CompTIA SECURITY+ Day 02

THREAT ACTORS AND VECTORS

In this course, we will:

- Compare threat actor types, attributes, and motivations
- Explore social engineering and common attack surfaces
- Look at supply chain vulnerabilities
- Examine application, O/S-based, web-based vulnerabilities
- Learn about hardware, virtualization, cloud, and mobile device vulnerabilities

THREAT ACTORS (AGENTS)

- Threat agents (or actors) are the persons, methods, operations, techniques, systems, or entities that act (or have the potential to act) with intent to initiate, transport, carry out, or in any way support a particular threat or exploit
- Threats are not realized without an agent or catalyst
- Can be comprised of an individual or a group
- The attacks can also be totally automated (bots)

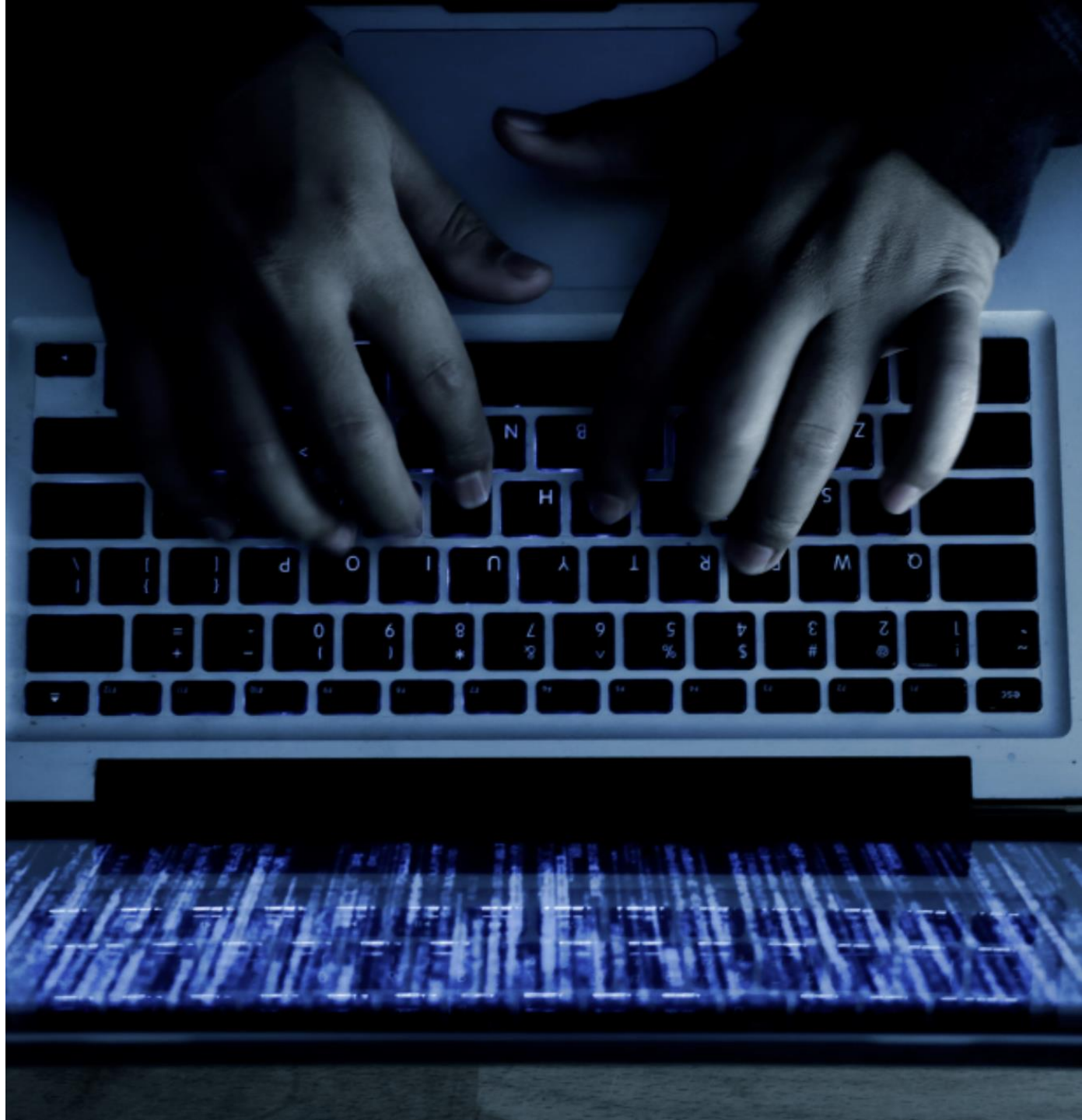
STRUCTURED	UNSTRUCTURED
Planned	Accidental
Organized	Non-malicious
Persistent	Drive-by web surfing
Multi-phased	No acceptable use policy (AUP)
Can be internal or external	Email and webmail
Exploit kits, zero-days, modules, ransomware	USBs and personal electronics

UNSKILLED ATTACKERS (SCRIPT KIDDIES)

- These originate from the combination of inexperienced crackers using script viruses and prepackaged malicious code (exploit kits and Malware as a Service [MaaS] campaign)
- The most common script viruses are spread via email attachments using preformed scripts and modules from exploit kits
- Newer techniques are often learned on YouTube and other social media sites in the dark web through ToR browsing
- These represent the lowest level of attacker sophistication and capability levels

HACKTIVISTS

- Hacktivism unofficially began in the late 1980s when viruses and worms spread messages of protest (e.g., "Worms Against Nuclear Killers")
- The term "hacktivism" was coined by the Cult of the Dead Cow, which also gave birth to "Hacktivismo," a group of international crackers protesting human rights abuses
- They are responsible for DoS, DDoS, ransomware, hijacking and defacing websites, and other cyber attacks to raise awareness



ORGANIZED CRIME SYNDICATES

- Organized cybercrime is a well-funded, multi-billion-dollar-a-year industry that affects all sectors of government and the economy
- They are the main contributors to advanced persistent threats (APTs)
- They perform cost-benefit analysis and other research before carefully choosing targets
- The campaigns may last months or years
- Example: The ALPHV/BlackCat ransomware operation

STATE-BASED ATTACKS

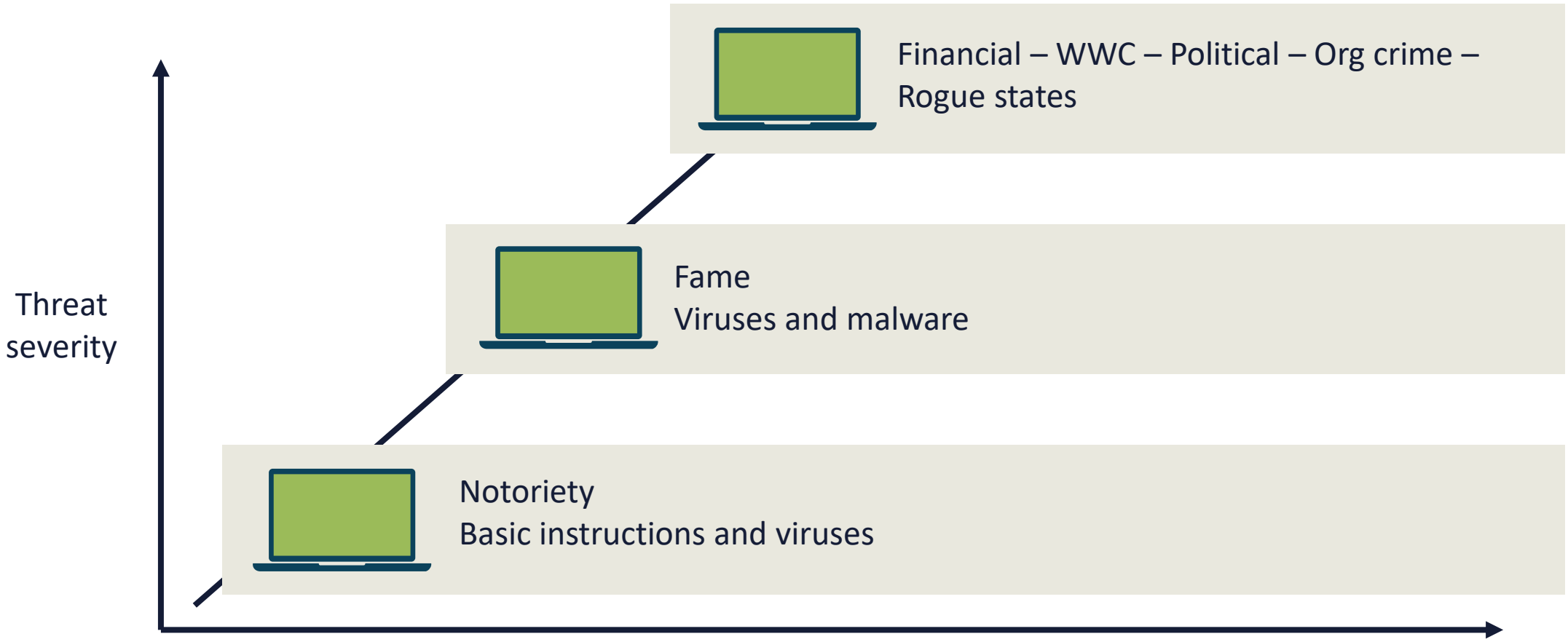
- The nation-state actor has a "license to hack" since they work for a government or military to disrupt or compromise target governments, organizations, or individuals to gain access to valuable data or intelligence
  - They might be part of a semi-hidden "cyber army" or "password crackers for hire" for companies that are aligned with the aims of a government or dictatorship
- They can create incidents and false flag operations that have international significance
- The nation-state actor has developed (along with criminals) many zero-day malware exploits that are waiting to be activated (e.g., a logic bomb)

Many security industry analysts and experts contend that the world has already entered a third world war in the form of a cyber war known as WWC (World War Cyber)

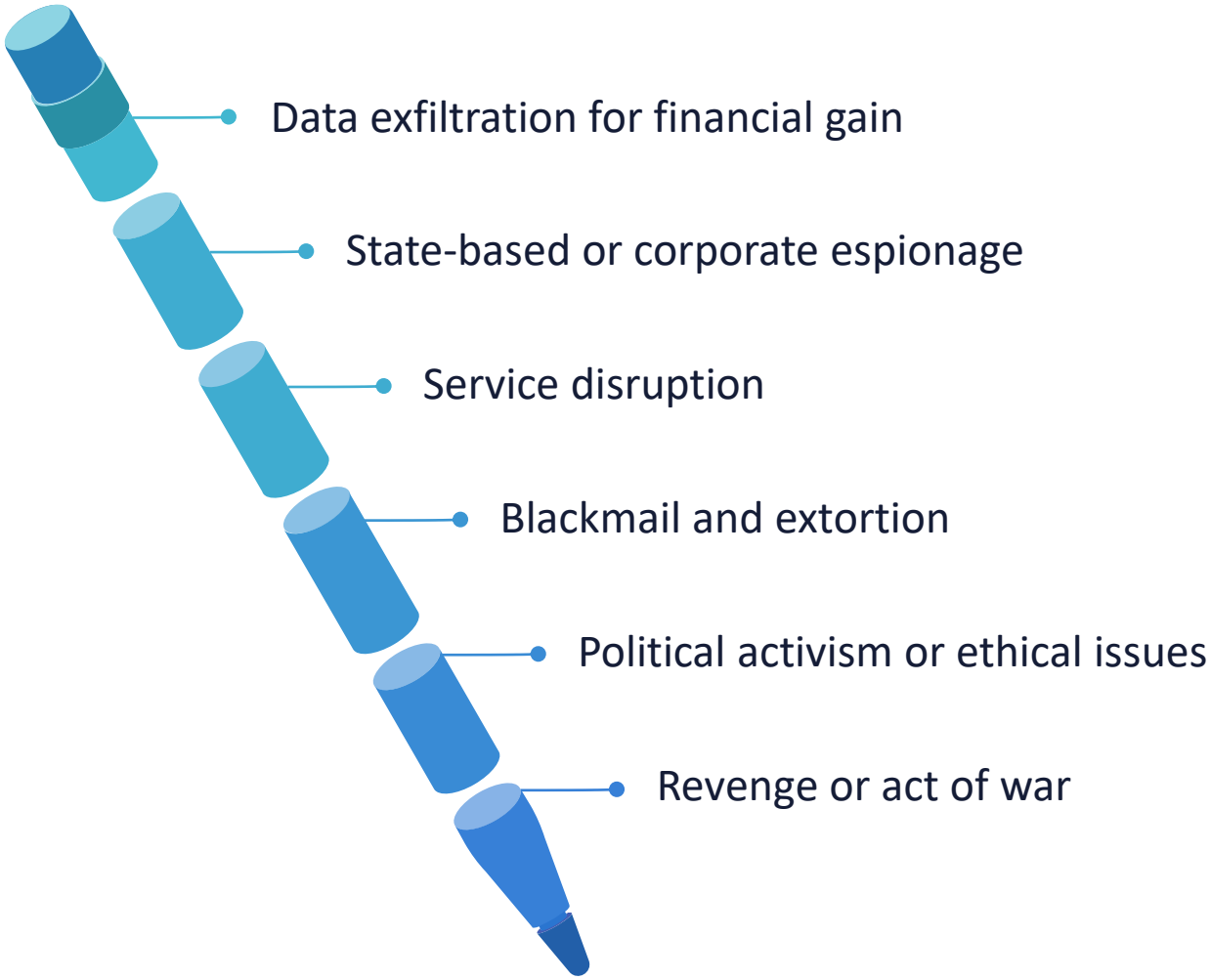
COMPROMISED PRIVILEGED INSIDERS

- These existing and recently released employees or contractors should be considered "public enemy number one"
- They can often have unfettered and elevated access and are the most likely to leave backdoors and other covert channels upon exit from the organization
- The term "compromised" is more accurate than "disgruntled" since there are several factors that can put an employee in a compromised position without being dissatisfied with the organization or other personnel

INTENT AND MOTIVATION



THREAT ACTOR MOTIVATIONS



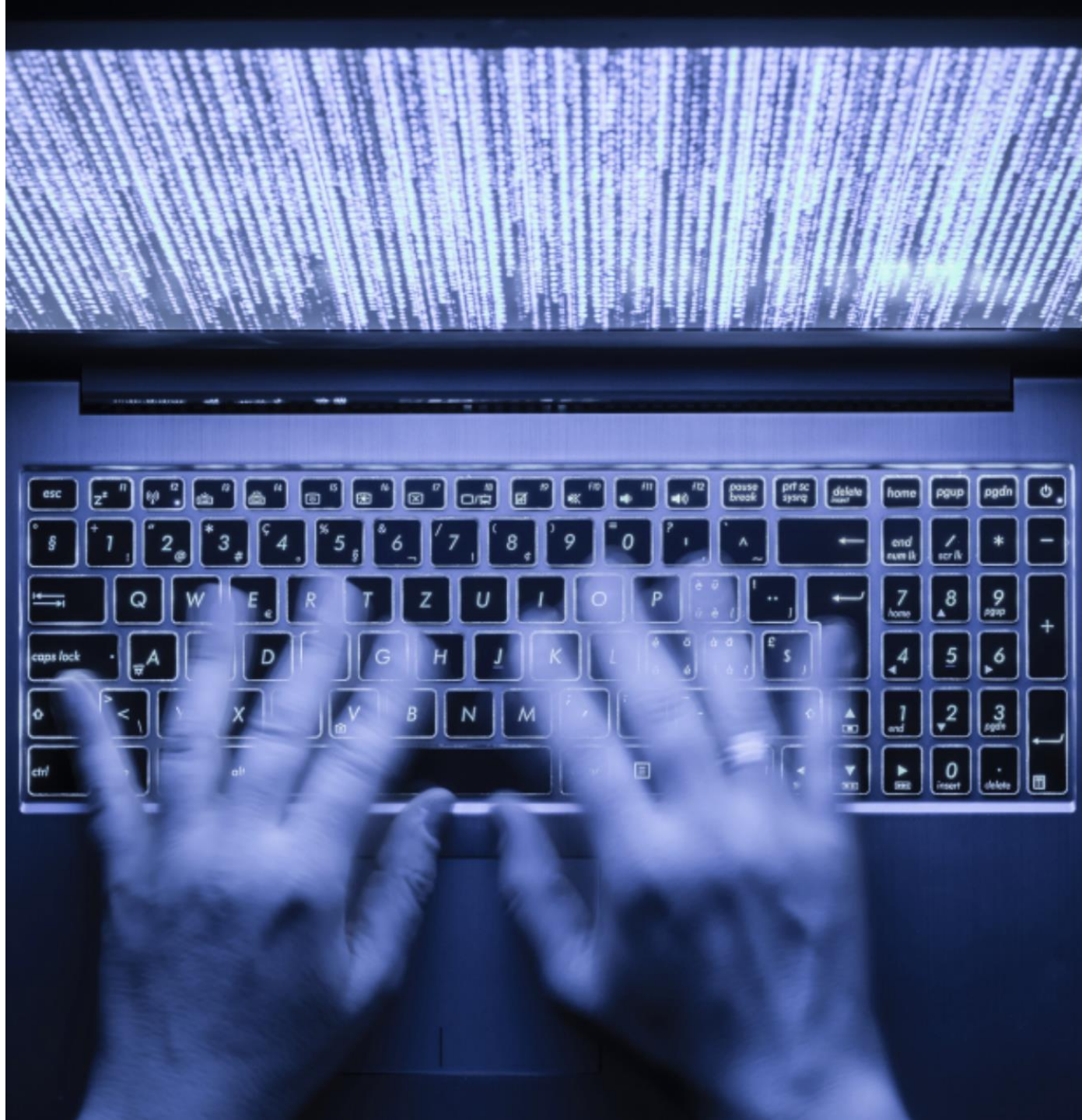
- Data exfiltration for financial gain
- State-based or corporate espionage
- Service disruption
- Blackmail and extortion
- Political activism or ethical issues
- Revenge or act of war

