacks (many of which are DDoS) continue to be on the rise and are some of the most common attacks faced by organizations, targeting around a third of all businesses.

DoS Attack

What you need to know:

A DoS attack is where cyberattackers seek to make a machine or network inaccessible to 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:

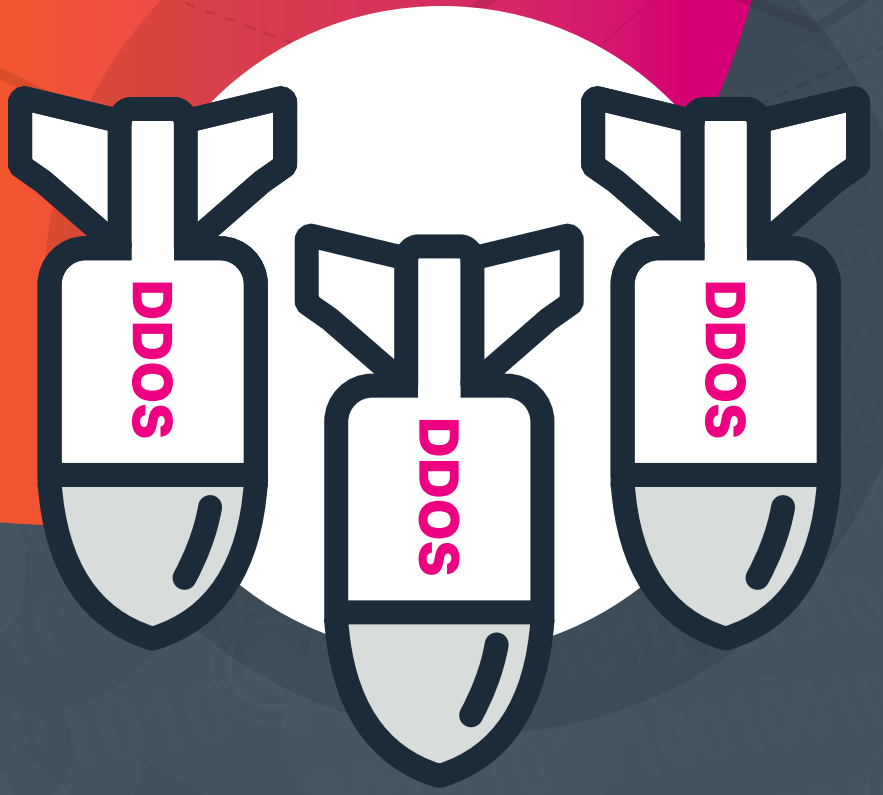
How the attack happens: DoS attacks occur in one of two ways: by flooding or crashing a targeted network. In flood attacks, cybercriminals bombard victim computers with more traffic than they can handle, causing them to slow or shut down altogether. Various flood attacks include buffer overflow attacks,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

Other DoS attacks exploit vulnerabilities that prompt the target system to crash. In these attacks, bad actors exploit system vulnerabilities with malware that subsequently triggers a crash or severely disrupts the system.

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.

DDoS Attack



To date the biggest — if not the most significant — distributed denial-of-service (DDoS) attack occurred in 2018 against popular online code management system GitHub. GitHub was hit by an onslaught of traffic, which at its peak came in at a rate of 1.3 terabytes per second, sending packets at a rate of 126.9 million per second. The attack wasn't just massive, it was record-breaking. In this attack, the botmasters flooded memcached servers with spoofed requests, which gave them the ability to amplify their attack by 50,000x. The good news? GitHub wasn't caught entirely unprepared. Administrators were alerted to the attack and it was shut down within 20 minutes.

What you need to know:

A DDoS attack is an attempt by hackers, hacktivists or cyber spies to take down websites, slow down and crash the target servers and make online service unavailable by flooding them with traffic from multiple sources. As their name suggests, DDoS attacks are widely-distributed brute-force attempts to wreak havoc and cause destruction. These attacks often tend to target popular or high-profile sites, such as banks, news and government websites, to thwart or deter target organizations from publishing important information or to weaken them financially.

How the attack happens:

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.

The hacker or group of hackers that control these infected computers then become botmasters, who infect vulnerable systems with malware, often Trojan viruses. When enough devices are infected, the botmaster gives them the command to attack and the target servers and networks are bombarded with requests for service, which in turn effectively chokes them and shuts them down.

Where the attack comes from:

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 thwart these attacks simply by securing or blocking a single source.

Disabling Security Tools

Sometimes hackers use the very tools meant to protect us to gain access to our systems. Microsoft Windows became the world's desktop operating system of choice when it was first released in 1985. And while its market share has gotten smaller in recent years, it still remains a dominant force compared to its distant runner up, Apple OSX. The mass adoption of Windows, and the fact that it more easily falls victim to attacks, such as malware and bots, has made it a favorite playground for hackers.

That's partly why Microsoft began installing a native anti-spyware and antivirus program called Windows Defender with the release of Windows Vista. Unfortunately Microsoft did not consider that hackers would attack the very thing supposed to protect Windows users.

Novter, also known as Nodersok or Divergent, was a trojan attack seen in 2019 that attacked Windows Defender's real-time protection features. Once disabled, the trojan would download additional malware to the system.

Disabling Security Tools

What you need to know:

Hackers use a variety of techniques to avoid detection and operate without barriers. This often involves modifying the configuration of security tools, such as firewalls, to get around them or explicitly disabling them to prevent them from running at all.

How the attack happens:

The fingerprints of this attack revolve around hackers trying to disable various security mechanisms. They may attempt to gain access to registry files, where much of the configuration for Windows and various other programs live. The hackers may also attempt to shut down security-related services.

Other times, attackers attempt various tricks to prevent specific programs from running, such as adding the certificates with which the security tools are signed to a blacklist, preventing those protection tools from running altogether.

Where the attack comes from:

An attack centered around disabling security tools can originate anywhere because these types of attacks can target an almost endless list of tools. The Nodersok attack, for example, mostly attacked PC users in the U.S. and the U.K. (81%).

DNS Amplification

The Spamhaus Project — an international nonprofit organization — runs a global threat intelligence network that provides major internet networks with a list of email spammers that they've tracked. The hope is that the list will help reduce the amount of spam that reaches users' inboxes.

In 2013, a group of spammers decided to strike back with a Domain Name System (DNS) amplification attack. The attack threw more than 300 gigabytes per second at the Spamhaus website, taking it offline. The attack was so intense that it also took down the website of the content delivery firm hired to protect Spamhaus from this exact type of attack.

What you need to know:

DNS amplification has been around for a long time. 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.

How the attack happens:

A DNS amplification attack is a type of distributed denial-of-service (DDoS) attack, where 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

On a Thursday morning in 2017, WikiLeaks readers woke up expecting to find the latest state secret released on the whistleblowing website, only to discover a message from a hacker collective called OurMine announcing that they were in control of the domain.

Wikileaks founder Julian Assange quickly took to Twitter to clarify that the takedown was not a traditional hack, but instead a domain name system (DNS) attack.

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 very 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.

On January 22, 2019, the US Department of Homeland Security 2019's Cybersecurity and Infrastructure Security Agency (CISA) raised awareness around some high-profile DNS hijacking attacks against infrastructure, both in the United States and abroad.

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 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.

