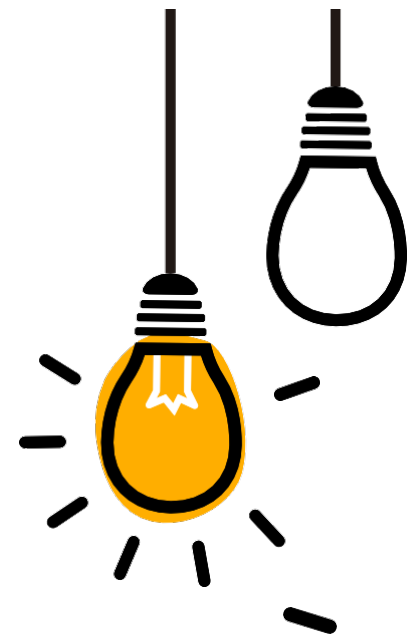
Top 100
Cyber Threats
Introduction & Solution

01

Credential Phishing

Credential phishing is a type of cyber attack where attackers masquerade as legitimate entities to trick individuals into divulging sensitive information such as usernames, passwords, or financial data.



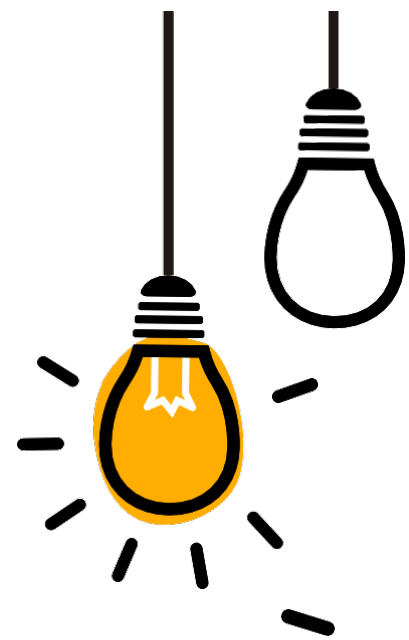
Solution:

- Implement email filtering and anti-phishing technologies to detect and block phishing emails before they reach users' inboxes, reducing the likelihood of successful credential theft.
- Enable multi-factor authentication (MFA) for accessing sensitive accounts or systems to add an extra layer of security and mitigate the risk of unauthorized access even if credentials are compromised.

02

DNS Tunneling

DNS tunneling is a technique used by attackers to bypass network security controls by encapsulating data within DNS queries and responses, allowing them to exfiltrate data or communicate with command-and-control servers covertly.



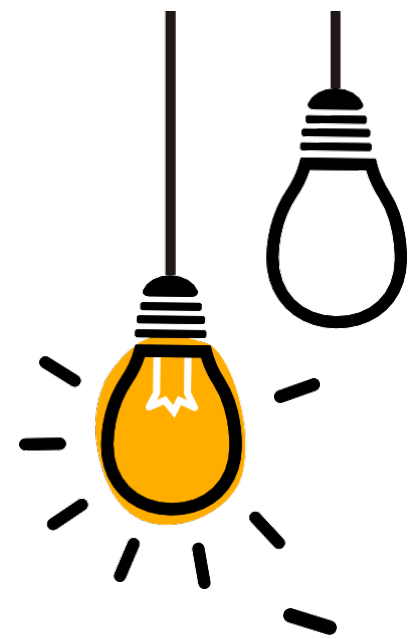
Solution:

- Monitor DNS traffic for anomalies, such as unusually high query rates, long domain names, or unexpected data payloads, which may indicate DNS tunneling activity.
- Implement DNS security solutions, such as DNS firewalls, DNS sinkholing, or threat intelligence feeds, to detect and block malicious DNS traffic associated with tunneling techniques used by attackers.

03

Cross-Site Request Forgery (CSRF)

Cross-Site Request Forgery (CSRF) attacks exploit the trust relationship between a user's browser and a web application to execute unauthorized actions on behalf of the user without their consent.