THE DARK WEB

- The dark web is the veiled collective of Internet sites that are not indexed and are only accessible by a specialized web browser such as ToR, Freenet, or Subgraph OS
- It is considered a part of the deep web
- It is a vast repository of Malware as a Service (MaaS) campaigns and resources

THE DARK WEB

- It is used for keeping Internet activity anonymous and private, which can be helpful in both legal and illegal applications
- While some use it to evade government censorship, it has also been known to be utilized for highly illegal activity, such as purchases of contraband and child pornography



PHISHING ATTACKS

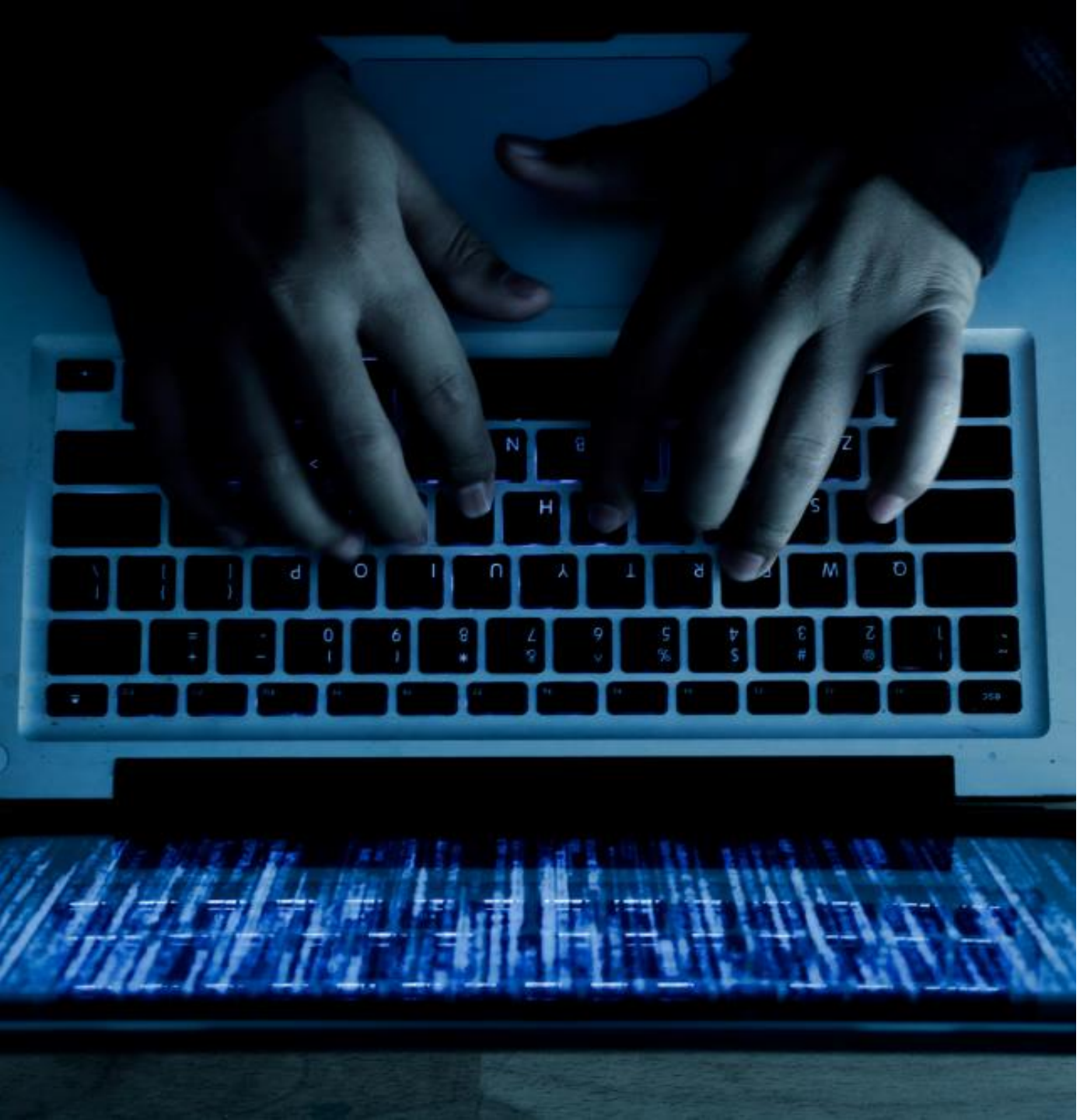
- Email phishing attacks or hoaxes are one of the most common exploit vectors available to crackers
- Phishing is a cyber attack that uses disguised email and webmail as a vector
- The goal is to trick the recipient into believing that the message is legitimate so they will click a link or download an attachment
- Common indicators are vague salutations, suspicious domains, wrong paths or hypertext, awkward grammar, urgency, lack of contact info, and spoofed headers/logos

PHISHING VARIANTS

- **Spear phishing** is a select, targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, often for malicious reasons
- **Whaling** is a spear phishing attack against high-level and highly privileged employees
- **Smishing** is using various text messaging formats (i.e., SMS) as a vector
- **Vishing** uses a voice over IP or telephony as the hoax vector

BUSINESS EMAIL COMPROMISE (BEC)

- Business email compromise (BEC) is a form of attack that targets companies that outsource, conduct wire transfers, and process invoices, often abroad
- It is often an elaborate advanced persistent hoax that targets corporate email accounts of high-level employees
- They are either spoofed or compromised through keyloggers or phishing attacks, often to perform fraudulent wire and cyber currency transfers
- Some attackers have successfully spoofed large vendors and customers, lawyers, CPAs, and even government officials (e.g., IRS)



SOCIAL ENGINEERING

- Eliciting information and reconnaissance
  - Shoulder surfing
- Dumpster diving
  - Credential harvesting
- Hoaxes and impersonation
- Identity fraud and invoice scams
  - Pretexting using a fabricated story, or pretext, to gain a victim's trust; brand impersonation
- Disinformation and influence campaigns
- Watering hole attacks

REASONS FOR SOCIAL ENGINEERING EFFECTIVENESS

Lack of proper security and awareness training

Inadequate acceptable use policy (AUP)

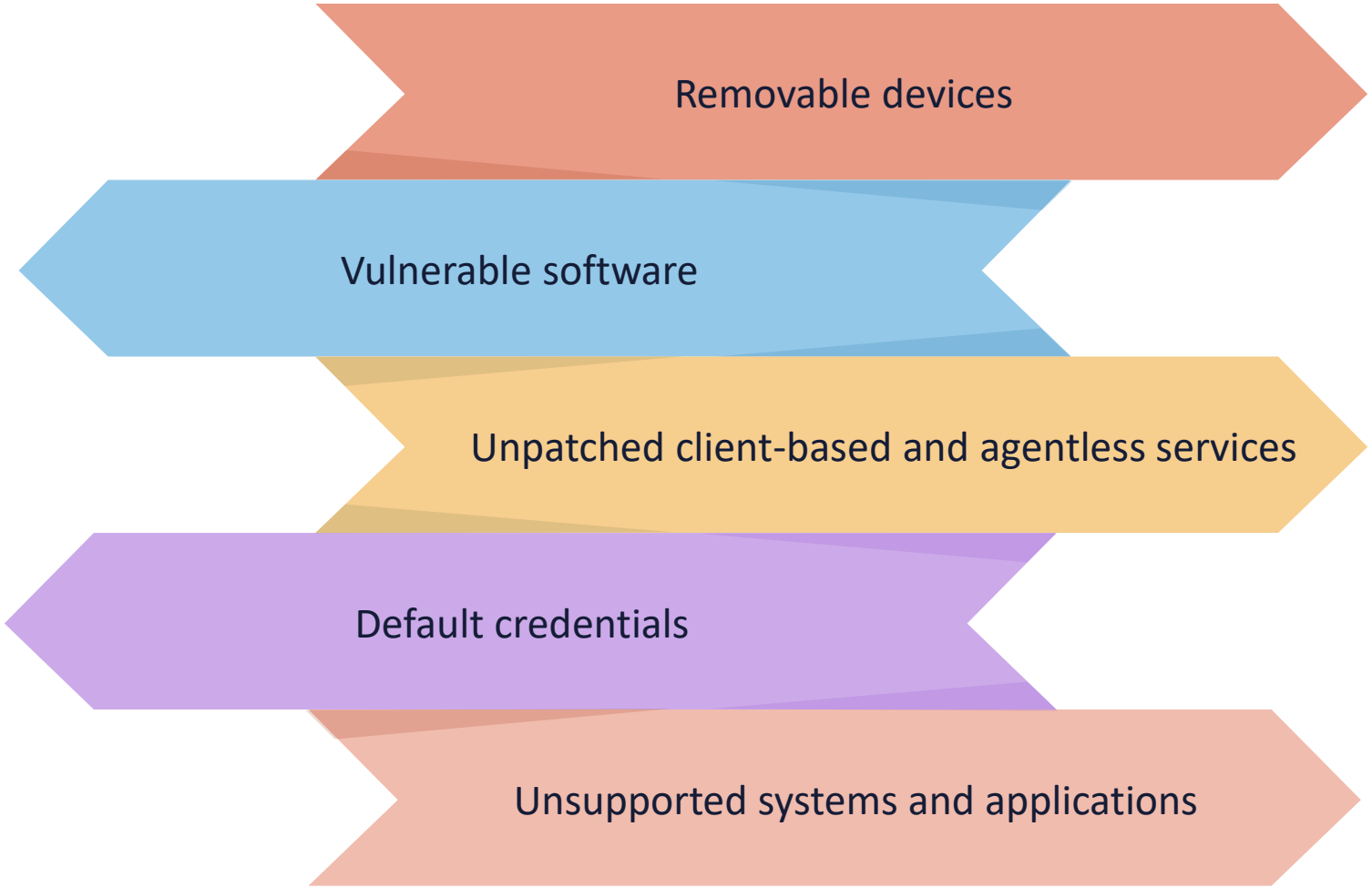
No buy-in from management and employees for prevention measures

No enforcement of policies – no carrot and no stick

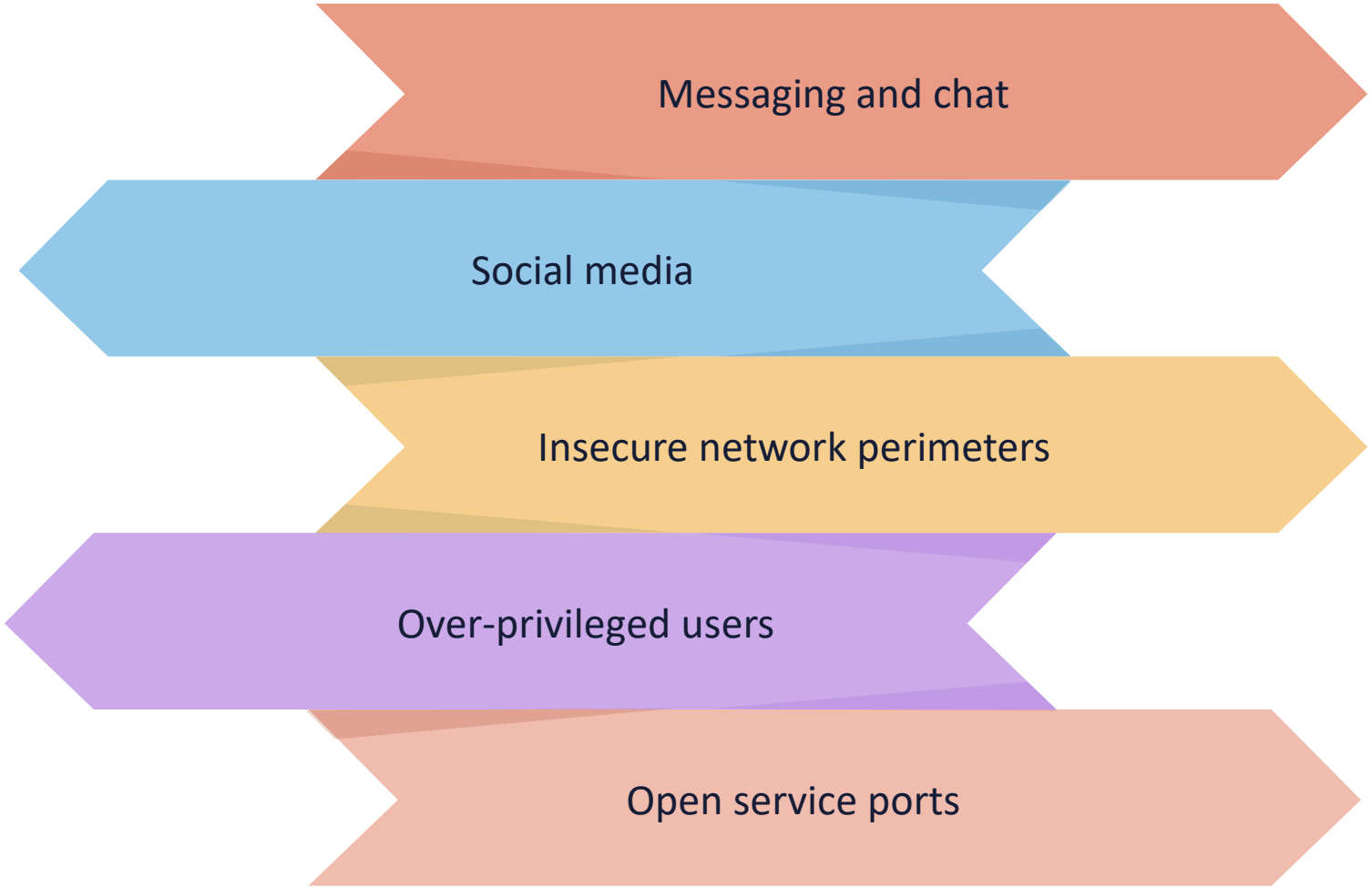
Outdated antivirus, DLP, and mobile device and application management tools

Poor perimeter security controls for email, messaging, telephony, and web activities