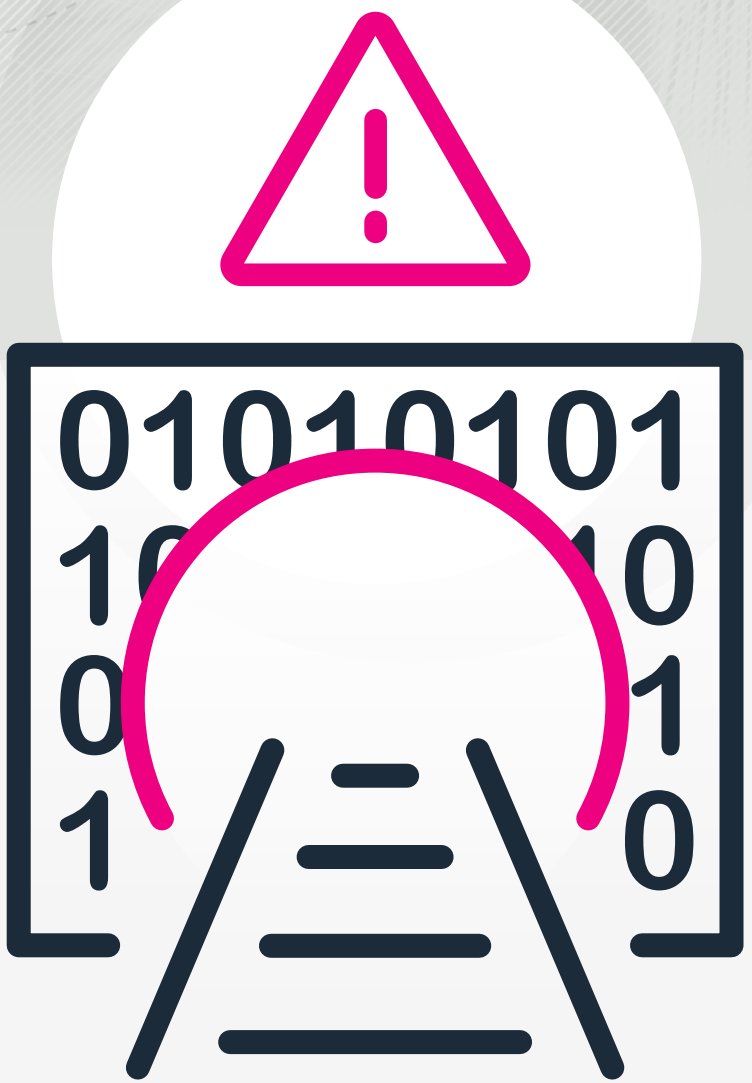
Where the attack comes from:

There is no one a 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.

Some of the more prominent DNS hijacking attacks have been attributed to hacking collectives such as OurMine in the Wikileaks case, or the Syrian Electronic Army in takedowns of The New York Times and The Washington Post.

DNS Tunneling

Since at least mid-2016, 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. An essential element of their efforts to disrupt daily operations and exfiltrate data is maintaining a connection between their command-and-control server and the system they're attacking using DNS tunneling.



DNS Tunneling

What you need to know:

The protocol that translates the URLs we enter in our web browsers into their numerical IP addresses is called the Domain Name System (DNS) — you can think of it as the phone book of the internet. The traffic that passes through DNS often goes unmonitored, since it is not designed for data transfer, leaving it vulnerable to several kinds of attacks, including DNS tunneling, which is accomplished 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 is important for organizations to monitor their DNS traffic thoroughly, allowing only trustworthy traffic to continue flowing through the network.

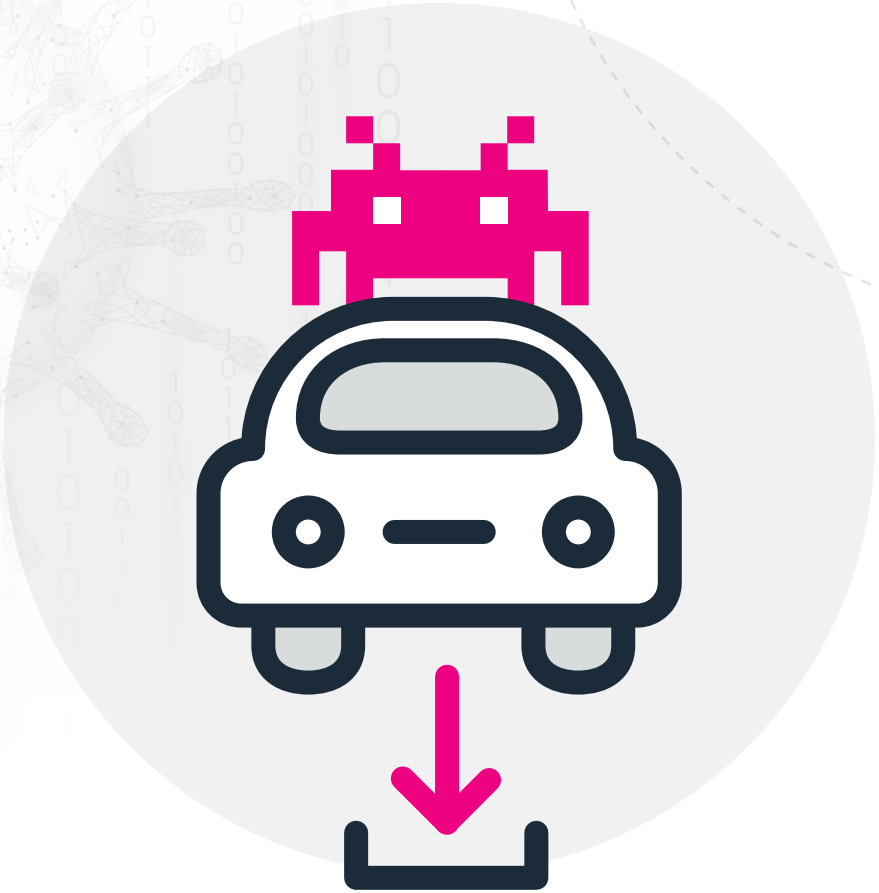
How the attack happens:

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 is a very slow system for data transfer.

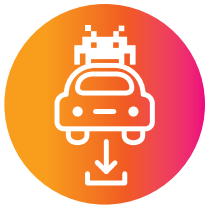
Drive-by Download Attack



One of the largest drive-by download campaigns of recent times struck a range of high-profile publishers whose sites have between millions and billions of monthly visitors. Among the affected websites were MSN, the New York Times, the BBC, Comcast's Xfinity and the NFL. Each of these sites were using seemingly legitimate ad networks that were compromised by the attacker. The prominence of these and other sites allowed the hacker to push malicious ads to a large number of innocent site visitors. These ads then redirected them through two malvertising servers.

The second server loaded the Angler exploit kit to victims, which could exploit vulnerabilities in Microsoft Silverlight, JavaScript, Adobe Flash and other common types of software. It could then be used to load a wide range of malware onto the victim's computer, according to the needs of the hacker. While the bigger publishers were relatively quick to take the malicious ads down, it's possible that the campaign ended up infecting tens of thousands of users.

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 is also advisable 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.

Host Redirection

In 2017, Office 365 experienced a widespread phishing attack on their users, when nefarious actors took advantage of the Google AppEngine's open redirect vulnerability, redirecting unwitting victims to a copycat website where they would then go on to download malware.

Host Redirection

What you need to know:

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

How the attack happens:

The hacker might make a phishing attempt, sending an 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

Insider Threat

The more an organization has, the more it has to lose — and the more insiders stand to gain. Tesla filed a lawsuit in 2018 against a former employee after learning that the altered source code exported gigabytes of proprietary data to unknown recipients outside the company.

The malicious insider allegedly created false usernames in order to make changes directly to the Tesla Manufacturing Operating System's (MOS) source code, and funneled data outside the company that included dozens of confidential photographs and a video of Tesla's manufacturing systems. The insider also pilfered information on Tesla's financials, the process for manufacturing batteries for its Model 3 luxury vehicle, and the amount of scrap and raw materials used at the battery factory, according to the lawsuit.

What you need to know:

An insider attack, also known as an insider threat, is a malicious assault carried out by insiders with authorized access to your bank's computer system, network and resources. In this assault, inside 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 come from within your organization — they can be insiders in your company with bad intentions, or cyberspies impersonating contractors, third parties or remote workers. They can work both 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 have some level of legitimate access to your systems and data.