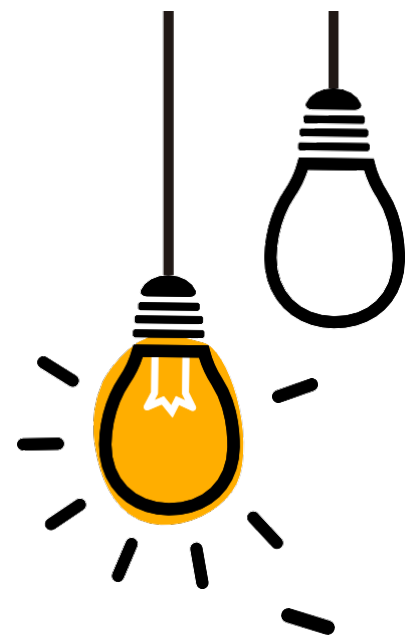
Solution:

- Implement anti-CSRF tokens, within web applications to validate the authenticity of incoming requests and prevent CSRF attacks by verifying that each request originated from a legitimate source.
- SOP and CORS headers to restrict cross-origin requests and prevent malicious websites from accessing sensitive data or invoking actions on behalf of authenticated users.

04

Data Manipulation Attacks

Data manipulation attacks involve unauthorized alterations or modifications to data stored in databases, files, or application repositories, compromising data integrity and reliability.



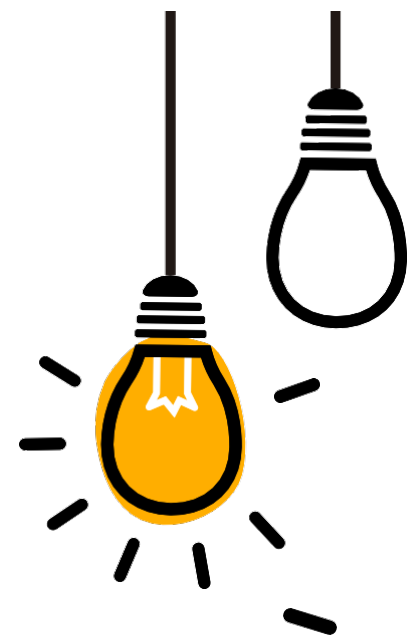
Solution:

- Implement data integrity checks, cryptographic hashing, or digital signatures to verify the integrity and authenticity of data at rest and in transit, protecting against unauthorized modifications or tampering attempts.
- Enforce access controls, role-based permissions, and audit trails to track changes to sensitive data, ensuring traceability of data manipulation activities by authorized users.

05

IoT Firmware Vulnerabilities

IoT firmware vulnerabilities refer to security flaws or weaknesses present in the firmware of Internet of Things (IoT) devices, which can be exploited by attackers to compromise device security or privacy.



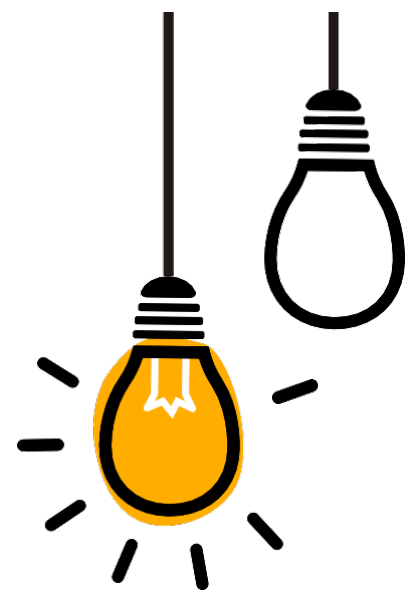
Solution:

- Implement secure firmware development practices, including code reviews, static analysis, and vulnerability assessments, to identify and remediate security flaws in IoT device firmware before deployment.
- Establish secure boot mechanisms, firmware signing, and over-the-air (OTA) update capabilities to ensure the authenticity, integrity, and timely deployment of firmware updates.