COMMON ATTACK SURFACES



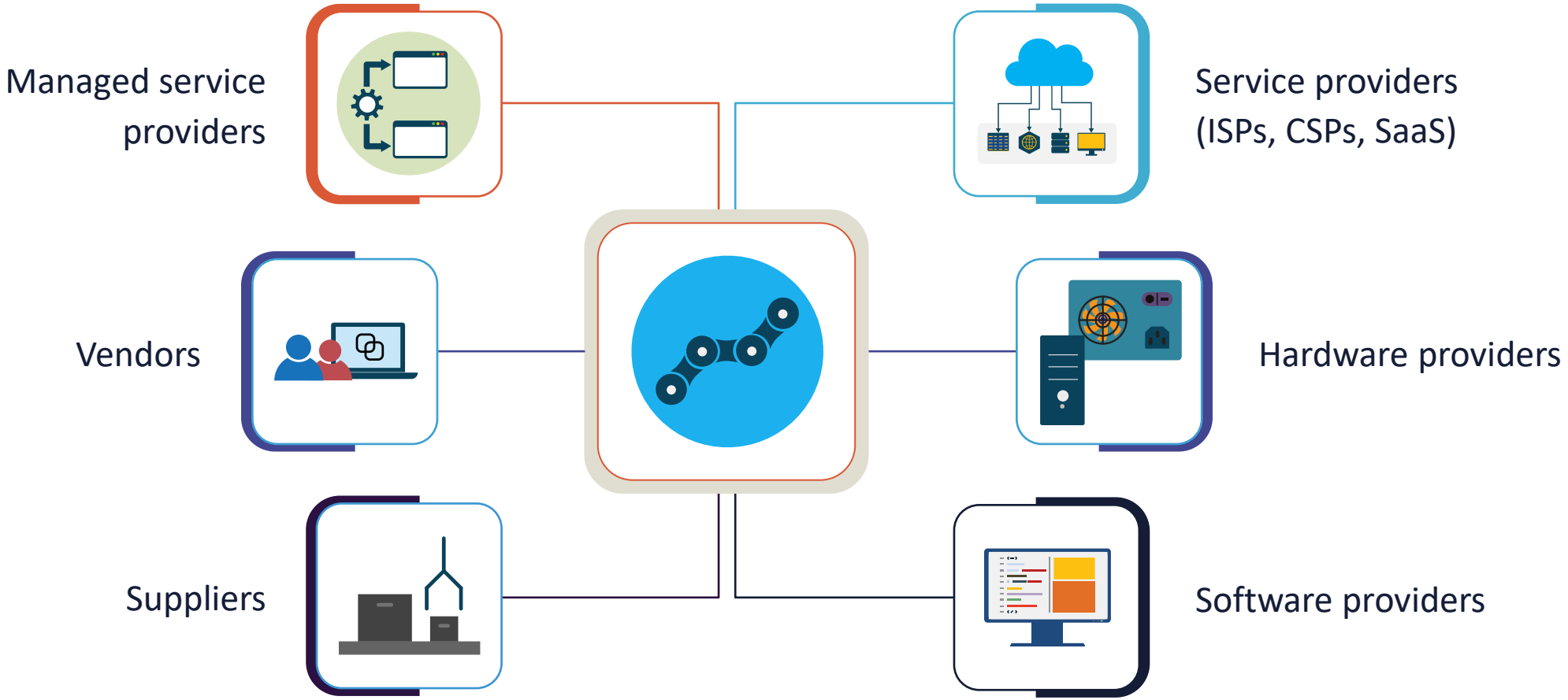
COMMON ATTACK SURFACES



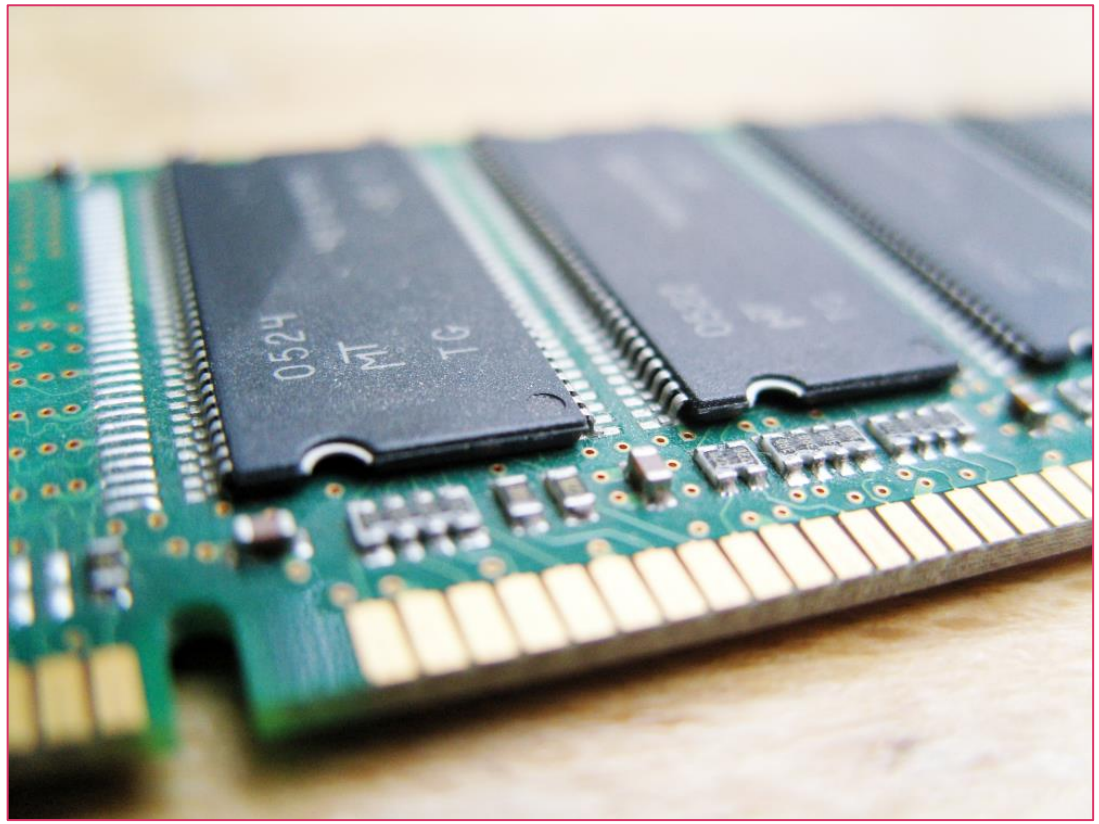
SUPPLY CHAIN VULNERABILITIES

- Software supply chain security continues to be a growing risk for organizations
- Experts predict this will only continue to rise, and damages could exceed 15% growth year-over-year for the foreseeable future
- Many organizations allow third-party organizations to have access to their networks and systems
- When an attacker exploits a vendor or partner, they can leverage this trust relationship to gain access to the organization’s infrastructure
- Zero trust initiatives are a powerful countermeasure to supply chain vulnerabilities

SUPPLY CHAIN VULNERABILITIES



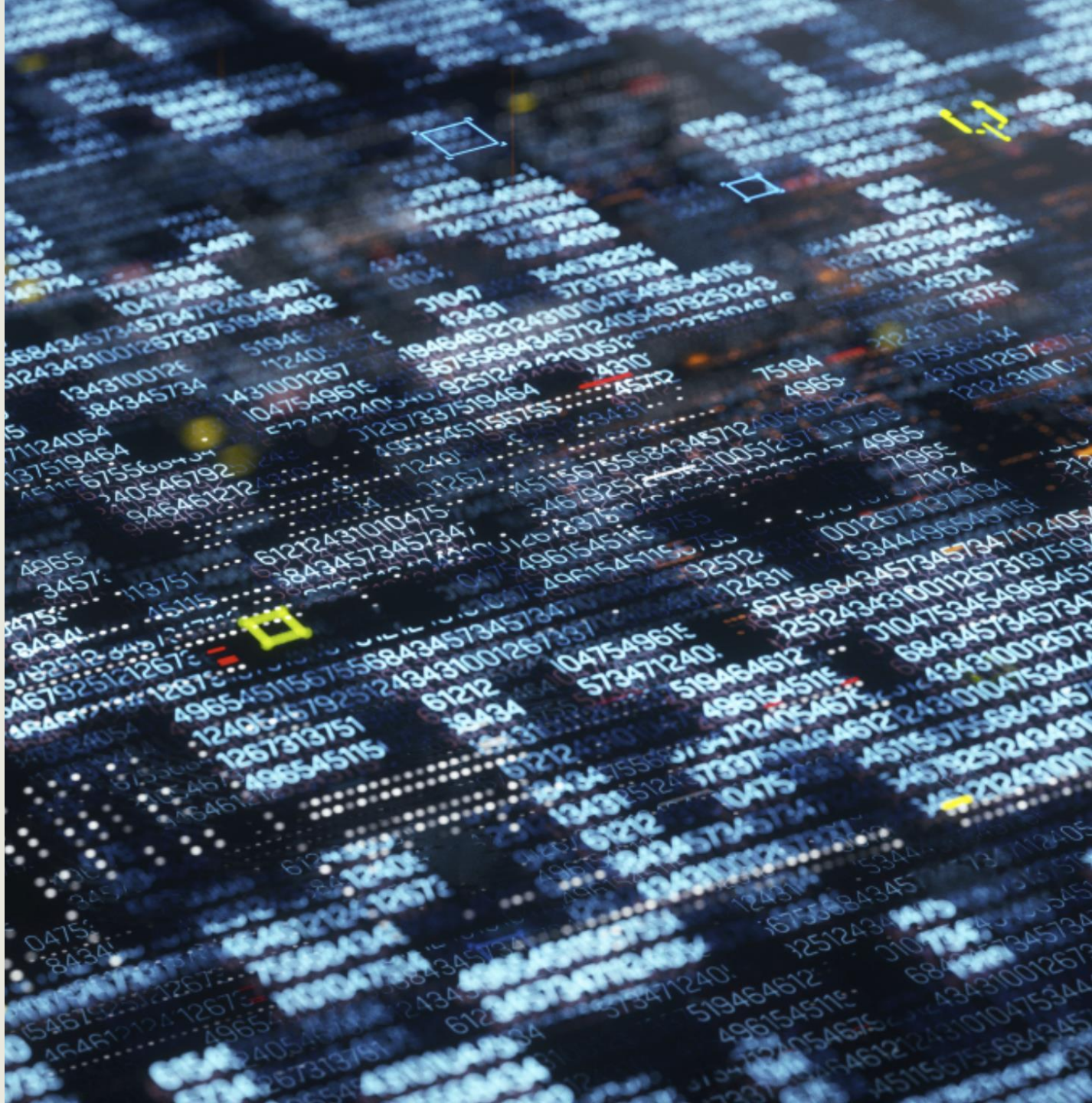
APPLICATION VULNERABILITIES: MEMORY INJECTION



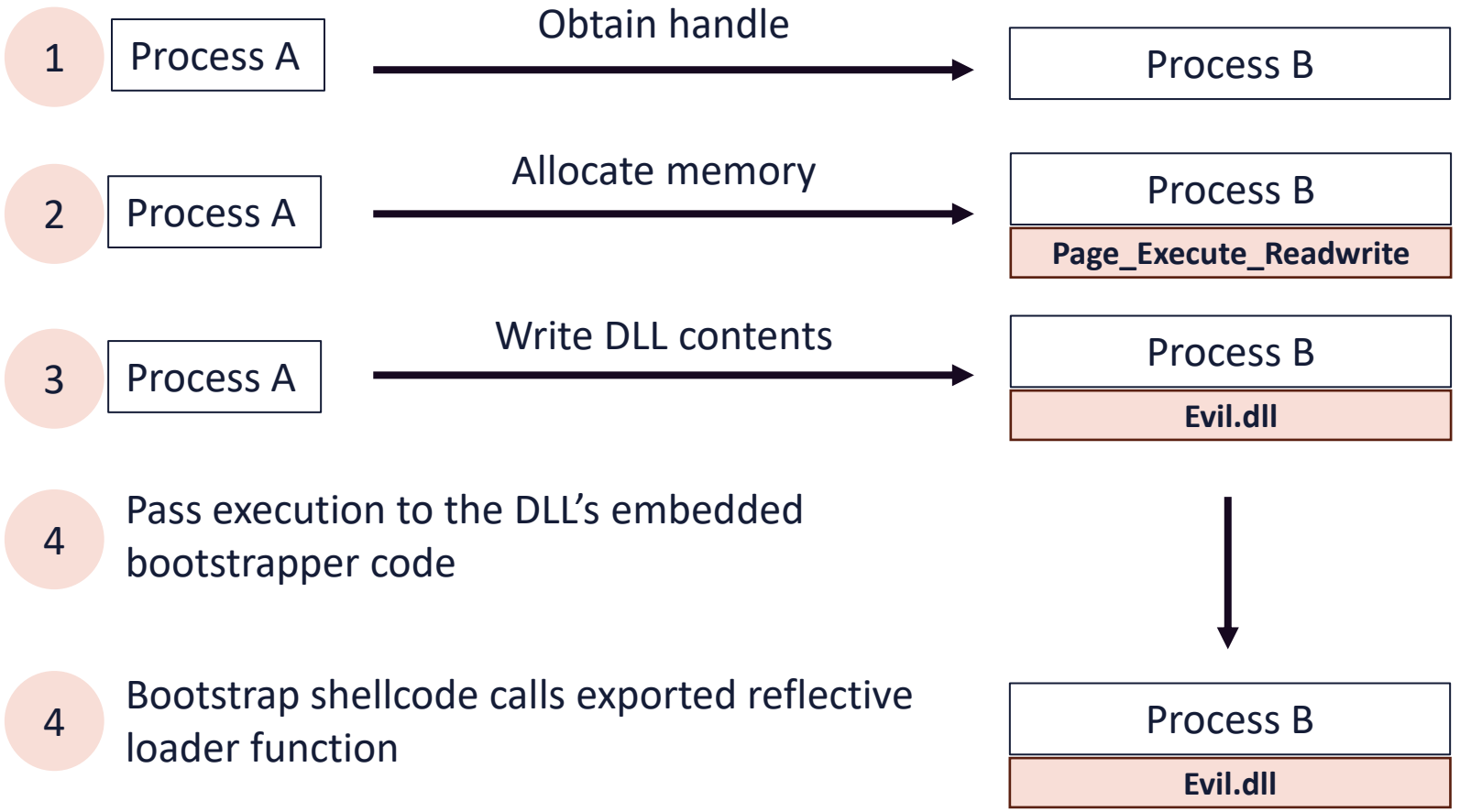
- **Shellcodes** are a small stub of code used as a payload
- A **DLL** is a shared library of functions that multiple programs can access
- A **process** is an instance of a program being executed
- A **thread** is a small sequence of instructions or a component of a process
- Windows API protocols allow interaction with the Windows OS
  - VirtualAllocEx reserves or changes a region of memory
  - WriteProcessMemory writes data to an area of memory in a specified process
  - CreateRemoteThread creates a thread in the address space of another process

APPLICATION VULNERABILITIES: EXAMPLES OF MEMORY INJECTION

- Shellcode injects malicious code into a running application of PowerShell, which is regularly used in attempts to execute in-memory attacks
- Process hollowing starts a legitimate process whose sole purpose is to be a container for malicious code - it delivers the process in a "suspended" state, then rewrites the content with the required code in memory, and continues to execution
- Reflective DLL injection is where contents of a rogue DLL are loaded into memory