IoT Threats

In September 2016, the Mirai botnet brought down the internet for millions of people by overwhelming Dyn, a U.S.-based internet infrastructure company, with wave after wave of malicious traffic. Mirai made a name for itself by infecting Internet of Things (IoT) devices and then incorporating them into a centrally controlled botnet. What made Mirai unique, though, was that it was adaptable, allowing hackers to develop different variants that could vector in on vulnerable IoT devices and rapidly increase the population of drones in the network. This army of bots was then used to execute distributed denial-of-service (DDoS) attacks that flooded victim servers. Among its targets were more than 900,000 Deutsche Telekom customers in Germany and almost 2,400 TalkTalk routers in the UK.

What you need to know:

There are an estimated 22 billion connected IoT devices globally — a number that is projected to increase to 50 billion by 2030. However, 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.

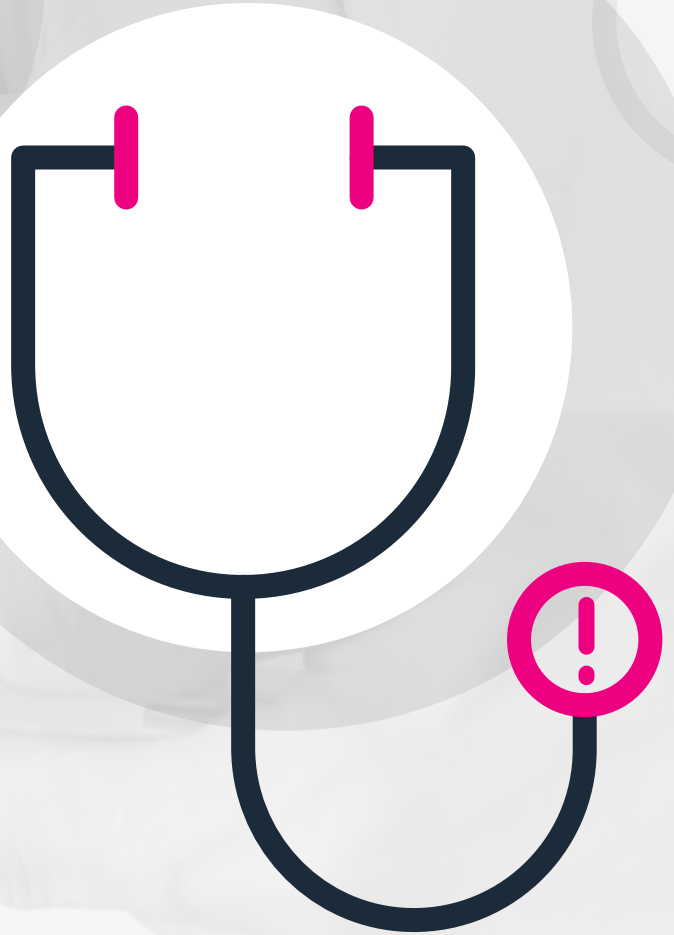
How the attack happens:

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.

IoMT Threats



The prevalence and complexity of attacks on healthcare organizations — as well as the risk to patient confidentiality and safety — means providers are coming under fire when it comes to medical device security. Due to recent attacks, including the WannaCry ransomware attack, lawmakers have outlined the severity of cybersecurity issues plaguing legacy software and equipment. The FDA has also issued recommendations for device manufacturers, but companies aren't required to follow these guidelines since they're not legal mandates.

What you need to know:

The Internet of Medical Things (IoMT) has disrupted the future strategy of healthcare organizations and market segments as we know it. Leveraging IoMT has the power to unleash countless opportunities in diagnosing, treating and managing a patient's health and wellness, and holds the key to lowering cost while improving quality of care. However, as the number of connected devices invariably grows, so does the cybersecurity risk. Major security breaches are a significant challenge for healthcare organizations, and with the increase in high-profile hacks and hospitals' growing dependence on IoMT devices, cybersecurity is now of absolutely critical importance.

How the attack happens:

Because digital technologies age faster than their physical counterparts — which typically have a long product life cycle — outdated equipment and software are creating serious cybersecurity vulnerabilities for both hospitals and patients. Currently, manufacturers don't allow customers to troubleshoot and patch their own devices, and will even go so far as to void warranties if they do. Compounded with lack of encryption, hardcoded credentials and lax security controls, there's little that healthcare organizations can do to mitigate risk where legacy devices are involved.

Where the attack comes from:

Generally from attackers who pinpoint healthcare providers with ambiguous security ownership, as well as poor asset or inventory visibility, and out-of-date systems and devices.

Macro Viruses

One of the best known virus incidents of all time, the Melissa virus of the late ‘90s, was none other than a macro virus. A Melissa-infected computer 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.

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.

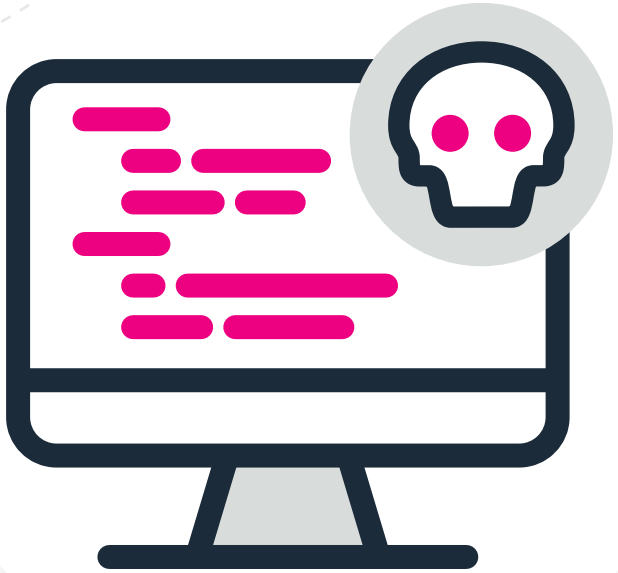
How the attack happens:

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:

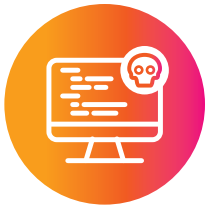
While macro viruses have fallen out of vogue for malicious attacks — primarily because antivirus software is better able to detect and disable them — they still represent a major threat. A cursory Google search for "macro virus" yields instructions for creating macro viruses and tools that assist non-coders 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 — a command-line and scripting tool developed by Microsoft — are increasingly on the rise thanks to their ability to propagate viruses across a network. A notorious banking trickbot that targeted customers of major banks relied on the tool to carry out their attacks, and threat group Advanced Persistent Threat 29 (also known as Cozy Bear) conducted an elaborate attack incorporating a PowerShell element.

Malicious PowerShell



What you need to know:

PowerShell is a command-line tool 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. Unfortunately, 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, doing their damage 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.

Man-in-the-Middle Attack

In 2010, the average website only encrypted data that was considered absolutely necessary to protect, like credit card numbers and account credentials. They left other elements of user sessions entirely unencrypted, allowing any interested party to gain unfettered access to user accounts while they were on the same network.

That all changed when a Firefox plugin called Firesheep was released. The plugin was a specialized packet sniffer, user-friendly and purpose-built to find unencrypted Facebook sessions on a shared network, then provide one-click access to take over the exposed accounts. Firesheep quickly expanded to support a laundry list of sites including Amazon, Google, Github, Twitter and many others. Hundreds of thousands of people downloaded Firesheep at the height of its popularity, each of them instantly becoming a casual hacker.

Man-in-the-Middle Attack

What you need to know:

A man-in-the-middle (MITM) attack is a type of eavesdropping cyberattack where a malicious actor inserts him/herself as a relay or proxy into a communication session between two parties or systems, impersonates both parties and gains access to information that the parties or systems were trying to send to each other. A man-in-the-middle attack allows a malicious actor to intercept, send and receive data meant for someone 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:

In the case of Firesheep, 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 U.K. governments released warnings that Russian state-sponsored actors were actively targeting routers in homes and enterprises for the purpose of MITM exfiltration.