06

Side Channel Attacks

Side channel attacks exploit unintended information leakage from physical or implementation characteristics of computing systems to extract sensitive information or cryptographic keys.



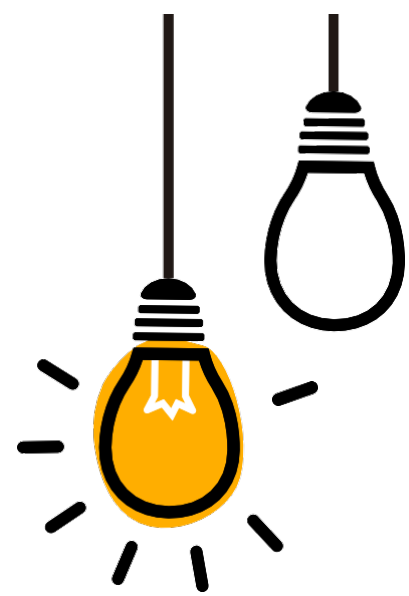
Solution:

- Implement countermeasures such as constant-time algorithms, algorithmic masking, or cryptographic blinding to mitigate side channel vulnerabilities and prevent attackers from exploiting timing, power, or electromagnetic side channels to extract sensitive data.
- Employ hardware-based security mechanisms, such as TEEs, HSMs, or secure enclaves, to isolate sensitive computations and cryptographic operations from side channel attacks.

07

SIM Swapping

SIM swapping, also known as SIM hijacking, is a social engineering technique used by attackers to fraudulently transfer a victim's phone number to a SIM card under the attacker's control, allowing them to intercept calls, SMS messages, or two-factor authentication (2FA) codes.



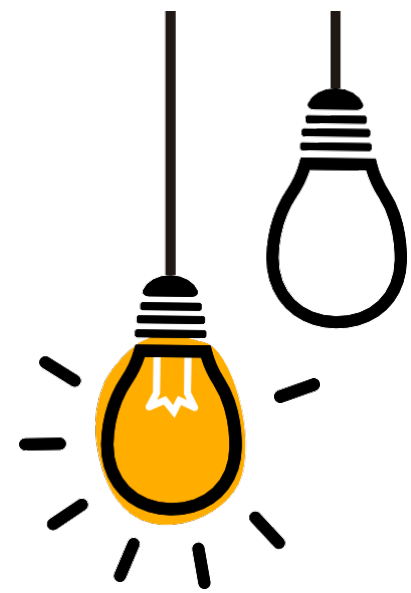
Solution:

- Enable additional layers of authentication, such as biometric verification, security questions, or PIN codes, to validate SIM card swaps and prevent unauthorized changes to user accounts or phone numbers.

08

Ransomware

Ransomware is a type of malware that encrypts files or locks users out of their systems, demanding payment (usually in cryptocurrency) for decryption or restoration of access.



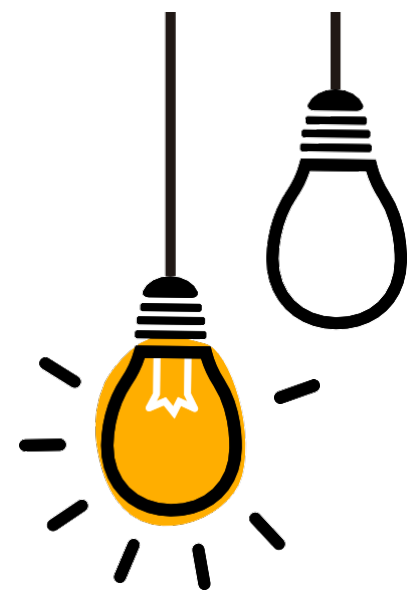
Solution:

- Regularly update software and systems to patch known vulnerabilities.
- Educate employees about phishing tactics and encourage cautious online behavior.
- Maintain robust backup systems to restore data without paying ransom.

09

Phishing Attacks

Phishing attacks involve fraudulent attempts to obtain sensitive information such as usernames, passwords, and financial details by posing as a trustworthy entity.