REFLECTIVE DLL INJECTION

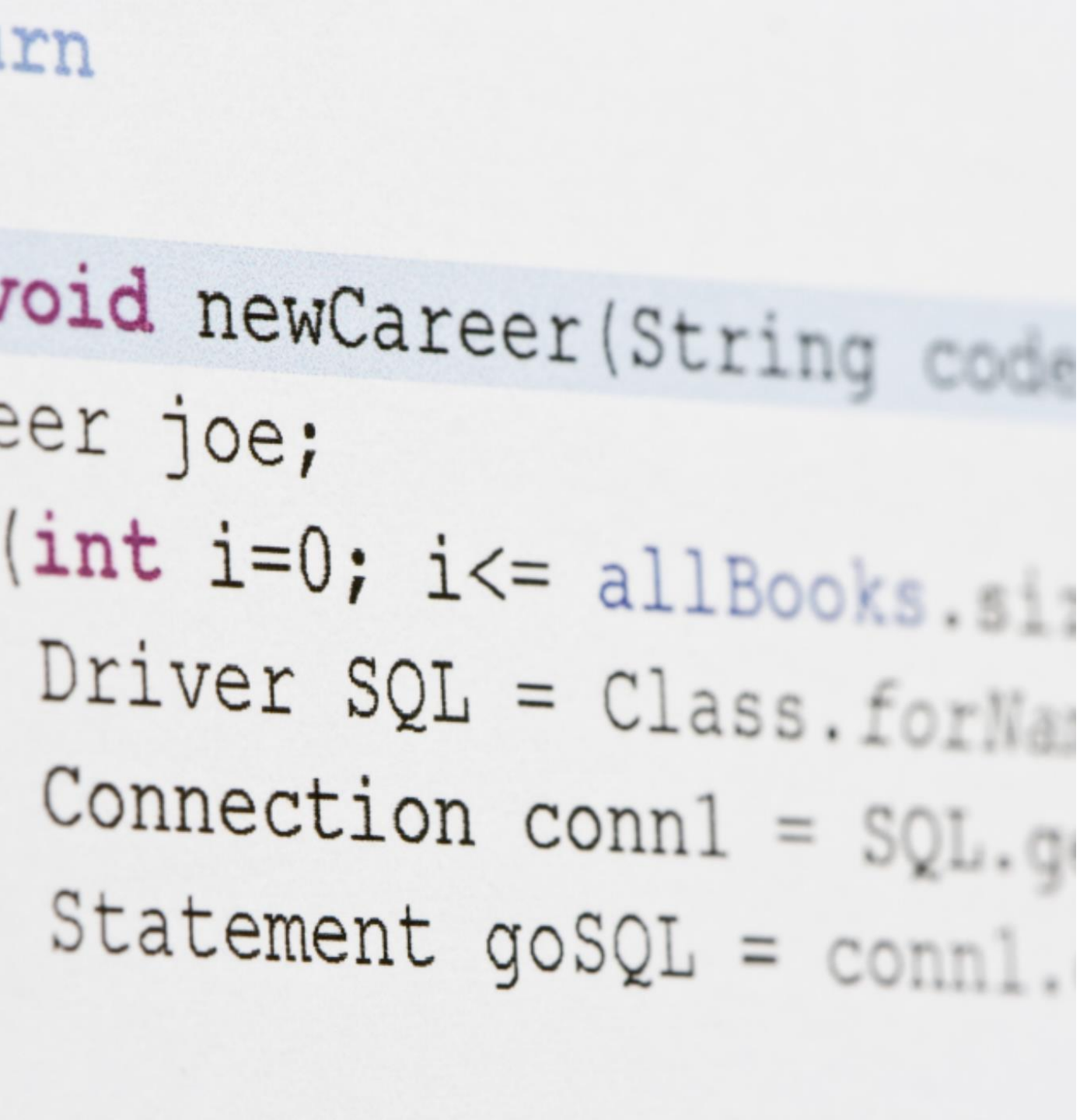


BUFFER OVERFLOWS

- In a buffer overflow attack, the attacker sends a larger-than-expected input
- For instance, when a front-end web server accepts it and writes it to memory areas
- Associated buffers are filled, and the adjacent memory is overwritten as a result
- This "overwrite" may contain malicious instructions or code that crash the server or runs a persistent remote access trojan

OS-BASED AND WEB-BASED VULNERABILITIES

- One of the most prevalent misconfiguration habits is leaving debugging features enabled in production environments
- It is critical to make sure that debugging functionality is disabled or properly secured in production environments
- Another common misconfiguration comes from the use of default or weak credentials for various system components such as operating systems, databases, network devices, or application interfaces
- All systems should use tested patch management

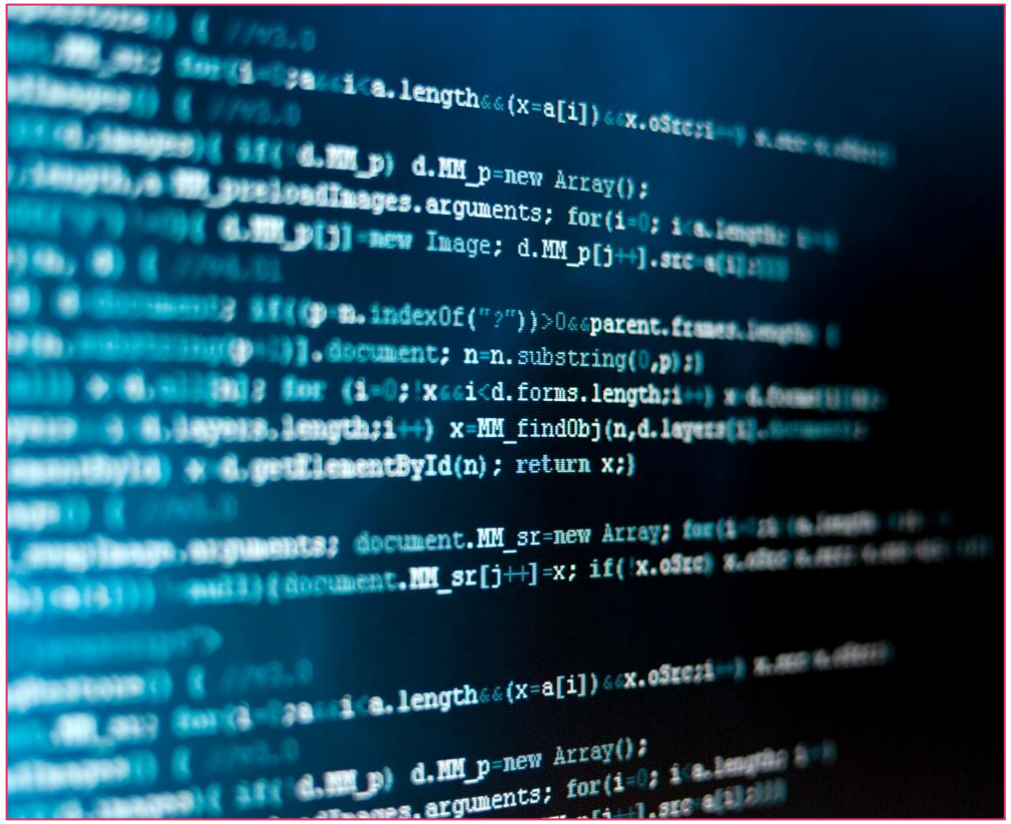


SQL INJECTION (SQLI)

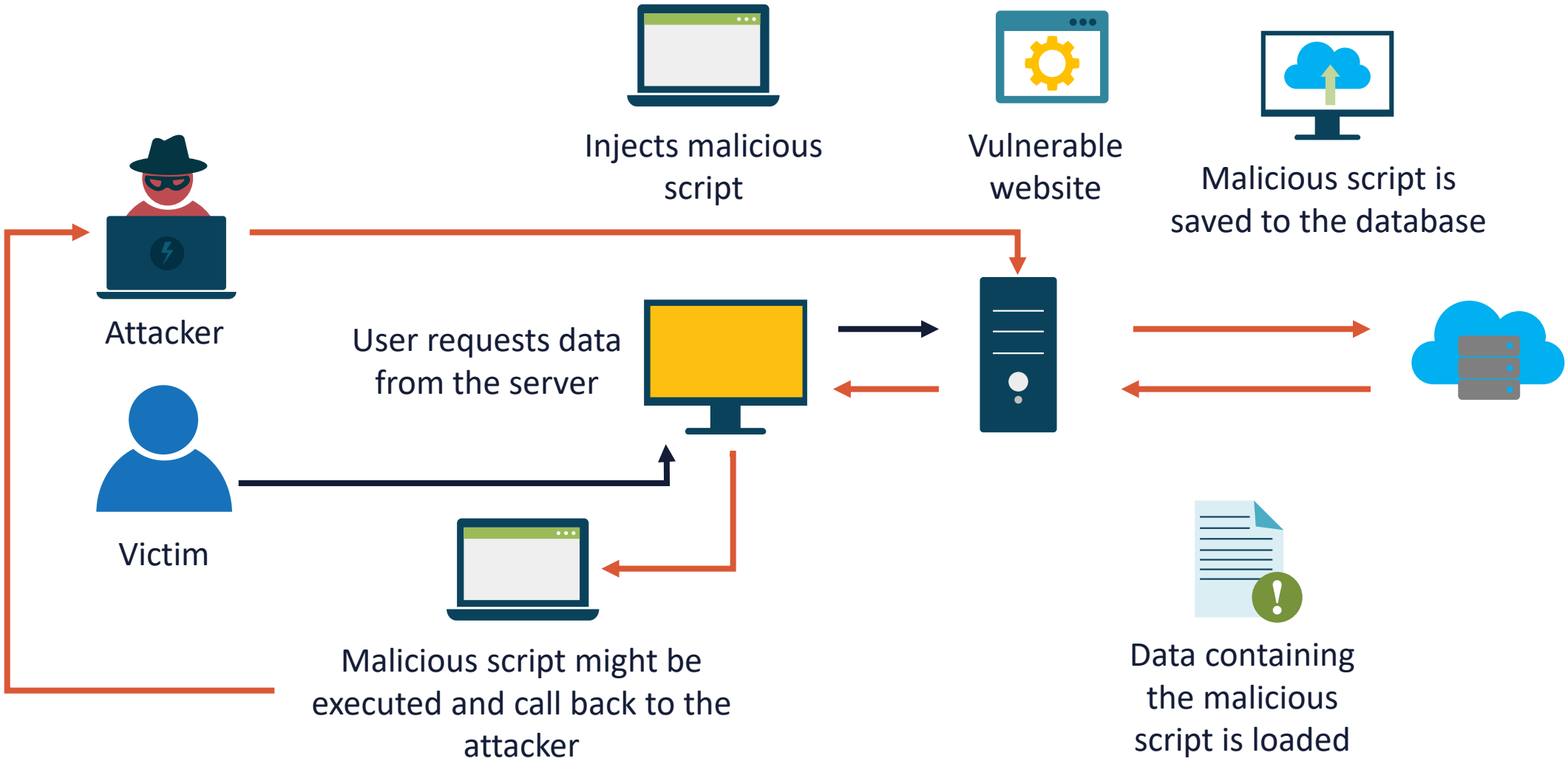
- This common attack has been run against front-end services like web servers and Microsoft SharePoint that use SQL as a database repository
- It involves inserting a SQL query through input data from client-to-server applications:
  - Read sensitive database data (SELECT FROM)
  - Change database data (INSERT, UPDATE, DELETE)
  - Execute administrative functions (e.g., shut down DBMS)
  - Get the contents of files on a database management system (DBMS)
  - Run commands on an operating system

CROSS-SITE SCRIPTING (XSS)

- Flaws in pages rendered by web servers and not the web server code itself (i.e., Apache, IIS) where malicious scripts or code are injected into trusted or innocent website pages
- Malicious scripts can steal cookies, session tokens, or other sensitive data stored by the browser and used with the site
- Attacker typically sends browser-side scripts to end user
- Can occur anytime a web program uses user input within the output it generates without validating or encoding

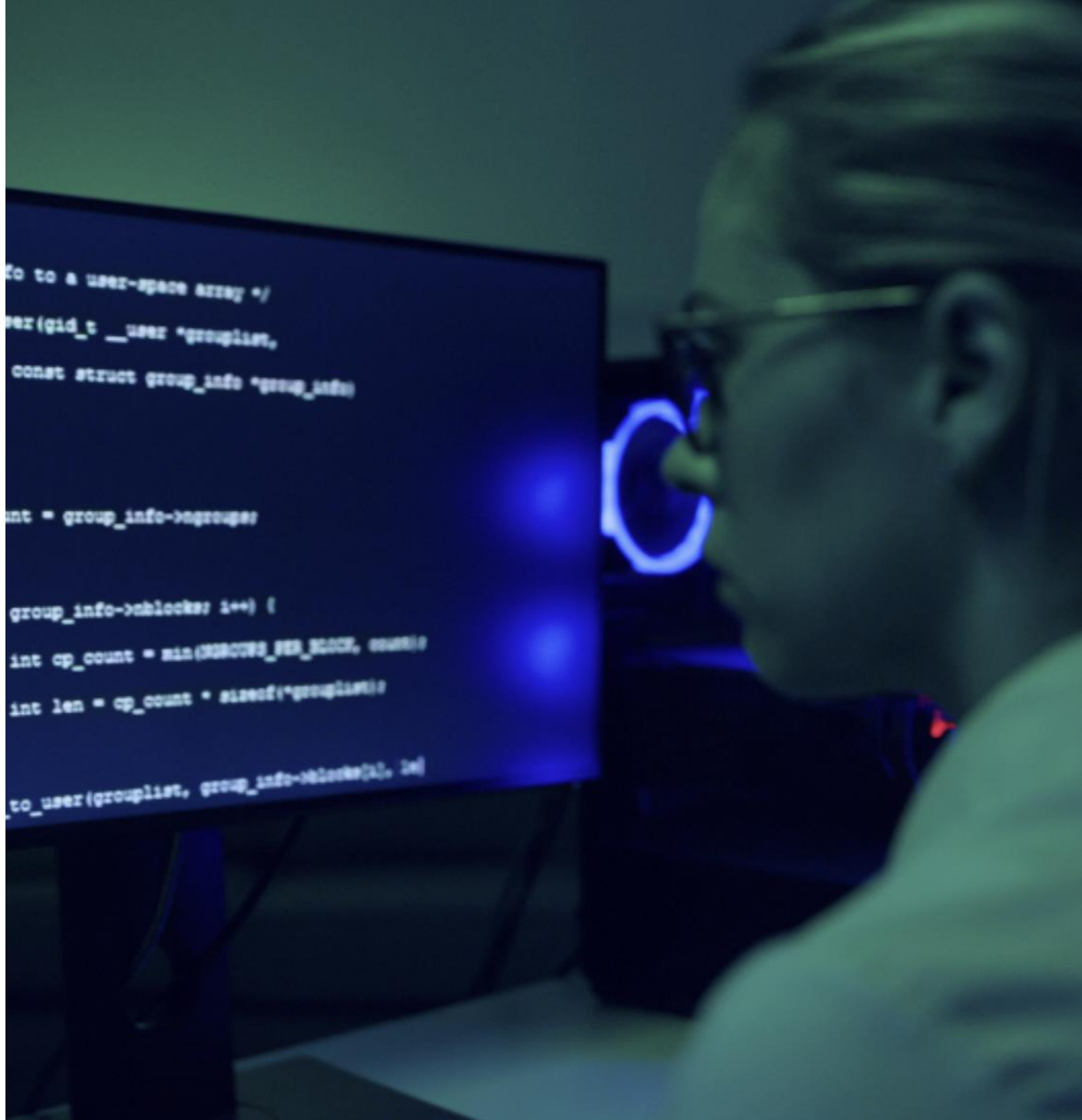


CROSS-SITE SCRIPTING (XSS)