Masquerade Attack

In December 2013, Target experienced a massive credit card breach which affected over forty million customer accounts. The states' investigation into the breach revealed that attackers stole the credentials of Target's HVAC contractor, Fazio Mechanical Services. After using the third-party vendor's details to get into Target's internal web application, they installed malware on the system and captured names, phone numbers, payment card numbers, credit card verification codes and other highly sensitive information.

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 the 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. In 2018, 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.

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.

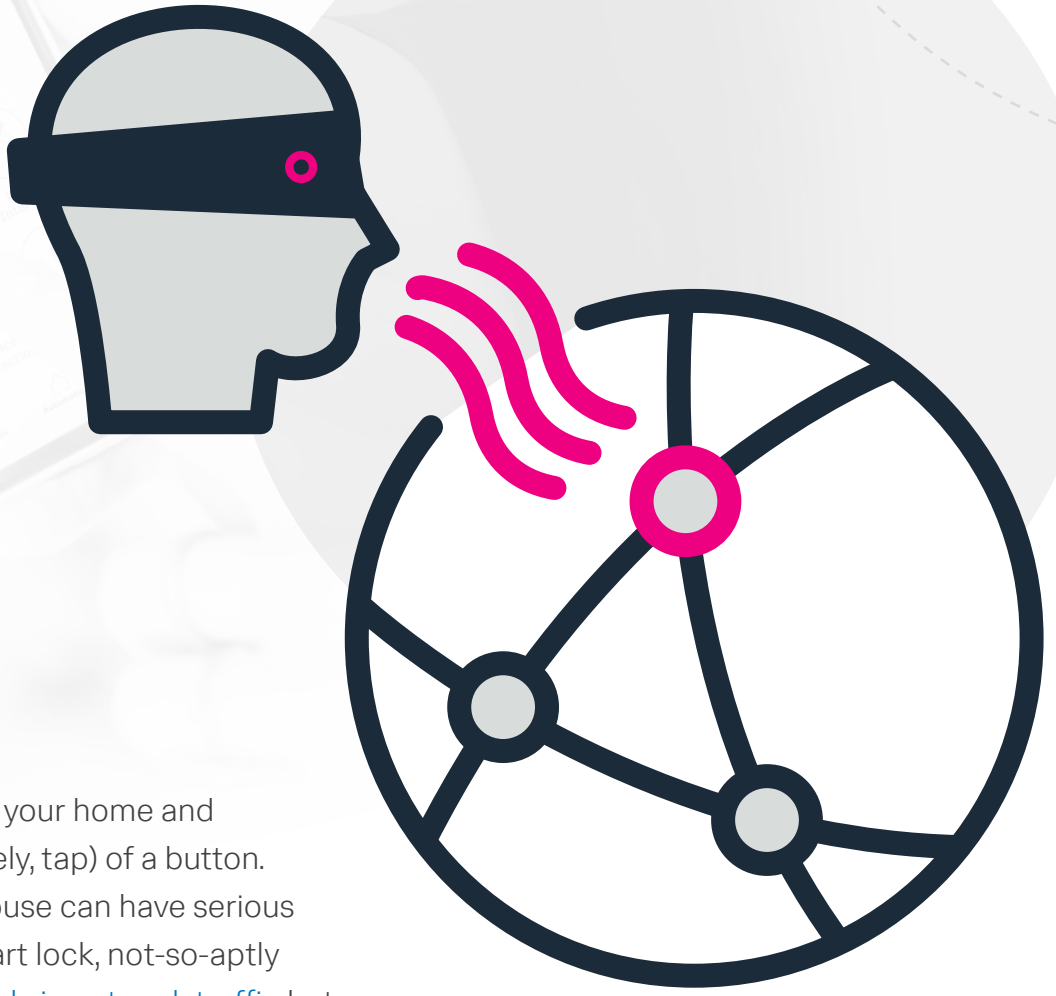
The attack breaks the norm of computing where programs are not allowed to read data from other programs. The types of information that attackers typically target are passwords stored in a password manager or browser as well as emails, financial records, personal information such as photos and instant messages, and more.

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 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 can also be a vector for attack.

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:

PtH 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.

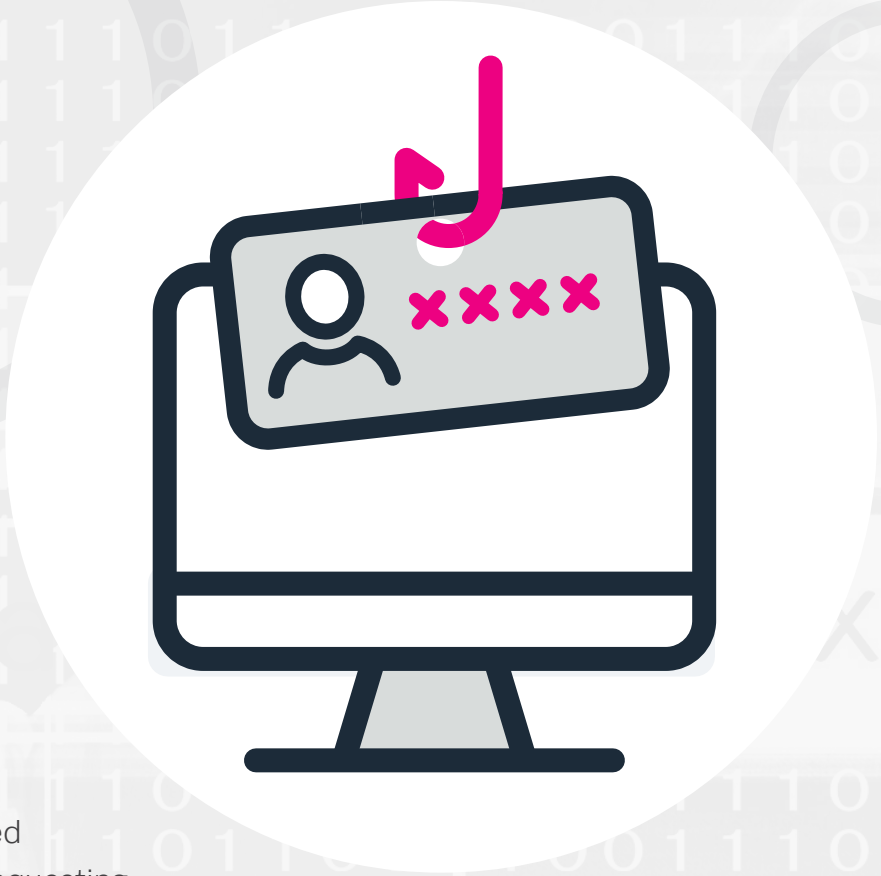
How the attack happens:

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 threat groups. These perpetrators are often organized, with their sights set on a specific organization or person and with a mind to political or financial gain.

Phishing



When it comes to phishing attacks, there are a few that stand out above the rest — such as the Sony attack of 2014. Hackers likely executed the now infamous attack on Sony's network by sending phishing emails requesting verification for Apple IDs to system engineers, network administrators and other unsuspecting employees with system credentials. The attackers absconded with gigabytes worth of files, which included emails, financial reports and digital copies of recently released films. On top of that, the malicious actors then infused Sony's workstation computers with malware that erased the machines' hard drives. A few weeks later, the FBI formally pointed to the North Korean government as the masterminds behind the attack.

What you need to know:

A phishing attack tricks banking consumers 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, IM 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 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 have the ability to launch phishing campaigns. The people behind these campaigns run the range from individual hackers to organized cybercriminals.