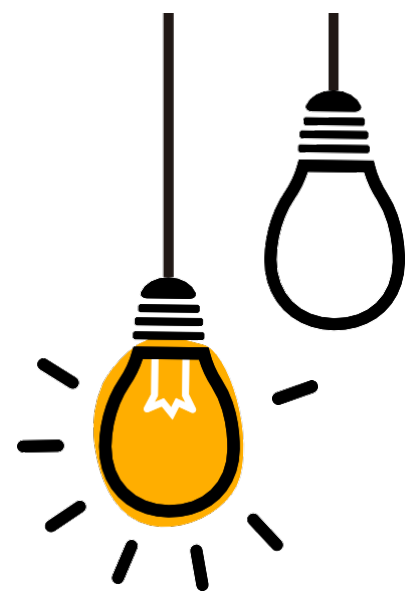


Solution:

- Implement email filters to detect and block phishing attempts.
- Train employees to recognize phishing tactics and report suspicious emails.
- Use multi-factor authentication to add an extra layer of security.

10

Distributed Denial of Service (DDoS) Attacks



DDoS attacks overwhelm a targeted system or network with a flood of traffic, disrupting normal operation and causing downtime. Attackers utilize botnets or other means to generate massive amounts of traffic, exhausting the target's resources.

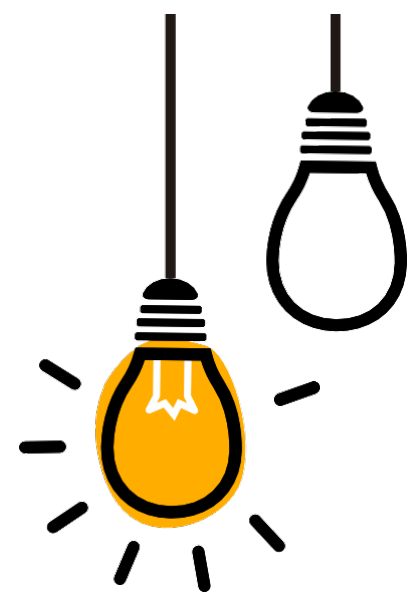
Solution:

- Employ DDoS mitigation services or hardware appliances to filter malicious traffic.
- Configure network infrastructure to handle sudden spikes in traffic.
- Implement rate limiting and access controls to prevent abuse.

11

Insider Threats

Insider threats involve malicious or negligent actions by individuals within an organization, posing risks to data security and integrity. Employees, contractors, or partners may intentionally or unintentionally compromise sensitive information or systems.



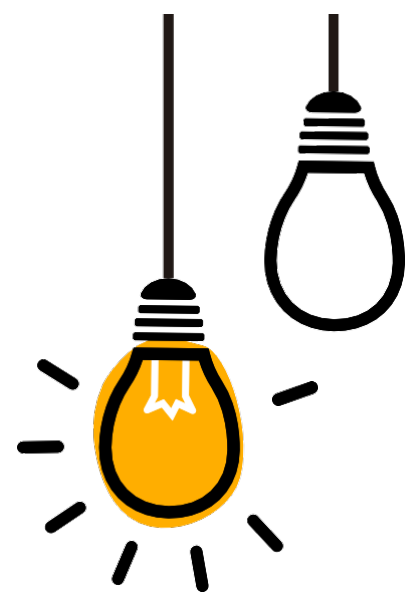
Solution:

- Implement access controls and least privilege principles to limit employees' access to sensitive data.
- Monitor and analyze user behavior for signs of suspicious activity.
- Conduct regular security awareness training to educate employees about security best practices.

12

Zero-Day Exploits

Zero-day exploits target previously unknown vulnerabilities in software or hardware, giving attackers the advantage of exploiting systems before a patch is available. Attackers discover and exploit vulnerabilities before developers can release patches or updates to fix them.