XSS VARIANTS

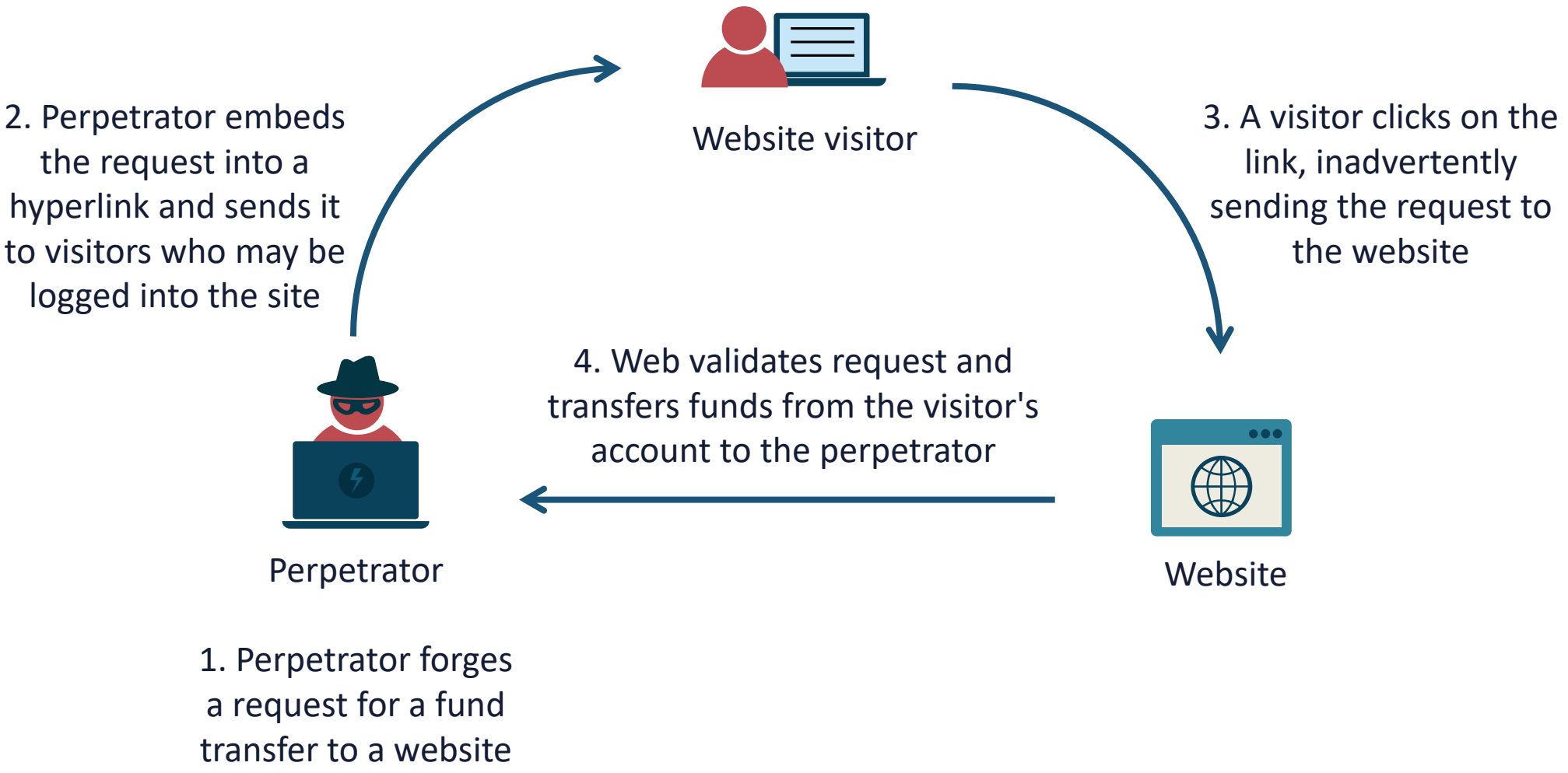
- **DOM-based** is also called local XSS or type 0
  - It does not involve vulnerable web servers but rather insecurely written HTML pages on the end user's system or local gadgets and widgets (Widgets – Apple, Nokia, Yahoo; Gadgets – Microsoft and Google
- **Reflected XSS** (Nonpersistent or Type 1)
  - This is a classic input trust vulnerability where the application is expecting some input (i.e., a query string), and the attacker sends something the developer did not expect
- **Stored XSS** (Persistent or Type 2)
  - This is a variant of type 1 where, rather than reflecting the input, the web server persists the input
  - The difference is an intermediate phase where the untrusted input is stored in a file or a database before unloading on the victim – often found in blogs and review/feedback web application



CROSS-SITE REQUEST FORGERY (CSRF/XSRF)

- Attacks force an end user to perform undesirable actions in a web application in which they are authenticated
- An effective CSRF/XSRF attack can force users to perform state-changing requests:
  - Transferring funds
  - Changing their email address
  - Changing their password
- If the victim is an administrative account, the CSRF attack can compromise the entire web application

CROSS-SITE REQUEST FORGERY (CSRF/XSRF)



HARDWARE VULNERABILITIES

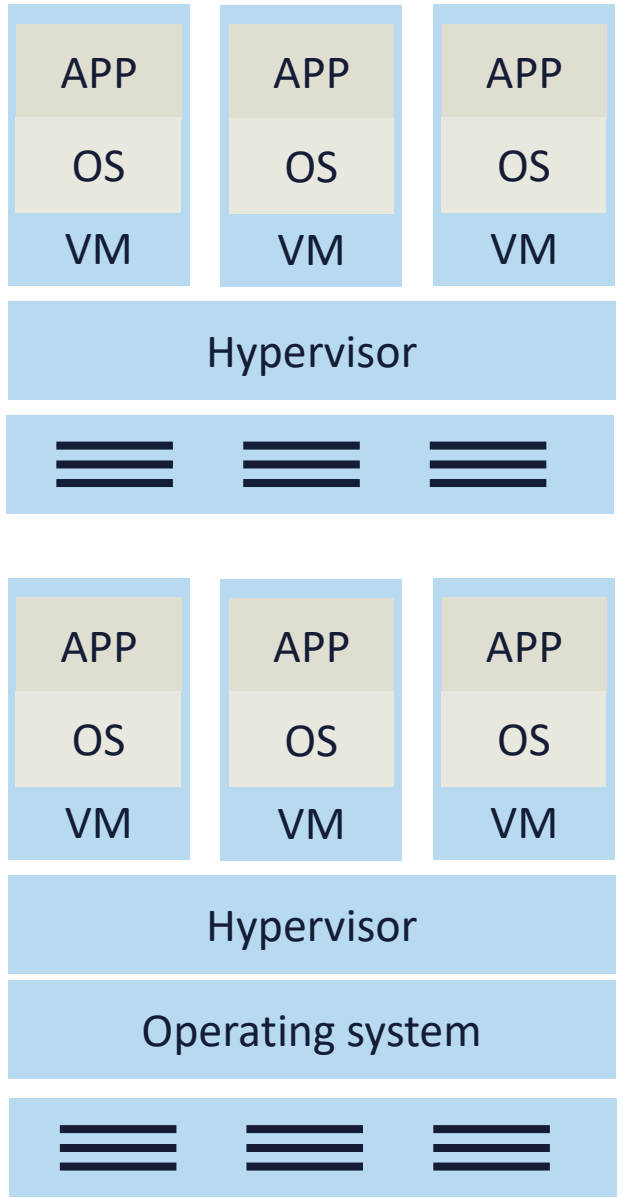
- Some of the dominant factors that contribute to vulnerabilities and flaws in hardware are
  - Vendors going out of business
  - Original equipment manufacturers (OEMs) cutting corners
  - Product becoming end-of-support and/or end-of-life with few or no alternatives
  - The usage of outdated and legacy systems
  - Unsecure and unsigned device drivers

FIRMWARE VULNERABILITIES

- Firmware is software that is embedded within hardware devices and provides low-level control and functionality
- Some firmware can be remotely reprogrammed and may be accessed by attackers through remote code execution (RCE)
- Common firmware exploits are authentication bypass, buffer overflows, and injection flaws
- The rapid emergence of the Internet of Things (IoT) and smart devices has introduced more security vulnerabilities

HYPERVISORS

- The virtual machine manager software system that runs and controls virtual machines
- It allocates and shifts resources as well as manages the interaction between the VMs and the hardware
- Type I – bare metal or native
  - Runs directly on the underlying hardware
  - XenServer, KVM, Hyper-V, ESXi
- Type II – hosted
  - Runs on the OS installed on the hardware
  - Oracle VirtualBox 6, VMWare Player/Workstation



HYPERVISOR VULNERABILITIES

- **VM sprawl** – involves having no centralized control of hypervisors and virtual machines
- **VM hopping** – when administrators do not enforce the partitioning of guests from each other
- **VM escape** – a flaw in the hypervisor that allows a guest to access the underlying hypervisor or even the hardware that it runs on
- **Hyperjacking** – a scenario where a privileged insider installs malware, such as a rootkit, on the hypervisor to conduct unauthorized activities

THE CLOUD SECURITY ALLIANCE (CSA) TREACHEROUS 12

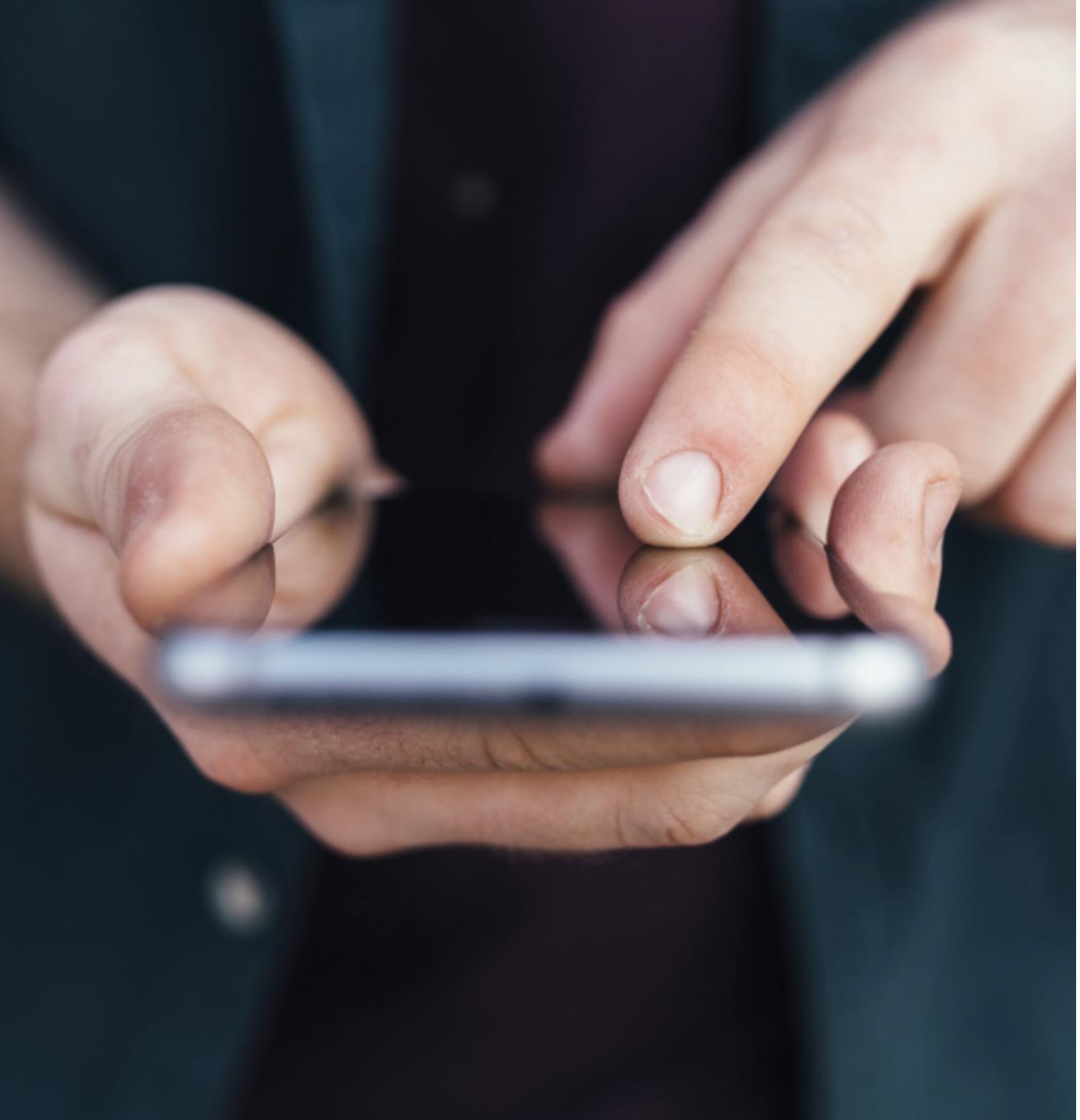
- *The Treacherous 12 – Cloud Computing Top Threats* report plays a vital role in the CSA research ecosystem
- The goal of the report is to offer organizations an up-to-date, expert-informed understanding of cloud security issues so that educated risk management decisions can be made concerning cloud adoption strategies
- The report reflects the current consensus among security experts in the CSA community about the most significant security issues in the cloud

THE CSA TREACHEROUS 12

1. Data breaches
2. Weak identity, credential, and access management
3. Insecure APIs
4. System and application vulnerabilities
5. Account hijacking
6. Malicious insiders
7. Advanced persistent threats (APTs)
8. Data loss
9. Insufficient due diligence
10. Abuse and nefarious use of cloud services
11. Denial of service
12. Shared technology vulnerabilities

MOBILE DEVICE VULNERABILITIES

- There are several classic vulnerabilities with mobile devices – most of which have been addressed with vendor updates
- **Side loading**, in the context of smartphones, involves installing a compatible app for an Android or iOS device that is not available, approved, or at least monitored and maintained by your device platform's official app store



MOBILE DEVICE VULNERABILITIES

- **Jailbreaking** is the act of exploiting the flaws of a locked-down electronic device (iPhone) to install software other than what the manufacturer has made available for that device
  - It allows the device owner to gain full access to the root of the operating system and access all the features
- Rooting is the process of unlocking usually an Android smartphone or tablet
  - A rooted device gives the user much more freedom to customize the device and achieve more administrative control

ENTERPRISE MOBILITY MANAGEMENT (EMM)

- Organizations should employ the most robust authentication mechanisms feasible (biometrics, QR codes, trusted platform modules)
- This is accomplished through enterprise mobility management initiatives:
  - Mobile device management (MDM)
  - Mobile application management (MAM)

SURVEY OF MALICIOUS ACTIVITIES

Objectives

- Examine malware and physical attacks
- Explore network and application attacks
- Learn about cryptographic and password attacks
- Look at Indicators of Compromise (IoC)

MALWARE ATTACKS

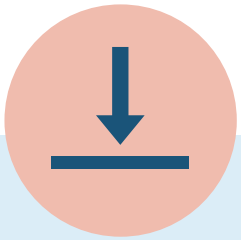
- A malware attack is a common cyberattack where malware (typically malicious software) executes unauthorized actions on the victim's system
- The malicious software (AKA virus or worm) encompasses many different types of attacks such as ransomware, spyware, command and control, and more
- Like other types of cyber attacks, some malware attacks end up with mainstream news coverage due to their severity
- An example of famous malware is the WannaCry ransomware attack

All security incidents can be considered an exploit, but not all exploits involve the usage or delivery of a malicious software (malware) payload

RANSOMWARE

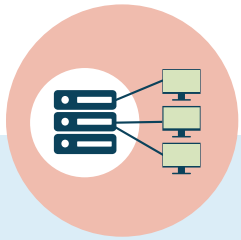
- This is a popular form of malware that encrypts key files and holds them for "ransom"
- Usually committed for cryptocurrencies such as Bitcoin (over 90%) or Monero
- Ransomware evolved from misleading "fix" apps to fake AV tools and bogus "fine" websites
- The average ransom demand has more than doubled since 2020
- Over 30% of victims are in the U.S.
- The newest trend is Ransomware as a Service (RaaS) on the dark net, which is a subset of Malware as a Service (MaaS)

RANSOMWARE CAMPAIGN



1. Installation

Crypto-ransomware installs itself after boot up



2. Contacting headquarters

Malware contacts a server belonging to an attacker or group

3. Handshake and keys

The ransomware client and server "handshake" and the server generates two cryptographic keys

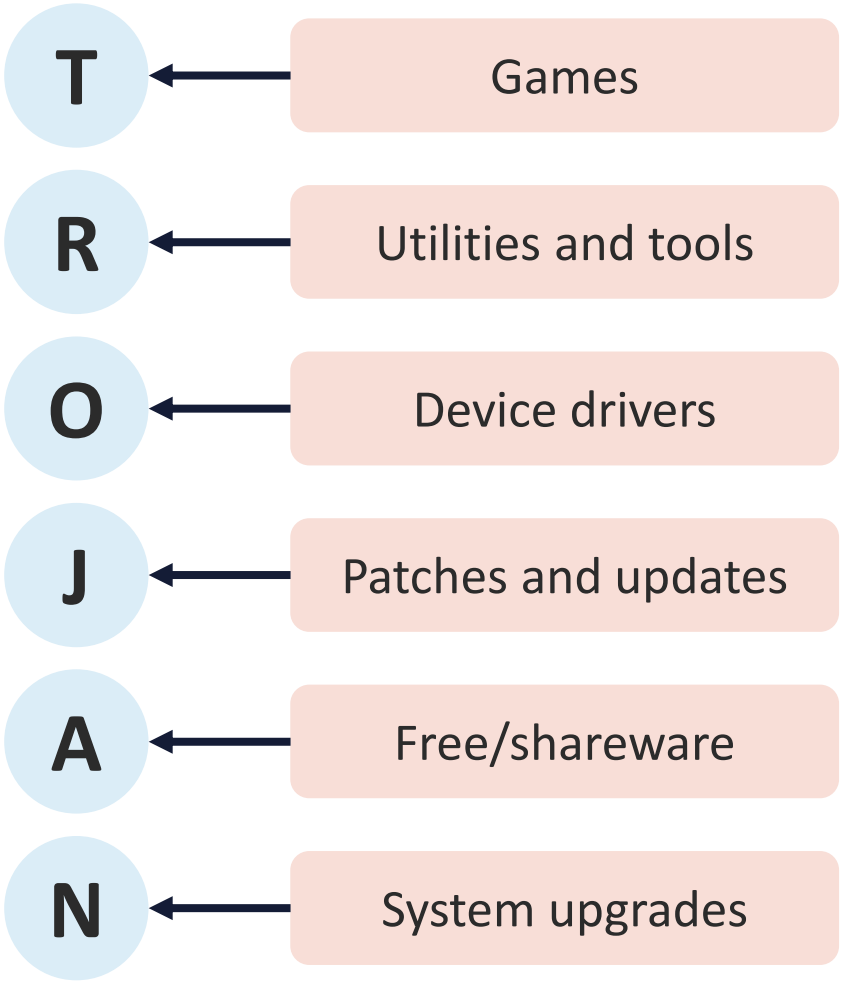
4. Encryption

The ransomware starts encrypting every file it finds with common file extensions

5. Extortion

A screen displays, giving a time limit to pay up before the criminals destroy the key the decrypt the files