Phishing Payloads

One of the most infamous phishing payload attacks happened in 2009, in what the FBI called Operation Phish Phry, sparking the largest international phishing investigation at the time.

The attack targeted hundreds of bank and credit card customers, who received emails with links to fake, but authentic-looking financial websites. On the site, customers were asked to enter their account numbers and passwords into fraudulent forms.

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.

In a phishing attack, the payload is simply a reference 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:

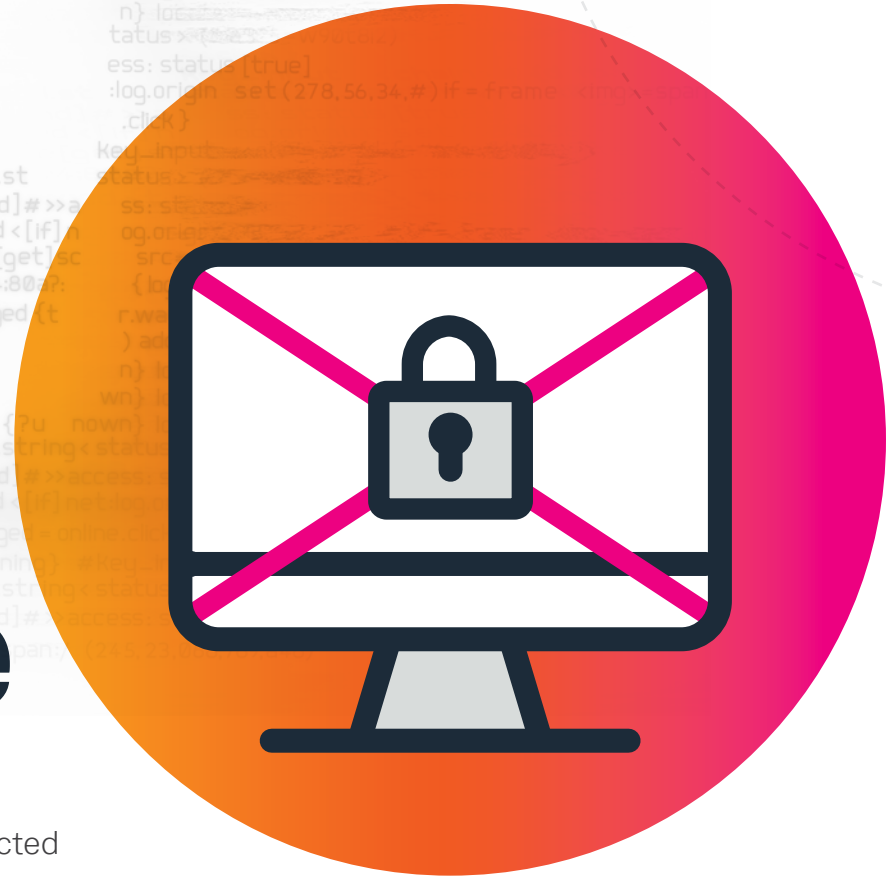
This attack has a typical attack pattern: First, the attacker sends a phishing email and the recipient downloads the attached file, which is typically a .docx or .zip file with an embedded .lnk file. Second, the .lnk file executes a PowerShell script and lastly the Powershell script executes a reverse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

Where the attack comes from:

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

Operation Phish Phry is a perfect example of this. In this attack, the FBI arrested more than 50 people in California, Nevada and North Carolina, while also charging "about 50 Egyptian citizens" in connection with the attack.

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, for example, 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 wherein an infected host encrypts a victim's data, holding it hostage until they pay the attacker a ransom. 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.

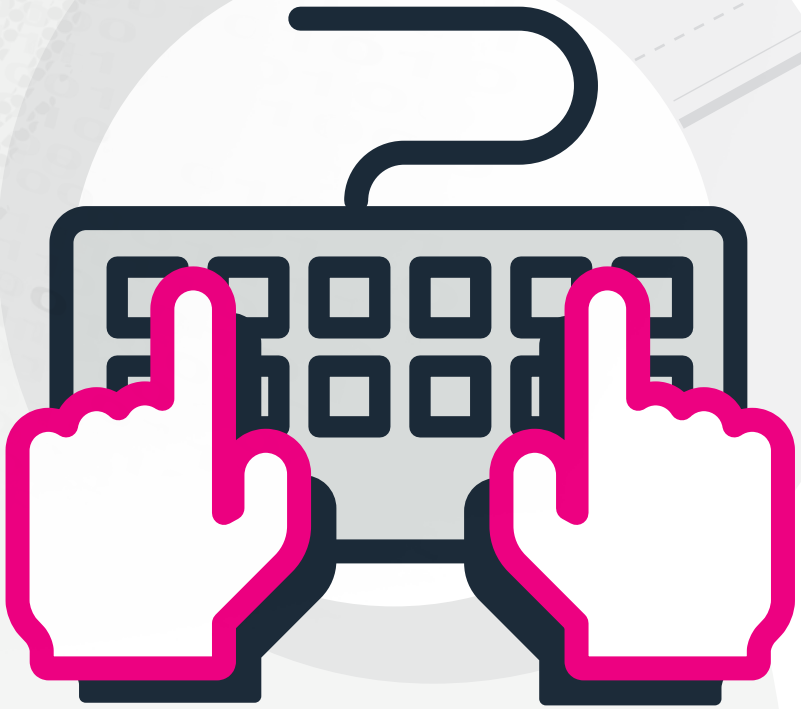
How the attack happens:

Attackers can deploy ransomware to enterprises 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 prompts the user with a pop-up or directs them to a website informing them that their files are encrypted and can be unencrypted if they pay the ransom.

Where the attack comes from:

Ransomware has typically been the work of advanced cybercriminal groups — to 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.

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 2019 Forbes Insights survey titled "Perception Gaps in Cyber Resilience: Where Are Your Blind Spots?" found that more than one in five organizations experienced a cyber incident originating from an unauthorized — or "shadow" — IT resource.

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 estimates a third of all enterprise cybersecurity attacks will be from shadow IT resources in 2020. 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.

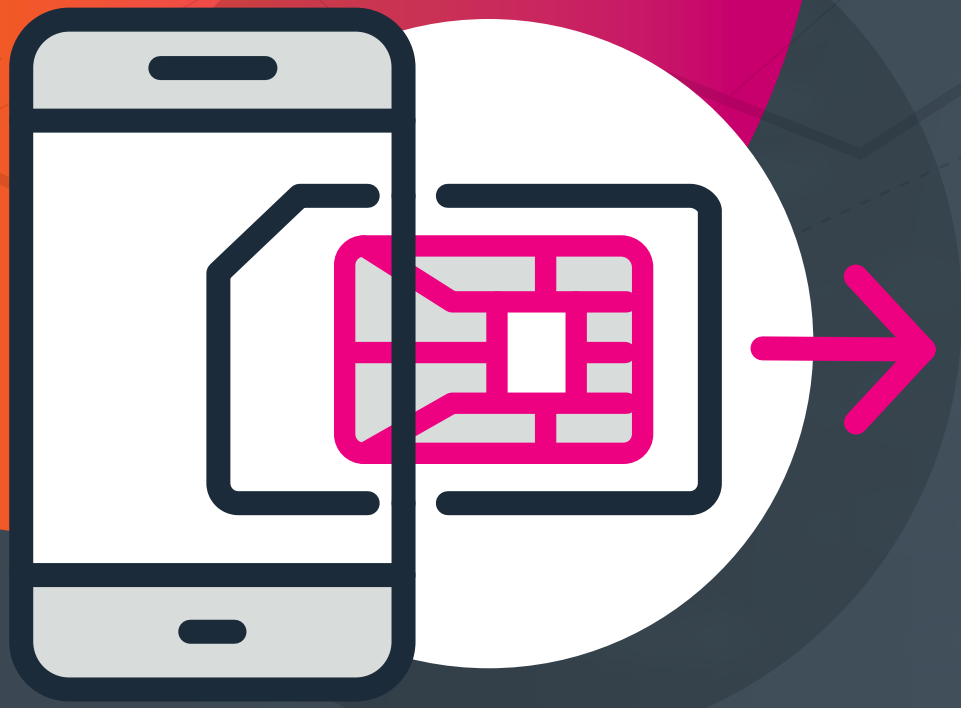
How the attack happens:

As the name suggests, the secretive nature of shadow IT is thanks 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.