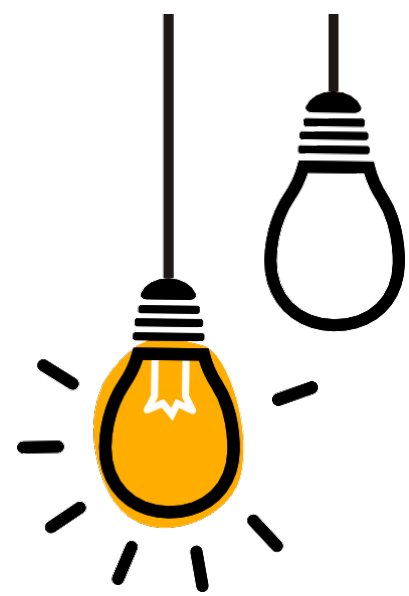
Solution:

- Employ intrusion detection systems to detect and block suspicious behavior.
- Encourage responsible disclosure of vulnerabilities to facilitate timely patching.
- Utilize virtual patching solutions to mitigate the risk until an official fix is available.

13

Data Breaches

Data breaches involve unauthorized access to sensitive or confidential information, potentially exposing individuals' personal data or intellectual property. Weak security measures, insider threats, or targeted attacks can lead to unauthorized access and exfiltration of data.



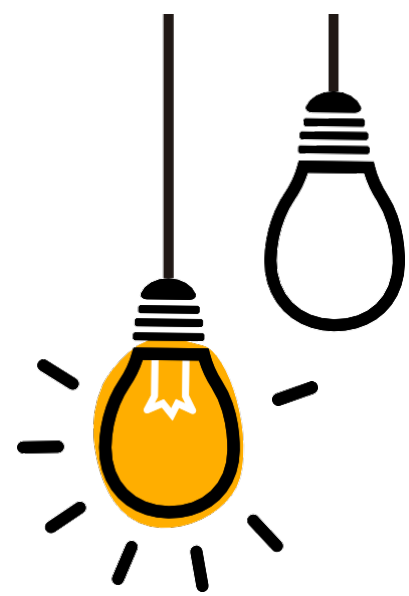
Solution:

- Encrypt sensitive data both in transit and at rest to mitigate the impact of a breach.
- Implement robust access controls and monitoring to detect and respond to unauthorized access attempts.
- Comply with data protection regulations and standards to prevent breaches and mitigate their consequences.

14

Malware

Malware encompasses various types of malicious software designed to disrupt, damage, or gain unauthorized access to computer systems or networks. Malware can be introduced through infected files, malicious websites, or vulnerabilities in software or operating systems.



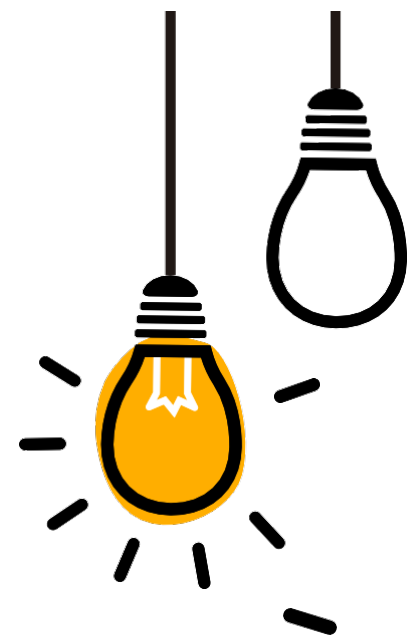
Solution:

- Use reputable antivirus & anti-malware software to detect and remove malicious programs.
- Keep software and systems up to date with security patches to mitigate known vulnerabilities.
- Practice safe browsing habits & exercise caution when downloading files or clicking on links.

15

Advanced Persistent Threats (APTs)

APTs are sophisticated, long-term cyber attacks orchestrated by skilled adversaries to infiltrate and maintain unauthorized access to targeted networks or systems.