TROJANS

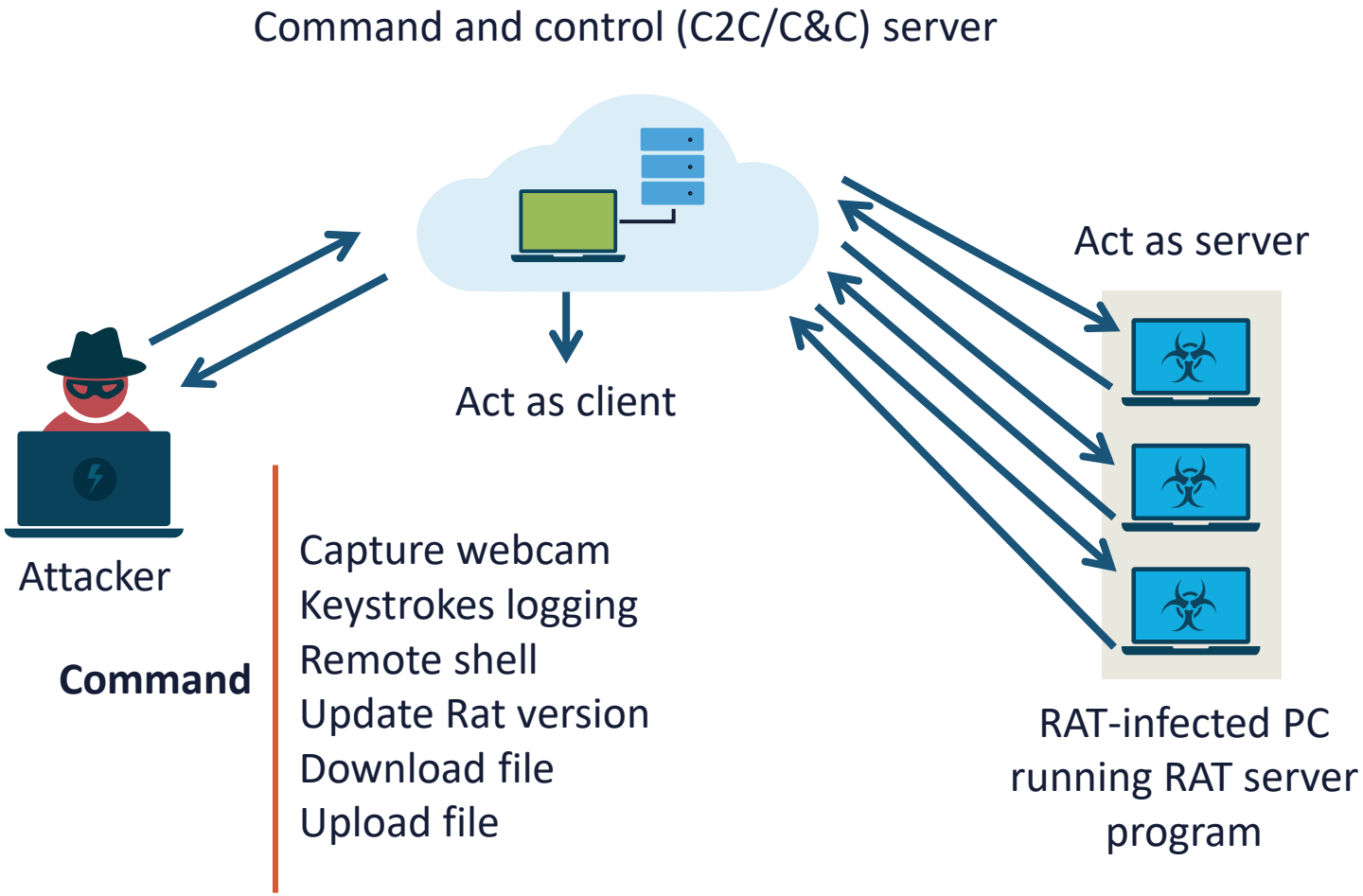


- Trojans are malicious code and programs that masquerade as legitimate applications or are embedded in real programs
- Trojan horses have no replicating abilities like viruses or worms
- They can either be a re-named benign program or the trojan code can exist in an operable application
- Trojans can also be part of a more elaborate distributed denial-of-service or botnet attack

REMOTE ACCESS TROJANS (RATS)

- Remote access trojans (RATs) are a variant of trojan malware engineered to permit an attacker to remotely control an infected computer
- Once the RAT is running on a compromised system, the attacker can send commands to it and receive data back in response
- The server can be a command and control server that is part of an automated botnet

REMOTE ACCESS TROJANS



VIRUSES

A computer virus is a type of malware that spreads between computers and causes damage to data and software

Viruses are distinctive in that they typically attach to executable files to disrupt systems, cause major operational issues, and result in data loss and leakage

The code then spreads from the document or software it is attached to via networks, drives, file-sharing programs, or infected email attachments

WORMS

Worms are a special form of self-replicating virus (malware) that generally spreads without user action

They distribute complete copies (possibly modified) of themselves across networks

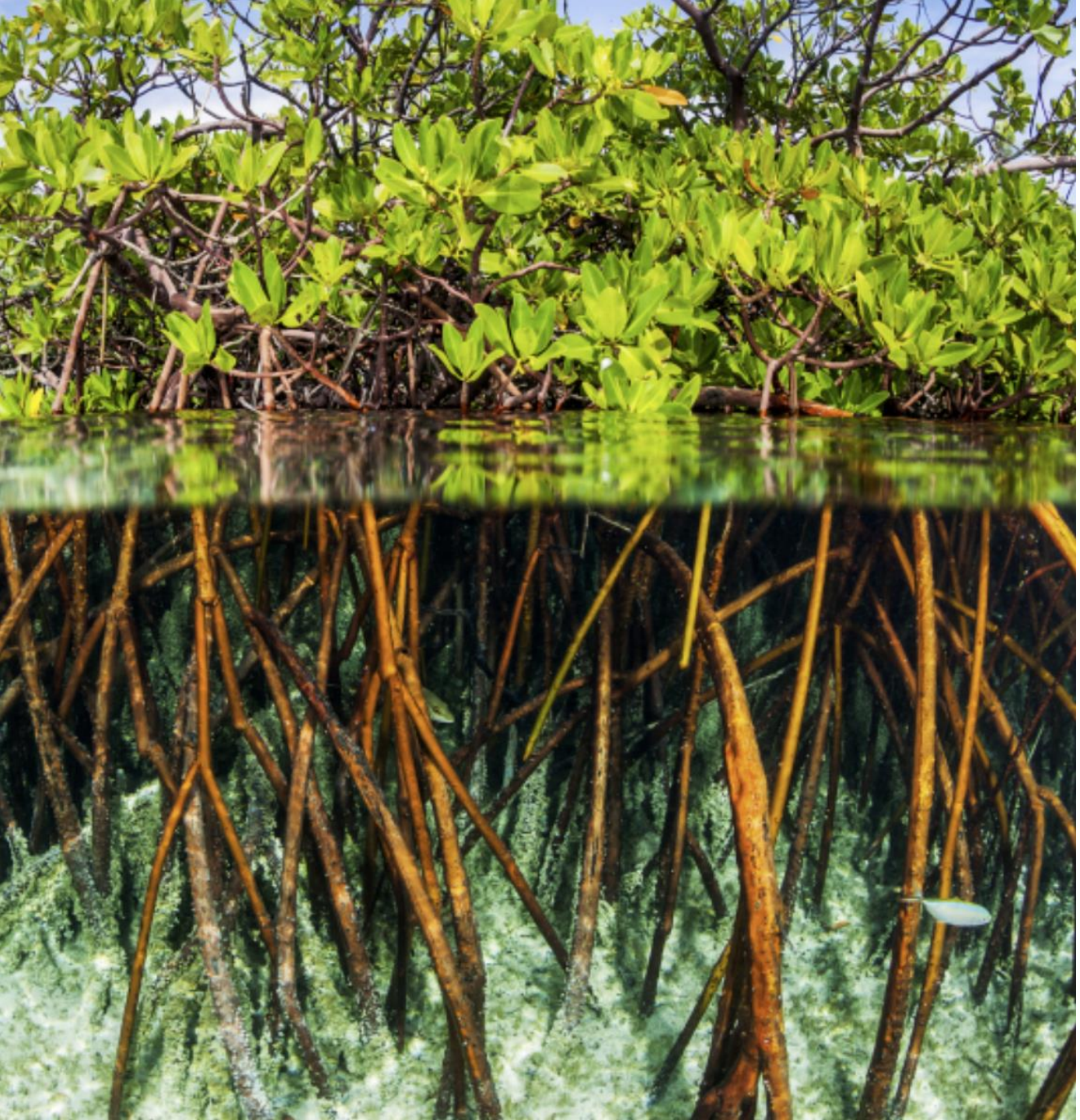
A worm can consume resources, infiltrate data, or simply cause the CPU on the system to waste cycles, resulting in a computer becoming unresponsive

SPYWARE AND BLOATWARE

- **Spyware** is often defined as malware intended to penetrate a device, collect personal data, and then send it to a third party without permission
- Spyware can also refer to legitimate software that monitors data for commercial purposes like advertising
- Technically speaking, practically all smart devices and IoT components are spyware
- **Bloatware** is unwanted and potentially harmful software preloaded onto new devices
- It is preinstalled by vendors, manufacturers, or carriers as a form of marketing to put services directly in front of customers

KEYLOGGERS

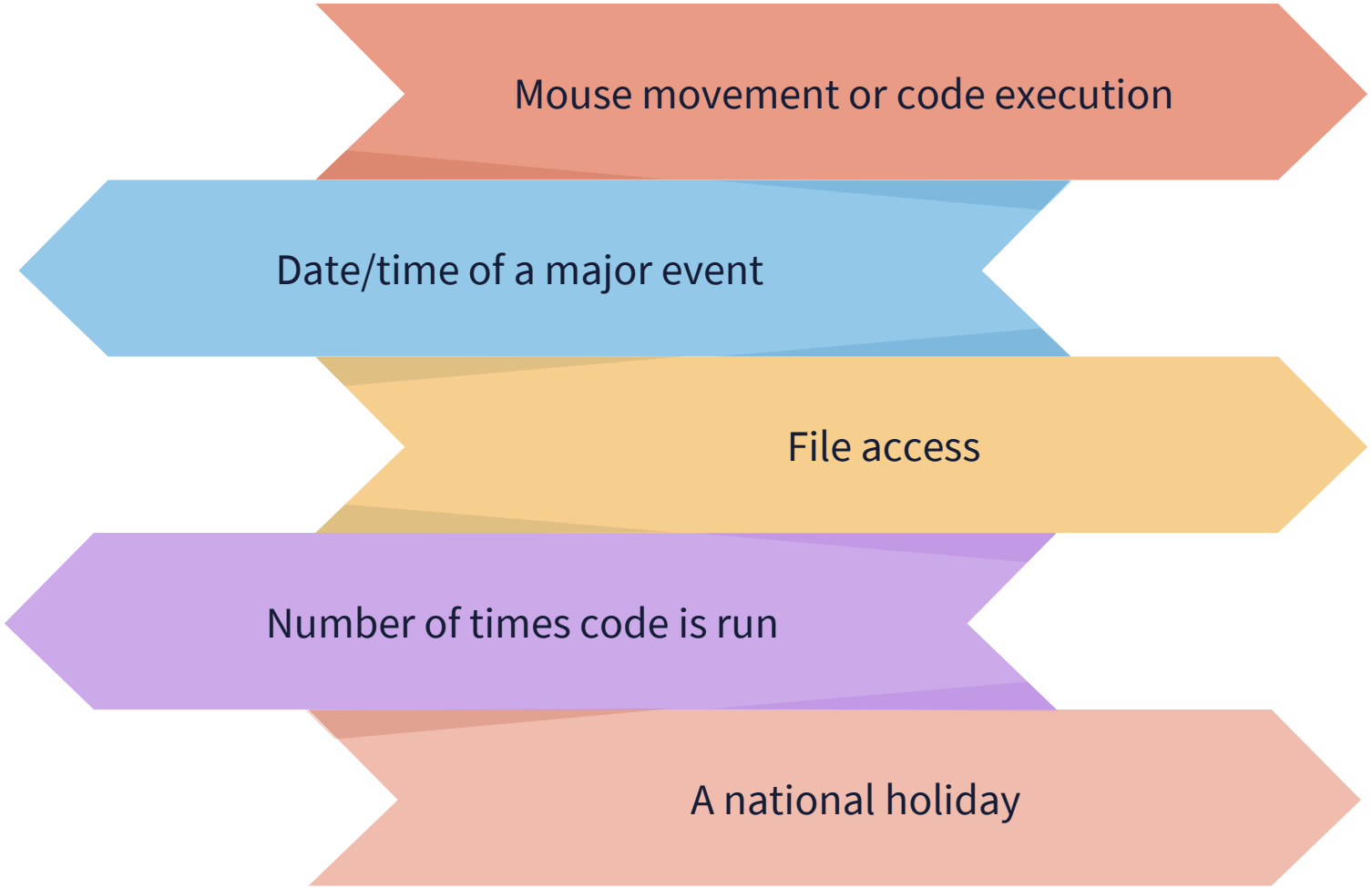
- Keystroke logging is typically done by malicious code that records keystrokes and sends data back to command and control servers
- Spyware uses keyloggers to capture passwords, credit card information, or other personally identifiable information (PII)
- Software can also be used to track employees or family members to adhere to acceptable use
- Keylogger detectors are special mitigation tools
- Examples: PAL KeyLogger Pro and KeyGhost



ROOTKITS

- Rootkits are a type of malware that can give a threat actor control of systems user consent or knowledge
- "Root," "admin," "superuser," or "system admin" are all interchangeable terms
- They are dangerous because they are designed to hide their presence
- A threat actor who has placed a rootkit onto a machine (often via phishing email) can remotely access and control it to deactivate the antivirus software, spy on activities, steal sensitive data, or execute other malware

LOGIC BOMBS ARE TRIGGERED BY EVENTS



PHYSICAL ATTACKS

- Safes and other containers are rated based on the amount of time a tool would take to penetrate with brute force
- Doors and windows of all types are also common targets of brute force attacks
- Although considered a preventative mechanism, locks are a delay component since all could be overcome by brute force