SIM jacking



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.

SIM Jacking

What you need to know:

SIM jacking (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, SIM jacking is when someone impersonates you to your cellular provider in order to steal your cell phone number by having it transferred to a different SIM card, which is already in the hacker's possession.

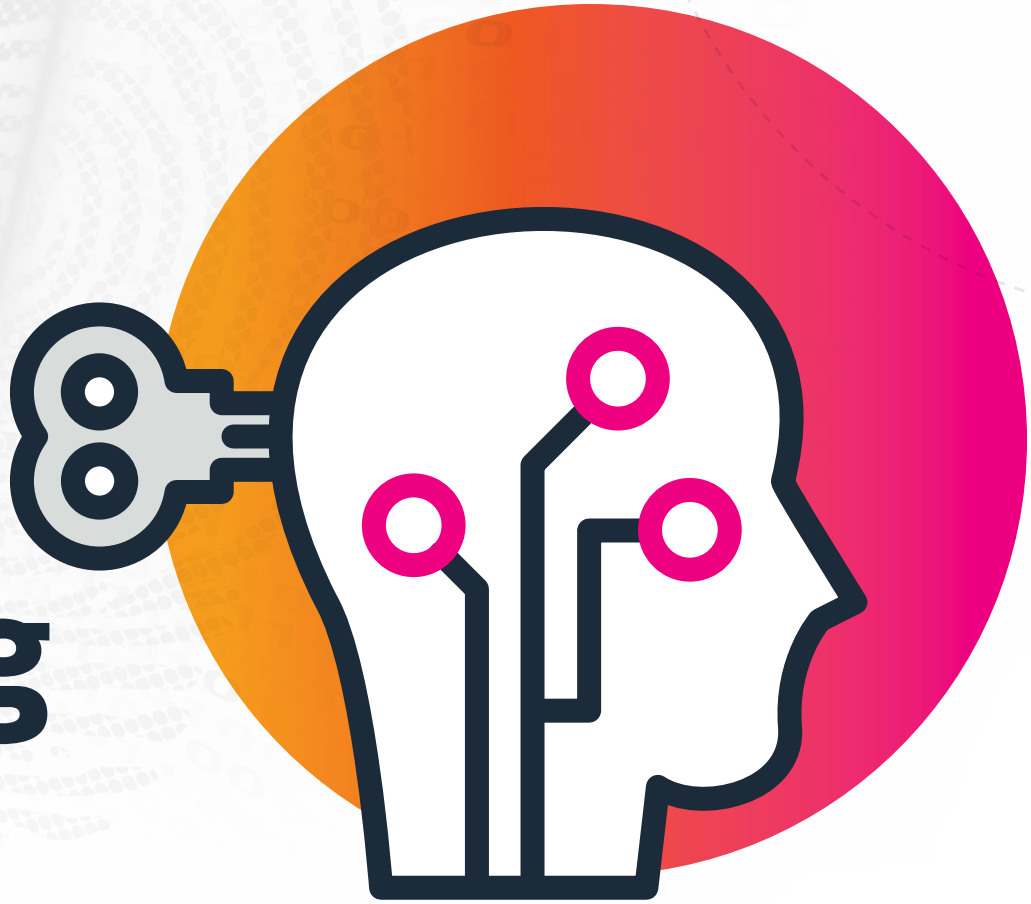
How the attack happens:

A hacker calls the support line for your mobile service provider, pretending to be you, saying they've lost their SIM card. They can verify their identity because they have acquired some amount of your 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 you, makes the switch. Instantly, your phone number — which is typically the key associated with the bulk of your digital life — is under someone else's control.

Where the attack comes from:

SIM jackers 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



The 2002 film Catch Me If You Can tells the true story of (perhaps) one of the most accomplished practitioners of social engineering of all time. In the film, Leonardo DiCaprio portrayed a man named Frank W. Abagnale, Jr., who executed various high-profile cons, committed bank fraud and masqueraded in a variety of personas, including as a physician and pilot. Abagnale's success depended on his ability to convince his victims that his forgeries, whether they were checks, diplomas or identities, were genuine. Abagnale was an active con man in the '60s and '70s, but the practice of social engineering has continued to develop and remains a powerful tool for hackers and fraudsters to gain access to closed systems around the world.

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 the five most common forms of digital social engineering assaults. A perpetrator first investigates the intended victim to gather 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. Most commonly, it comes in the form of phishing emails. Other forms include pretexting, wherein 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.

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. As recently as November of 2019, a vulnerability was discovered in phpMyAdmin, one of the world’s most widely used MySQL database management applications, that allowed hackers who created a specific username to gain access to the targeted site’s backend, allowing them to delete server configurations and revoke administrator access to the site.

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 10,887 results.

Spear Phishing

It's no secret that spear phishers target big fish. Walter Stephan, CEO of airplane part manufacturer FACC had been in his position for 17 years when he got duped by a phishing scam and unknowingly forked over $56.79 million of company funds. In the classic spear phishing scheme, cybercriminals pretended to be someone with authority in the company and sent an email to the CEO requesting a secret transaction. Stephan fell for the scam and was promptly fired for his lack of discretion. The firm did manage to recover about a fifth of the money, but the rest was irrevocably lost to criminal accounts in Slovakia and Asia.

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 you or your employees into giving away financial or proprietary data or unlocking access to your network. Spear phishers target individuals who either have access to sensitive information or are weak links to the network. If you're a high-value target, such as a C-level executive or company board member, you might be especially vulnerable, because you have access to critical systems and proprietary information within a company.

How the attack happens:

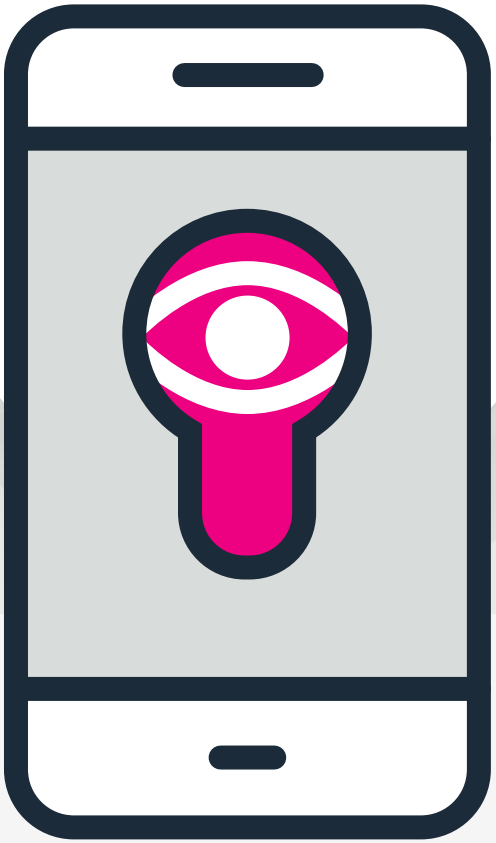
Spear phishers do their research to identify you and your position at your financial institution with social media sites like LinkedIn. From there, they'll spoof addresses to send highly personalized, authentic-looking messages to infiltrate your infrastructure and systems. Once the hackers gain access to your environment, they will 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, that have the resources to research their targets and bypass strong security filters. The Russian cyber espionage group Fancy Bear, for example, used spear phishing techniques to target email accounts connected to Hillary Clinton's 2016 presidential campaign, John Podesta, and former U.S. Secretary of State, Colin Powell. The group's attack was detailed in Robert Mueller's redacted 2019 "Report on the Investigation Into Russian Interference in the 2016 Presidential Election." While spear phishers hail from all over the world, in the last few years many complex spear phishing attacks have been based in Eastern Europe. Last year U.S. federal officials arrested three Ukrainians involved in the cybercrime organization FIN7, linked to hacking more than 3,600 businesses across the U.S. and stealing more than 15 million credit and debit cards.