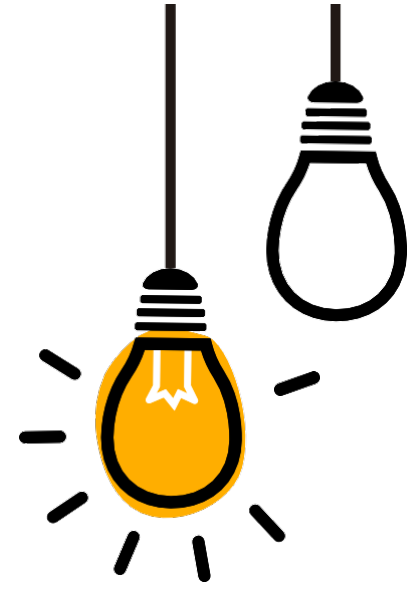
Solution:

- Implement defense-in-depth strategies combining network segmentation, encryption, and intrusion detection/prevention systems.
- Conduct regular security assessments and penetration testing to identify and remediate vulnerabilities.
- Foster a culture of security awareness and incident response readiness within the organization.

16

Supply Chain Attacks

Supply chain attacks target the software supply chain, exploiting vulnerabilities in third-party software or services to compromise the systems of end users or organizations.



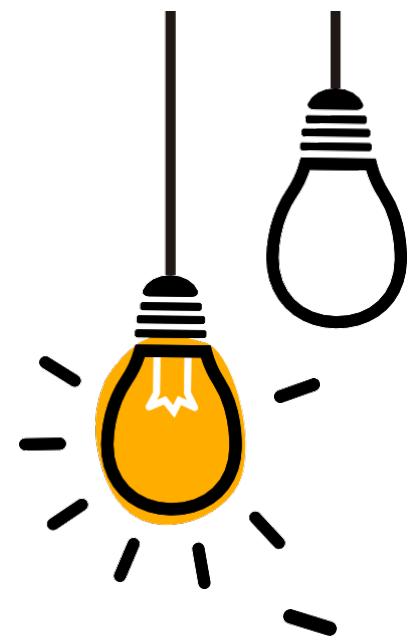
Solution:

- Vet and monitor third-party vendors and suppliers for security best practices and compliance with standards.
- Implement software composition analysis tools to identify and mitigate vulnerabilities in third-party components.
- Strengthen authentication and access controls to prevent unauthorized access to critical systems or data through the supply chain.

17

Cryptojacking

Cryptojacking involves the unauthorized use of someone else's computing resources to mine cryptocurrency, often done by infecting computers or websites with malware.



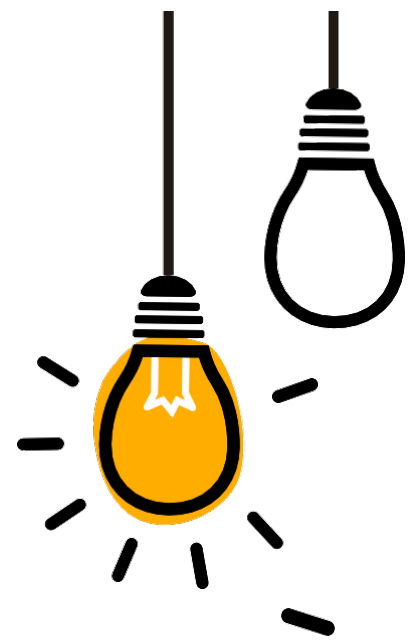
Solution:

- Employ robust endpoint security solutions to detect and block cryptojacking attempts.
- Utilize ad-blocking and script-blocking browser extensions to prevent cryptojacking scripts from executing.
- Monitor system resources for abnormal spikes in CPU usage, which may indicate cryptojacking activity.

18

Man-in-the-Middle (MitM) Attacks

MitM attacks involve intercepting communication between two parties to eavesdrop, manipulate, or impersonate either party, compromising the confidentiality and integrity of data.