RFID CLONING

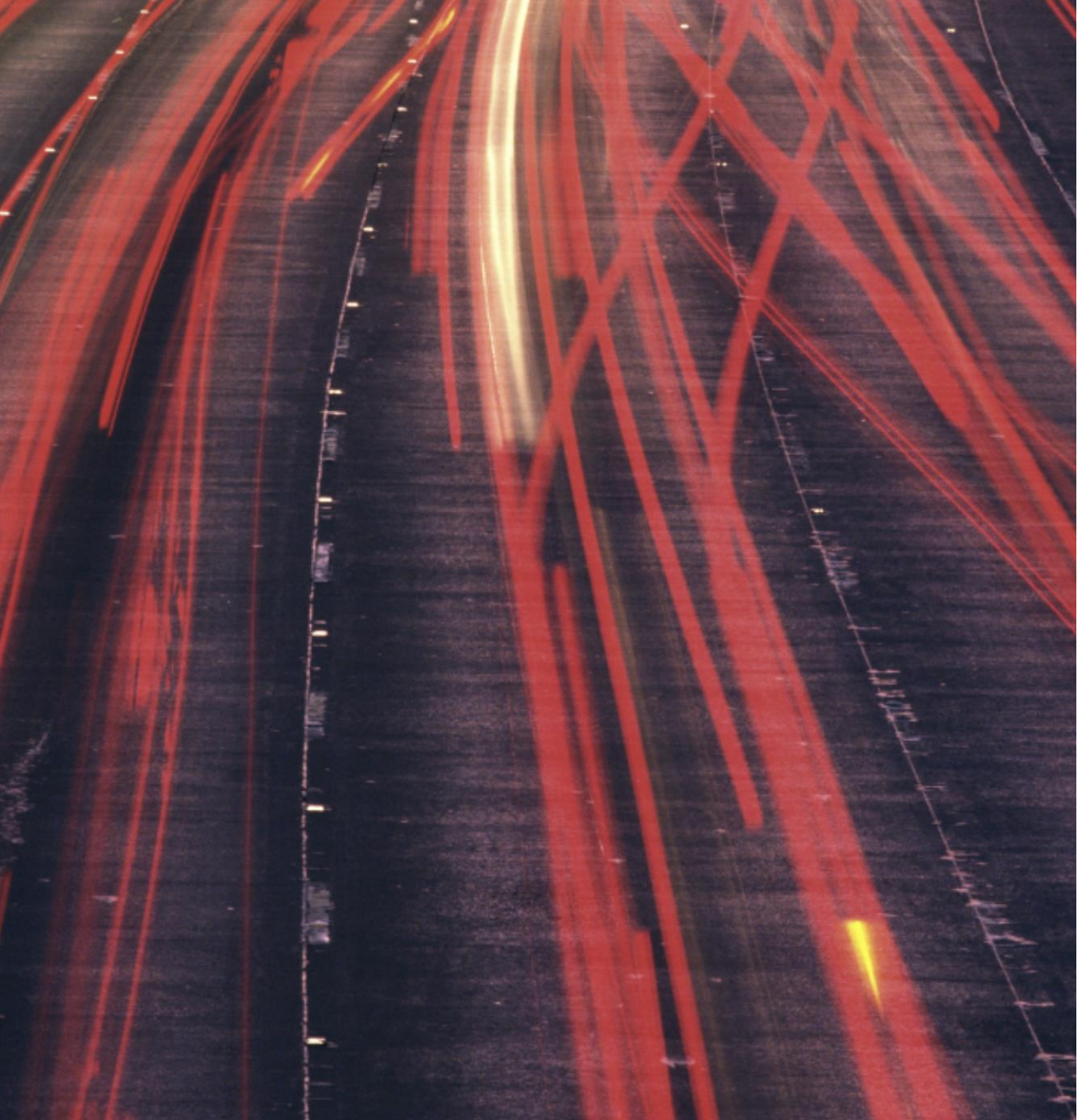
- RFID and NFC devices are vulnerable to a variety of physical attacks
- Crackers can clone credit and debit cards by stealing the name, account number, expiration date, and 3-digit code
- Data stored on RFID chips can be stolen, skimmed, and scanned by anyone with easily obtained RFID readers
- Skimming uses devices that overlay an ATM or point-of-sale scanner to steal the information from the victim

ENVIRONMENTAL ATTACKS

- Any environmental system that is not air-gapped can be compromised
- Many systems and sensors are "smart" or remotely accessible with IP
- They can be hacked to shut down systems, overload them, and hijack to change temperature or humidity
- If the environmental system connects to other networks, they can represent potential backdoors
- There should be a zero trust policy and high visibility when considering these critical systems

DENIAL-OF-SERVICE ATTACKS (DOS)

- A DoS attack happens when a malicious cyber threat actor prevents legitimate subjects from accessing information systems, infrastructure devices, or other network resources
- Affected services include email/webmail, websites, personal cloud storage, online accounts (e.g., banking), or other services that depend on a server or network
- A denial-of-service condition is accomplished by flooding the targeted host or network with traffic (i.e., ICMP, TCP, UDP) until the target cannot respond or simply crashes, preventing access for legitimate users

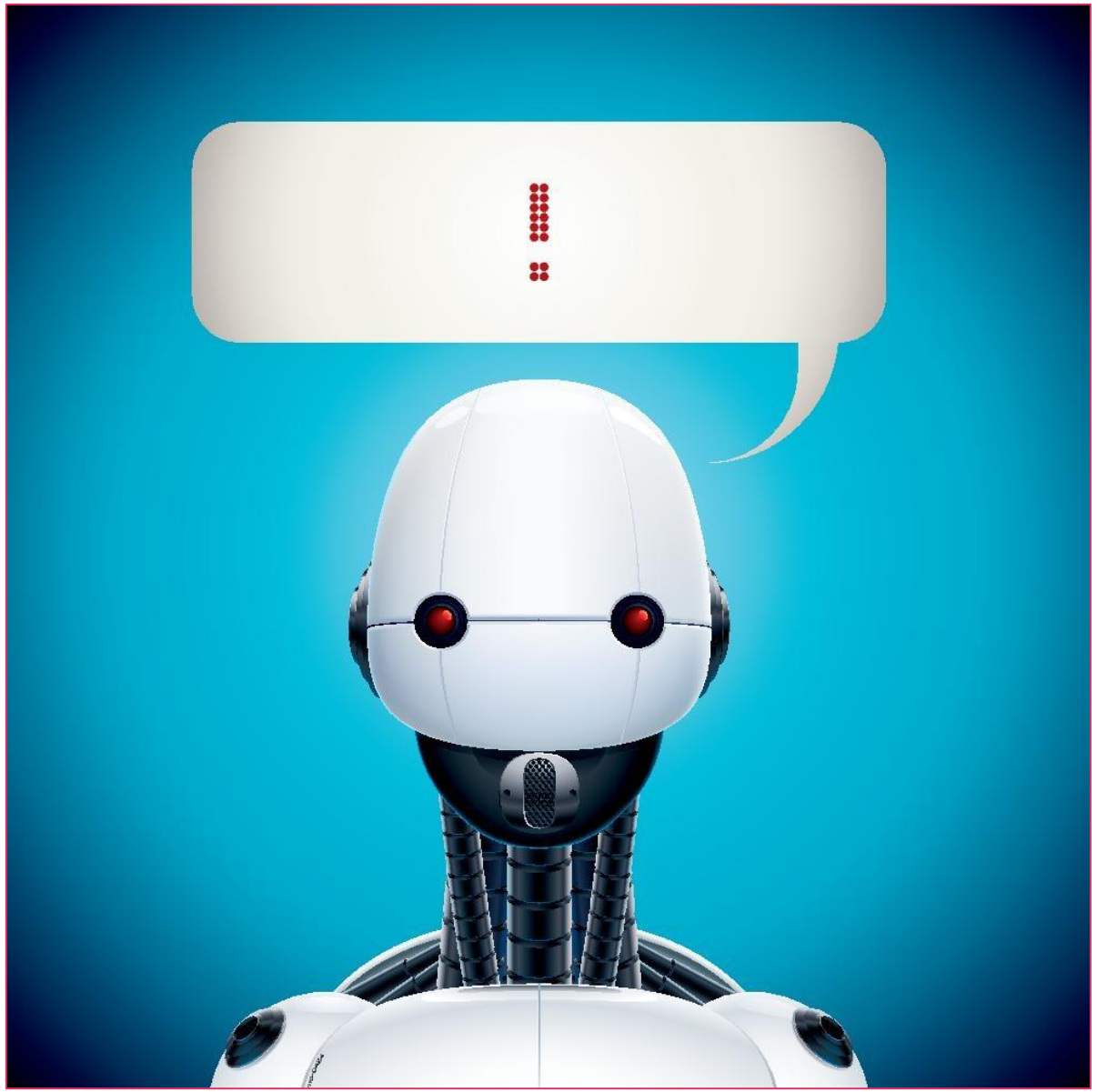


DISTRIBUTED DENIAL-OF-SERVICE (DDOS)

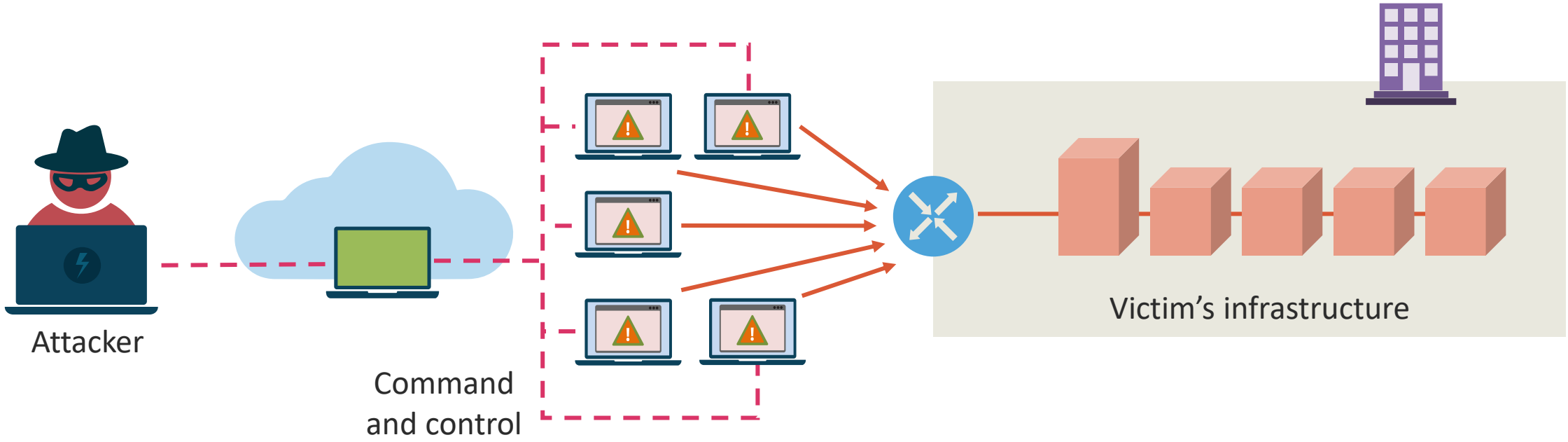
- DDoS floods a server with Internet traffic to prevent users from accessing connected online services and sites
- Some attacks are launched by hacktivists overloading an organization’s servers to make a statement or express displeasure
- Other DDoS attacks are financially motivated by competitors or involve extortion, in which perpetrators attack a company and install ransomware on their servers
- The most common form of DDoS attack is robot networks (botnets)

BOTNETS

- The most common form of DDoS attack today
- The robot network (botnet) consists of a zombie computer and a master command and control server to remotely control victims, and many victims are unaware
- The communication often occurs over Internet Relay Chat (IRC), encrypted channels, bot-centric peer-to-peer networks, and even social media
- Bots can exfil data, log keystrokes, scan memory, force a system to participate in mining cyber currency, and more



DDOS BOTNETS



DNS ATTACKS

DoS and DDoS

Attacker targets the root or down-level DNS servers to overwhelm the systems with a large amount of UDP queries

Cache poisoning

Attacker attempts to modify the DNS cache in the wrong way so that all DNS requests return an incorrect response

DNS hijacking

Similar to poisoning, the attacker often sets up a cloned site to redirect hijacked users to steal data or deliver malware

DNS spoofing

An attacker will represent a domain name and IP mapping to trick users or poison caches

DNS ATTACKS

NXDOMAIN attack

Attempts to make servers disappear from the Internet by flooding the DNS server with requests for invalid or nonexistent records

DNS flooding

This is considered a variant of the UDP flood attack, since DNS servers rely on the UDP protocol for name resolution

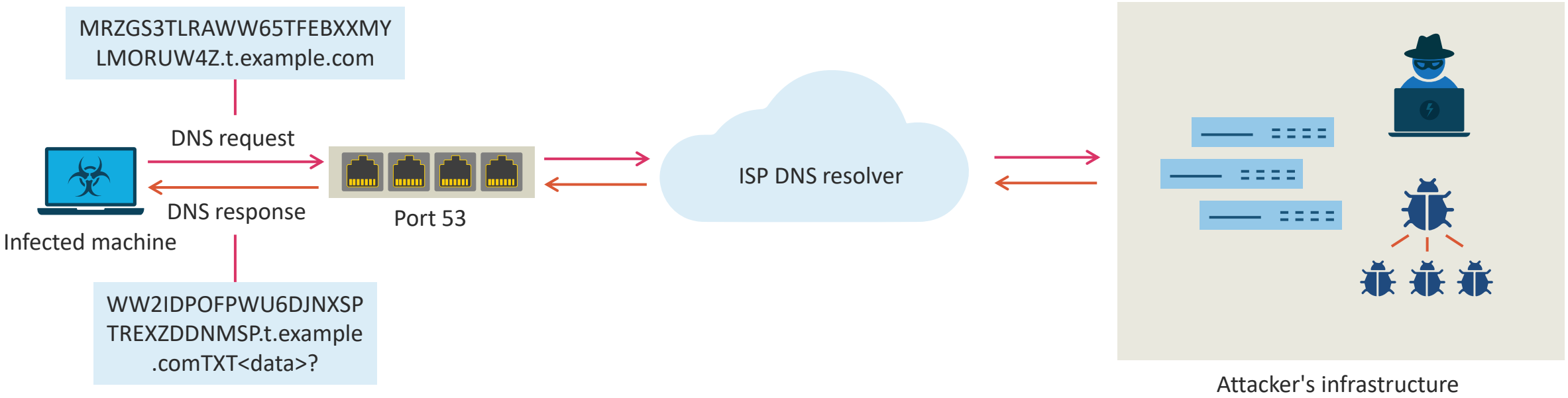
Amplification attack

A reflection-based DDoS attack in which an attacker leverages the functionality of open DNS resolvers to overwhelm a target server or network with an amplified amount of traffic

DNS tunneling

Exploits the DNS protocol to tunnel malware and other data by registering a domain server that points to the attacker's server, where a tunneling malware program is installed

DNS TUNNELING



WIRELESS ATTACKS

- Rogue access points and evil twins spoof real wireless LAN devices
- DHCP starvation uses up real leases so that a rogue server can be introduced
- Attacks target management and control frames (disassociation or de-authentication) used for roaming devices
- On-path attacks used to be called man-in-the-middle, where rogue devices inject into TCP connections and other communications
- Jamming is a form of denial-of-service attack towards access points (APs) and wireless controllers

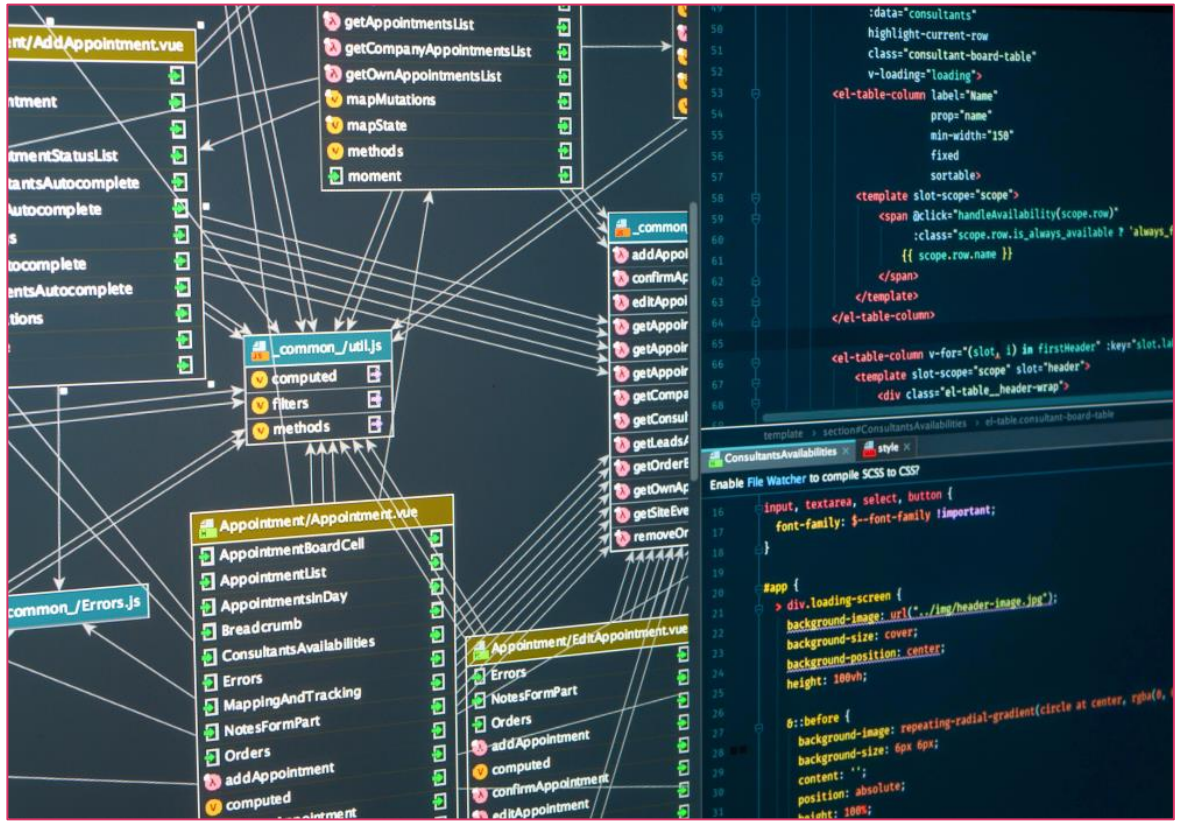
CREDENTIAL REPLAY

- A credential replay attack involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of generating an unauthorized effect or gaining unauthorized access
- Attackers will also perform other reconnaissance attacks, dumpster diving, and various social engineering to harvest the internal usernames of an organization