Spyware

In 2017, the infamous WannaCry attack caused a significant disruption across systems used by industrial and public services, including hospitals, transportation and manufacturers. Companies like FedEx and Spain's Telefónica were affected, as well as the UK's National Health Service. Scarily enough, this is just one example of how an attack can be executed by quietly infecting computers on critical city and network infrastructures, subsequently exfiltrating sensitive information for monetary gain.



Spyware

What you need to know:

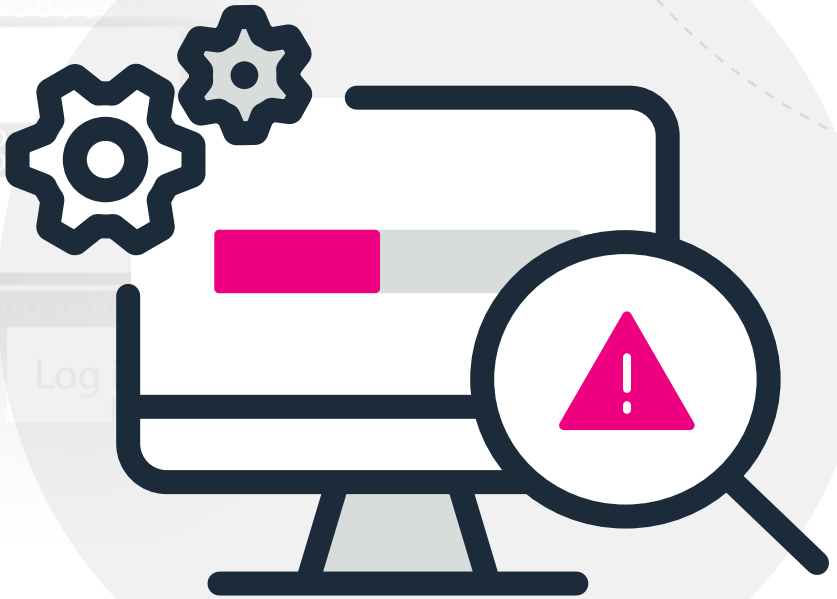
Spyware is a type of malware that aims to gather personal or organizational data, track or sell your web activity (e.g., searches, history, and downloads), capture your bank account information and even steal your identity. Multiple types of spyware exist, and each one employs a unique tactic to track you. Ultimately, spyware can take over your 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 your device through various means, but will commonly get a foothold in your system by duping the user or exploiting existing vulnerabilities. This can happen thanks to carelessly accepting a random prompt or pop-up, downloading software or upgrades from an unreliable source, opening email attachments from unknown senders, or pirating 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 your information to a third party.



System Misconfiguration

Chris Vickery, renowned security researcher, revealed a startling discovery: He had uncovered a public database containing personal information for almost 200 million US voters. Turns out, a conservative data firm had hosted voter information on an Amazon S3 server, but in doing so, completely messed up the configuration. Some of the data on the server was protected, but more than a terabyte of voter information was publicly accessible to anyone on the web.

System Misconfiguration

What you need to know:

Security misconfiguration is a wide spread problem that can put organizations at risk thanks to incorrectly configured security controls (or lack thereof). This can happen at almost any level of the IT and security stack, ranging from the company's wireless network, to web and server applications, to custom code.

How the attack happens:

This type of attack usually happens because of missing patches, use of default accounts, unnecessary services, insecure default configuration and poor documentation. This could range from the failure to set a security header on a web server, to forgetting to disable administrative access for certain levels of employees. This attack can also happen when hackers take root in legacy applications with inherent misconfigurations because of lack of updates.

Where the attack comes from:

Misconfiguration isn't considered a malicious act in and of itself, mostly due to being a result of human error. However, attackers may know where to look if they suspect a lax level of configuration across a certain organization's IT stack.

Typosquatting

Mike Rowe was an ordinary teen who wanted to make a buck. In 2004, he started a web design business where he displayed his brilliant marketing acumen.

Rowe realized his name had an uncanny resemblance to Microsoft. He just needed to add the last syllable to complete the trick. Inevitably, Microsoft sued Rowe, saying the Canadian was infringing on the company's copyright and that he was "typosquatting." Microsoft offered Rowe $10 to transfer the domain to the company. He refused, but eventually settled for little more than an Xbox.

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.

While you can educate your users and customers about the risks and threats posed by typosquatting, phishing and corporate espionage, human error is a fact of life. Of course, most adversaries are all too aware of this reality and will happily leverage it for insidious reasons whenever possible — like phishing with lookalike addresses, embedding faux command-and-control domains in malware, and hosting malicious content on domains that closely mimic your 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.

Watering Hole Attacks

Watering hole attacks are successful because cybercriminals bank on the likelihood that visitors will come to popular sites — like wildlife around watering holes. And they're often right.

That rang especially true when cybersecurity researchers uncovered a cyberespionage campaign in 2018 that leveraged watering hole techniques to target a central Asian country's national data center in an attempt to gain access to numerous government resources. Researchers attributed the attack to the Chinese-speaking threat group known as LuckyMouse, who apparently conducted classic watering hole attacks dating back to 2017. While the initial attack vector is unclear, researchers believed LuckyMouse possibly aimed to compromise national data center employee accounts.

Watering Hole Attacks

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 used is normally a zero-day attack — the goal being to infect the computer system with a zero-day exploit to gain access to their 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 they can exploit. By exploiting these vulnerabilities, 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 system and the ability to 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 and China. One famous example occurred in 2014, when a Chinese-based attack group exploited two zero-day vulnerabilities to display malicious code on the Forbes website, infecting anyone who visited Forbes.com.

Web Session Cookie

Almost every web application we use, from social media and streaming platforms to cloud services and financial applications, run on authentication cookies. These cookies make our experience on the web much more convenient, but represent a vulnerability that malicious actors can abuse to great effect. In late 2018, a malware program targeting Mac computers stole cookies tied to cryptocurrency wallets, stored credit card data, text messages and more, allowing the thieves to manipulate cryptocurrency values, create fraudulent charges and steal victims' identities.

Web Session Cookie

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.

Whale Phishing

Why go after little phish when you can phish a whale? Former presidential candidate Hillary Clinton found out the hard way.

In 2015, Clinton's campaign chairman John Podesta received an email that appeared to be from Google. It told him someone had tried to log into his Gmail account from Ukraine and he needed to change his password immediately.

The problem was that the email was not real and the link to change the password was a URL shortener. A group of hackers gained access to Podesta's account and the Democratic party's opposition research — the rest is history.

Whale Phishing

What you need to know:

Whaling is when hackers go after a “big fish” like Podesta or a CEO. The target is always someone specific, whereas a phishing email may go after anyone at a company. The hackers also usually go after the high-profile target because he or she may possess important or sensitive information.