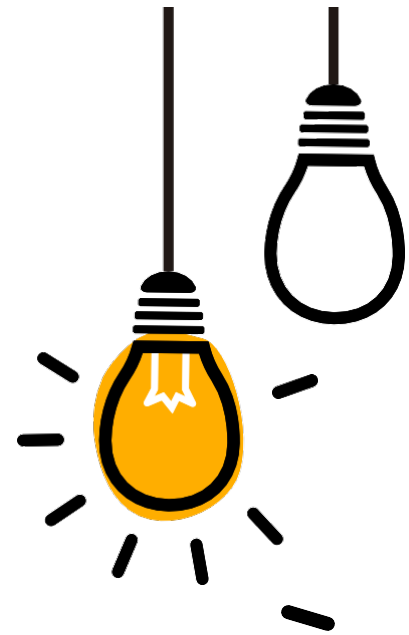
Solution:

- Implement encryption protocols such as HTTPS to secure communication channels and prevent eavesdropping.
- Use digital certificates & mutual authentication to verify the identity of communicating parties and detect potential MitM attacks.
- Regularly update network devices and software to patch known vulnerabilities that could be exploited in MitM attacks.

19

Social Engineering Attacks

Social engineering attacks exploit human psychology to manipulate individuals into divulging confidential information, providing access to systems, or performing actions beneficial to the attacker



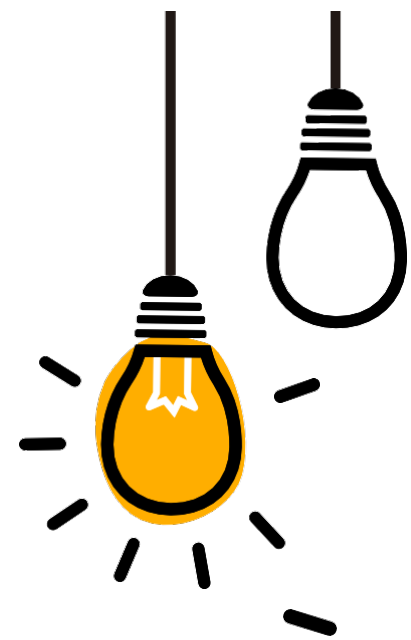
Solution:

- Provide security awareness training to educate employees about common social engineering tactics and how to recognize and respond to them.
- Implement strict access controls and verification procedures to validate requests for sensitive information or system access.

20

Fileless Malware

Fileless malware operates in memory without leaving traces on disk, making it difficult to detect using traditional antivirus or anti-malware solutions. Attackers exploit vulnerabilities in legitimate software to execute malicious code directly in memory, bypassing file-based detection methods.



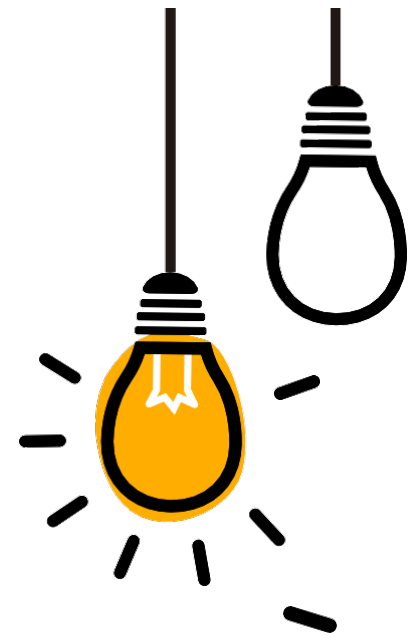
Solution:

- Implement behavior-based detection mechanisms to identify suspicious activities indicative of fileless malware.
- Monitor system memory and process execution for anomalies that may indicate fileless malware attacks.
- Utilize EDR solutions to continuously monitor and analyze system behavior for signs of compromise.

21

IoT Botnets

IoT botnets consist of compromised IoT devices infected with malware and controlled by a central command-and-control (C&C) server to orchestrate large-scale attacks, such as DDoS attacks.