SQL INJECTION (SQLI)

Involves inserting a SQL query through input data from client to server application and can allow for several exploits

- Read sensitive database data (SELECT FROM)
- Change database data (INSERT, UPDATE, DELETE)
- Execute administrative functions (e.g., shutdown DBMS)
- Get the contents of files on database a management system (DBMS)
- Run commands on the operating system



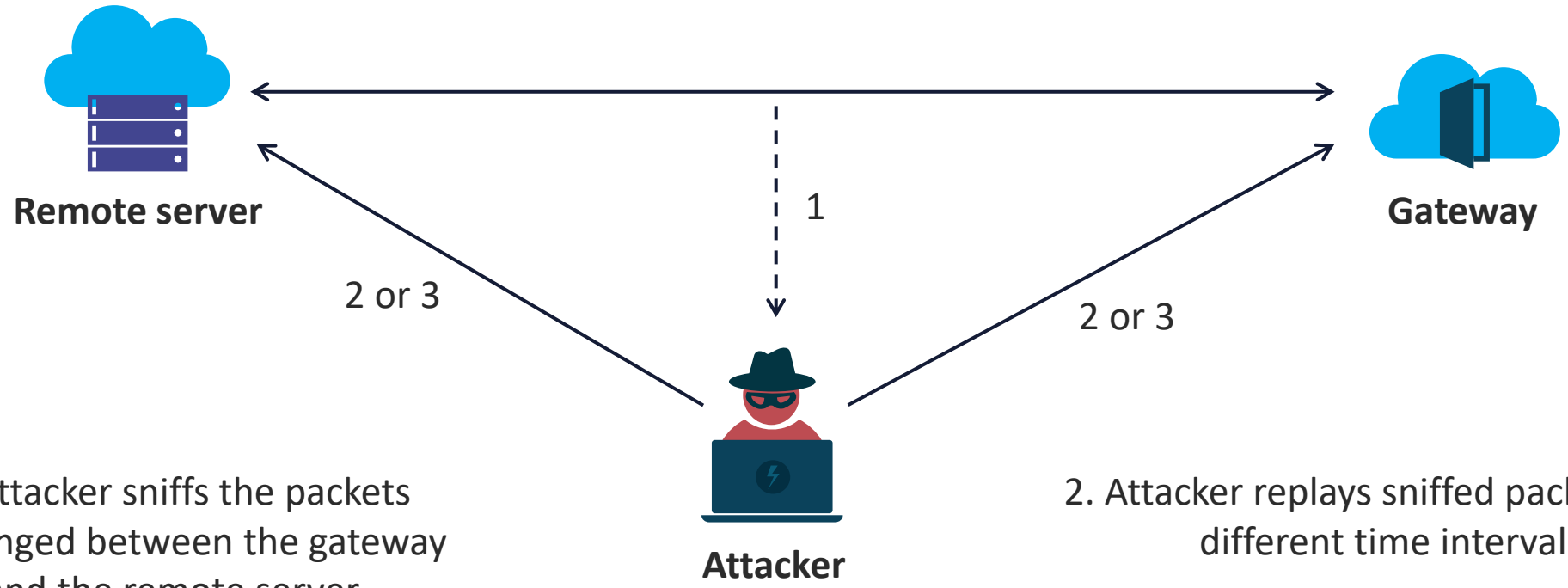
BUFFER OVERFLOWS

- The buffer overflow attacker manipulates coding errors to compromise affected applications running on critical servers
- It changes the program's execution path and overwrites elements of its memory, which amends the program's execution path to damage existing files or expose data
- It usually involves violating programming languages and overwriting the bounds of the buffers they exist on when code
  - Is reliant on external data to control its behavior
  - Is dependent on data properties that are enforced beyond its immediate scope
  - Is so complex that programmers are not able to predict its behavior accurately

REPLAY ATTACKS

- A replay attack happens when an attacker snoops on a secure network communication, intercepts it, and then deceptively delays or resends it to misdirect the receiver into doing what the cracker wants
- The added challenge of replay attacks is that a script kiddie does not need advanced skills to decrypt a message after capturing it from the network
- The attack could be successful simply by resending the entire communication

REPLAY ATTACK



1. Attacker sniffs the packets exchanged between the gateway and the remote server

2. Attacker replays sniffed packets at a different time interval

3. Attacker modifies and sends sniffed packets or forges new packets

PRIVILEGE ESCALATION

- Attackers exploit human misconfiguration, design flaws, or omissions in web applications
- This is closely related to lateral movement — tactics by which an attacker moves deeper into a network looking for sensitive assets
  - The result is an internal or external user with unauthorized system privileges
- Depending on the extent of the attack, bad actors can do minor or major damage
- It might be a simple unauthorized email or a ransomware attack on vast amounts of data

FORGERY AND DIRECTORY TRAVERSAL ATTACKS

Cross-site request forgery (CSRF) is an attack that tricks authenticated users into inputting a request to a web application

CSRF attacks exploit the trust a web application has in an authenticated user

It exploits a vulnerability in a web application if it cannot differentiate between a request generated by an end user and a request generated by a user without their consent

Directory (or path) traversal (or climbing) is a type of HTTP exploit where the attacker leverages the web server software to access data in a directory other than the server's root directory

The threat agent, usually a browser, can view restricted files or execute commands on the server

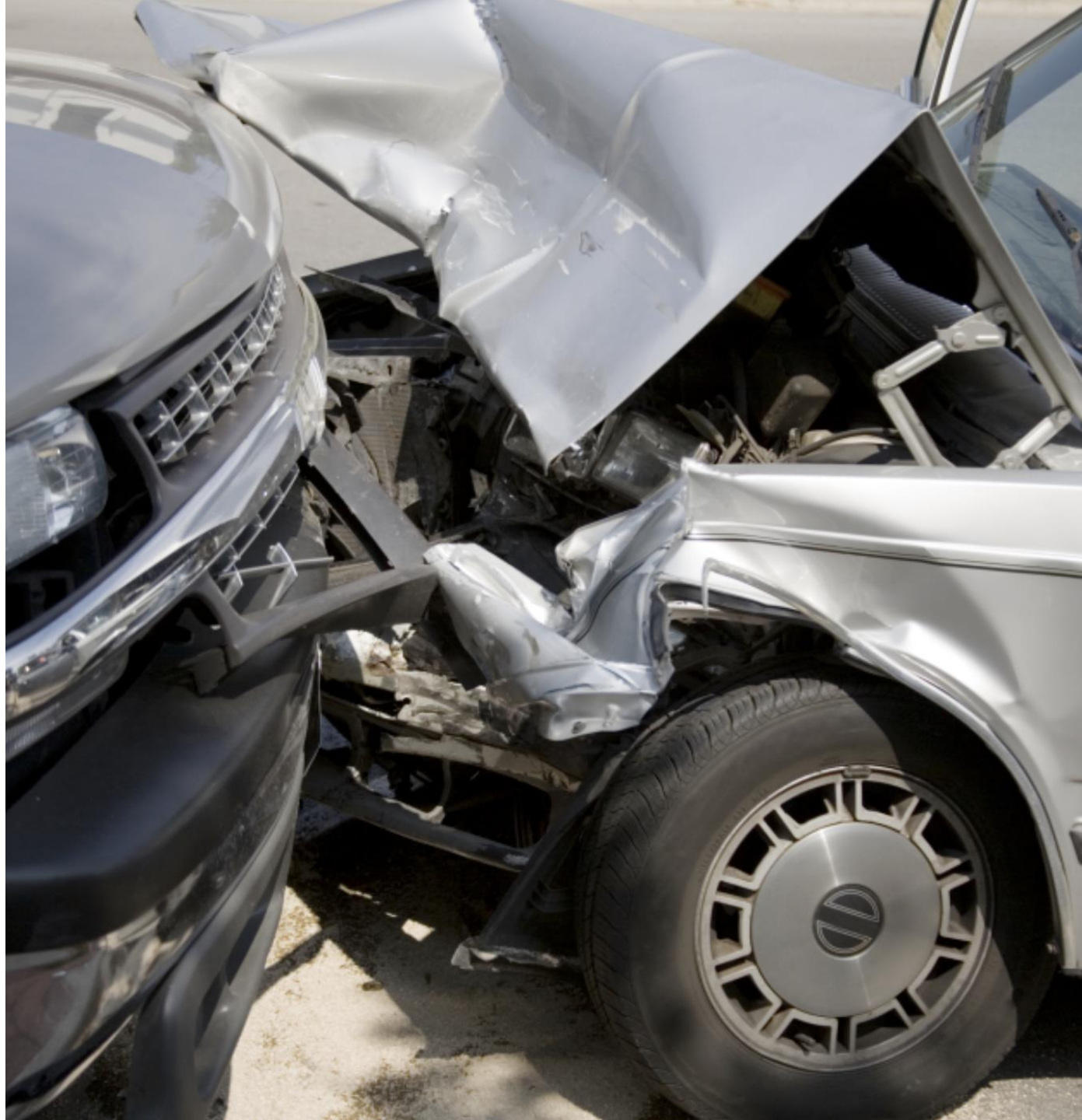
Any server that fails to validate input data from web browsers is vulnerable to a directory traversal attack

CRYPTOGRAPHIC DOWNGRADE ATTACK

- In a downgrade attack, the attacker attempts to force two hosts on a network (typically a browser and web server) to use an insecure or weakly protected data transmission protocol
- The downgrade is often HTTP instead of HTTPS or SSL instead of TLS
- If a downgrade attack is successful, the attacker can exploit connection vulnerabilities to intercept and read transmitted data
- It is considered a type of on-path

COLLISION ATTACKS

- To be considered trustworthy, a cryptographic hashing mechanism must be "collision-resistant"
- This means that two different inputs should never produce the same fingerprint or digest
- This collision can then be exploited by any application that compares two hashes together, such as password hashes, file integrity checks, and others
- MD5 is no longer considered collision-resistant



CRYPTOGRAPHIC BRUTE FORCE ATTACKS

- A brute force attack, also known as an exhaustive search, is a cryptographic hack that depends on guessing all possible combinations of a targeted password until discovered
  - If the password is weak, it could take mere seconds with hardly any effort
- A brute force attack is time and processor-intensive and may be impossible or absurd from a physics standpoint
- It can also relate to trying all possibilities in a cryptosystem keyspace, which is why the larger bit size or modulus is preferred

SIDE CHANNEL ATTACKS

- A side channel attack is enabled by leakage of information from a physical cryptosystem such as a smart card or cryptoprocessor
- Attributes that can be exploited in a side-channel attack, including timing, power consumption, and electromagnetic and acoustic emissions
- Wireless WPA3 had an early side-channel vulnerability in its Dragonfly protocol

EXPLORING PASSWORD ATTACKS

In this demo…

You will explore password attacks and tools

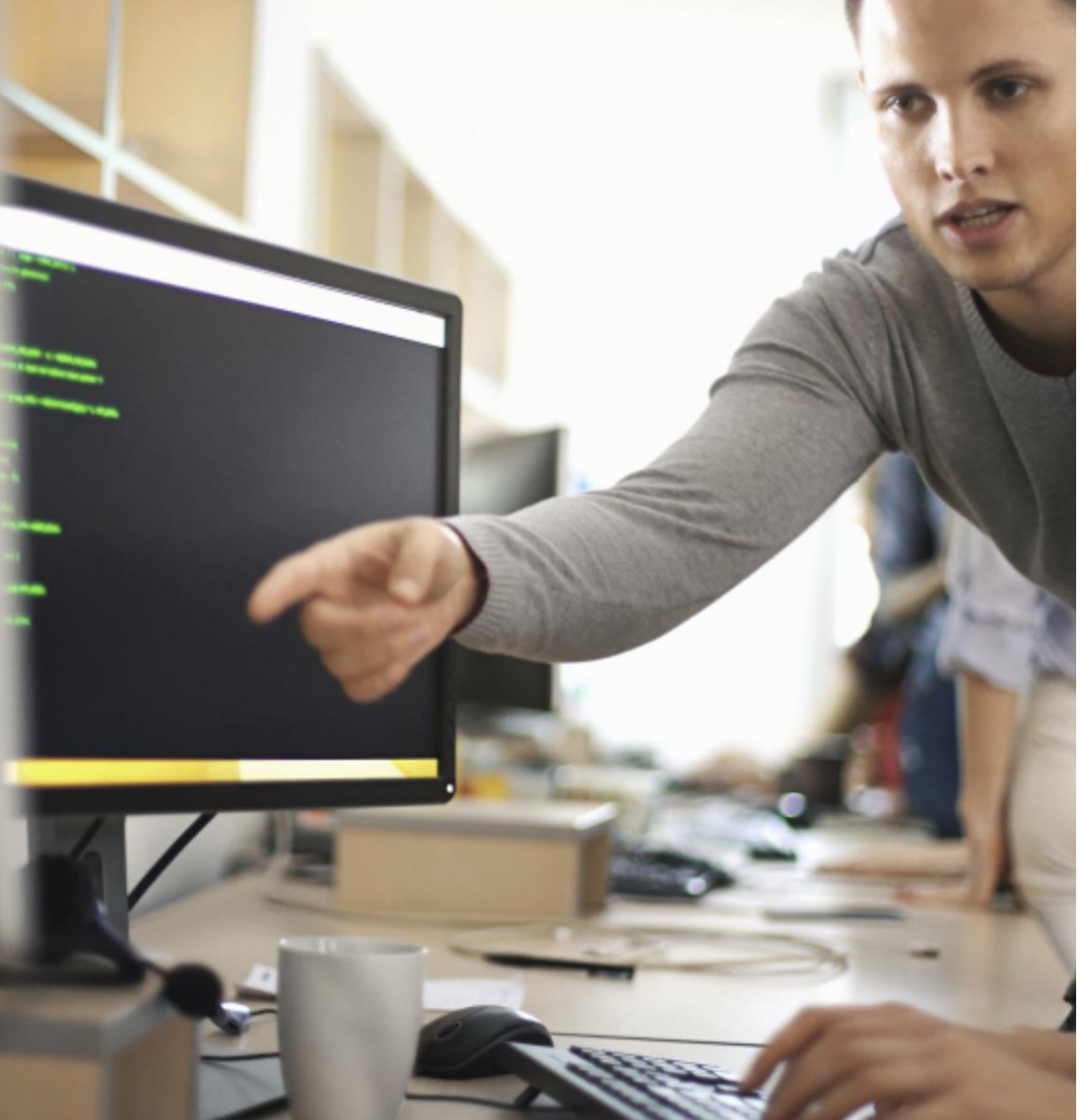
INDICATORS OF COMPROMISE (IOCS)

These are network or host-based cyber observables

Forensic artifacts of an incursion or disturbance

A measurable event or stateful property in the cyber domain

Registry entries, files on disk and in-memory, etc.



INDICATORS OF COMPROMISE

- Account lockout
- Concurrent session usage
- Blocked content
- Impossible travel
- Resource consumption
- Out-of-cycle logging
- Missing logs