How the attack happens:

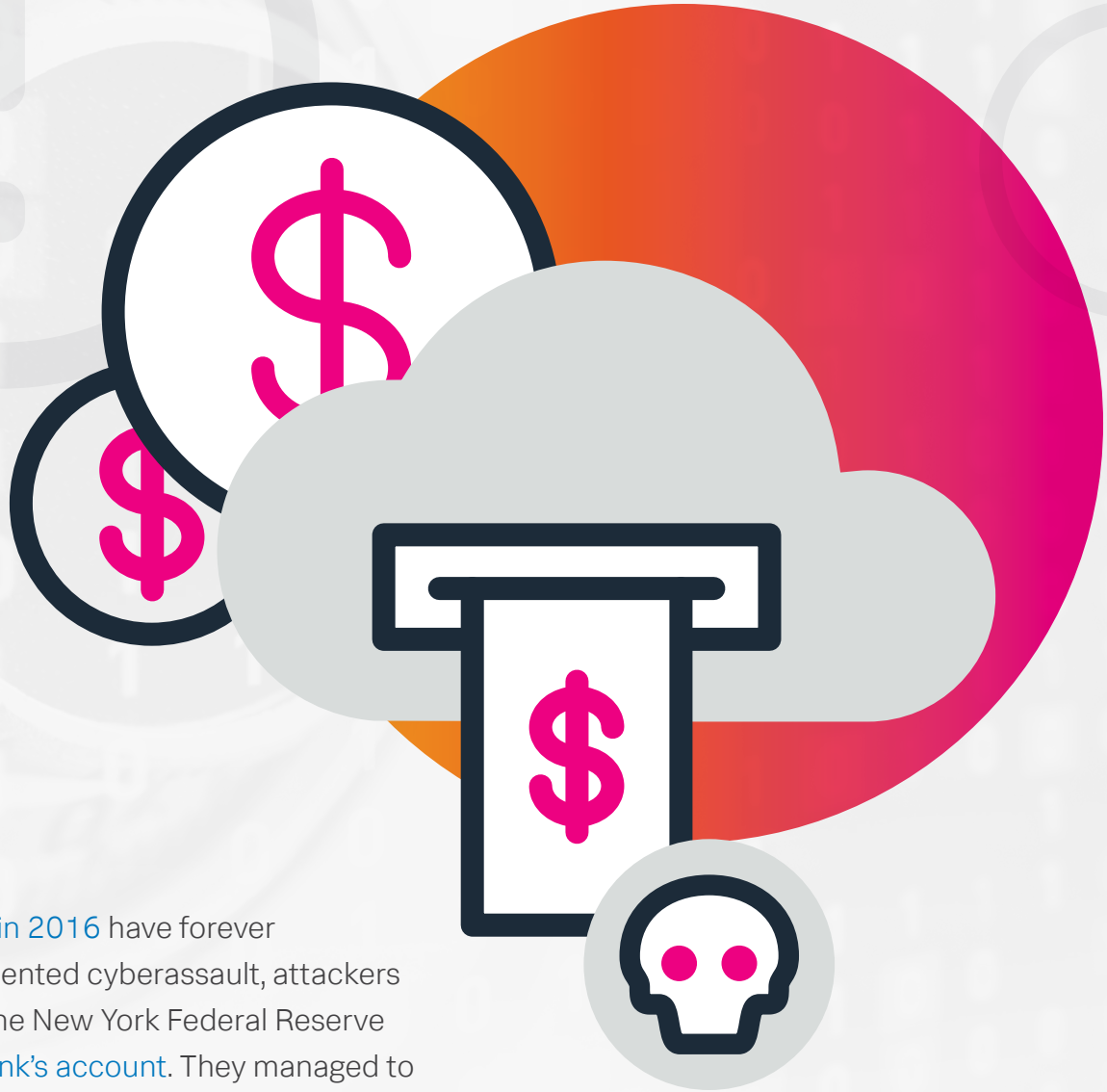
The technique used in a whaling attack is a classic phishing practice. The target receives an authentic-looking email, usually asking them to click on a link that contains malicious code or leads to a website that asks for sensitive information, such as a password.

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.

In the case of Podesta, the FBI indicted Russian citizens who were allegedly after sensitive information the Democratic party might have had in the run up to the 2016 presidential election.

Wire Attack



Advanced targeted attacks such as the SWIFT attack in 2016 have forever changed the cybersecurity paradigm. In this unprecedented cyberassault, attackers sent fraudulent messages over the SWIFT system to the New York Federal Reserve trying to transfer nearly $1 billion from Bangladesh Bank's account. They managed to successfully divert $81 million from the U.S. Federal Reserve to illicit accounts in the Philippines. Most of the money was never recovered.

Wire Attack

What you need to know:

Wire attacks are sophisticated schemes that send fraudulent high-value payments through the SWIFT international wire transfer network. Going beyond ordinary wire fraud, attackers often target banks in emerging markets with limited cybersecurity infrastructure or operational controls. These cybercrime syndicates are after one thing: money. And lots of it.

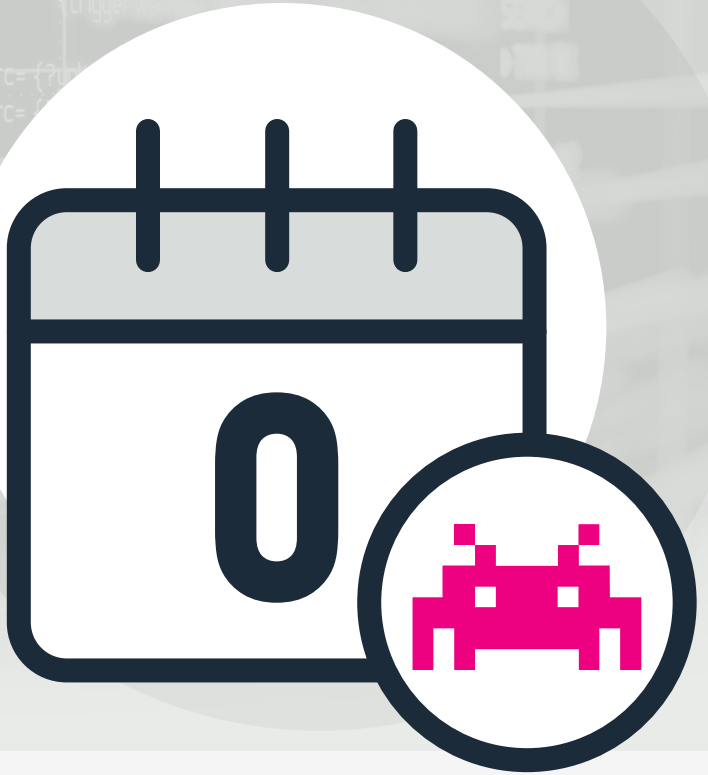
How the attack happens:

Attackers use sophisticated malware to bypass your local security systems. From there, they gain access to the SWIFT messaging network and send fraudulent messages to initiate cash transfers from accounts at larger banks.

Where the attack comes from:

Highly organized international and nation-state cybercrime groups, such as APT38 and the Lazarus Group, have historically been behind wire attacks. These groups have the necessary infrastructure and resources to successfully carry out these complex and multifaceted assaults. While it's unclear who exactly is behind the Lazarus Group and APT 38, some reports have indicated that they might have ties to North Korea. 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.

Zero-Day Exploit



In 2018, the Zero Day Initiative — a bounty program for zero-day vulnerabilities — reported 1,450 cases of launch day flaws in the products of some of the world's biggest and best-known companies. Adobe, Apple, Cisco, Google, Microsoft, Oracle and Samsung are among the many companies on the list, which lists vulnerabilities in networking devices, consumer and enterprise software and industrial machinery — technologies that affect every facet of our lives. In September 2017, Equifax's systems were breached due to a zero-day vulnerability, resulting in the theft of names, social security numbers, addresses and driver's license numbers for more than 143 million people.

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) scans 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. A 2016 report from Cybersecurity Ventures estimated that developers would generate 111 billion lines of new software code the following year. That volume of code provides a virtually infinite space for any type of hacker to discover and exploit zero-day vulnerabilities. Another report from Cybersecurity Ventures predicts that by 2021 a new zero-day exploit will take place every single day.

Learn More.

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

20-15119-SPLK-Top-50-Security-Threats-210-11x8.5-EB

splunk> turn data into doing™