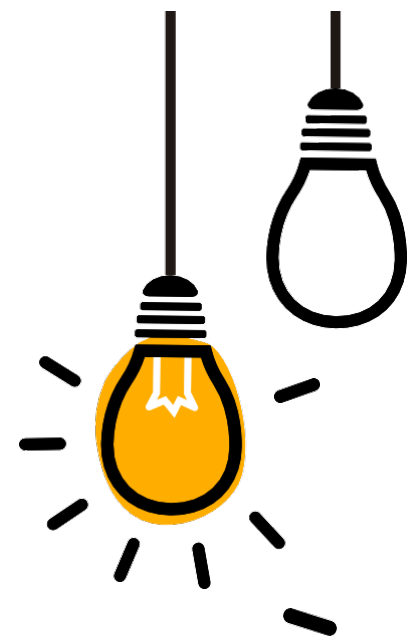
Solution:

- Strengthen IoT device security by changing default passwords, applying security patches, and disabling unnecessary services.
- Segment IoT devices from critical networks to limit the impact of compromised devices and prevent lateral movement within the network.
- Employ network traffic monitoring and anomaly detection to identify and mitigate botnet-related activities.

22

Cross-Site Scripting (XSS) Attacks

XSS attacks involve injecting malicious scripts into web pages viewed by other users, allowing attackers to execute scripts in the context of their victims' browsers.



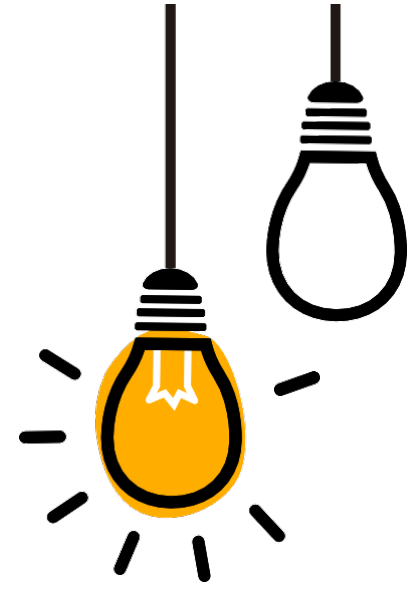
Solution:

- Implement input validation and output encoding to sanitize user input and prevent XSS attacks.
- Use security headers, such as CSP, to mitigate the impact of XSS attacks by controlling the sources from which resources can be loaded.
- Conduct regular security assessments and code reviews to identify and remediate XSS vulnerabilities in web applications.

23

Identity Theft

Identity theft involves the unauthorized use of someone else's personal or financial information to impersonate them or commit fraudulent activities.



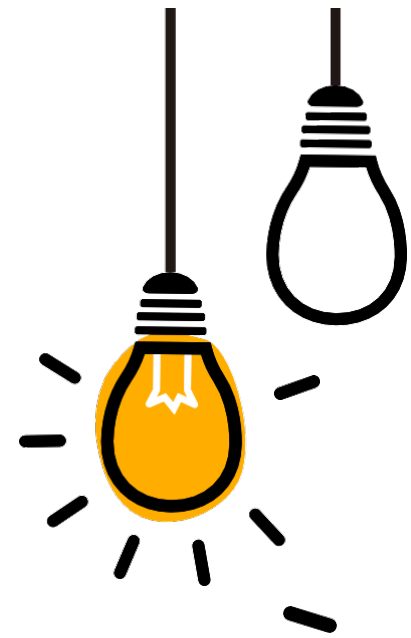
Solution:

- Enable multi-factor authentication (MFA) to add an extra layer of security and prevent unauthorized access to accounts.
- Monitor financial transactions and credit reports for suspicious activity indicative of identity theft.
- Educate individuals about the importance of safeguarding personal information and practicing good security hygiene to mitigate the risk of identity theft.

24

Data Leakage

Data leakage occurs when sensitive or confidential information is unintentionally or maliciously disclosed to unauthorized parties, compromising data privacy and integrity.



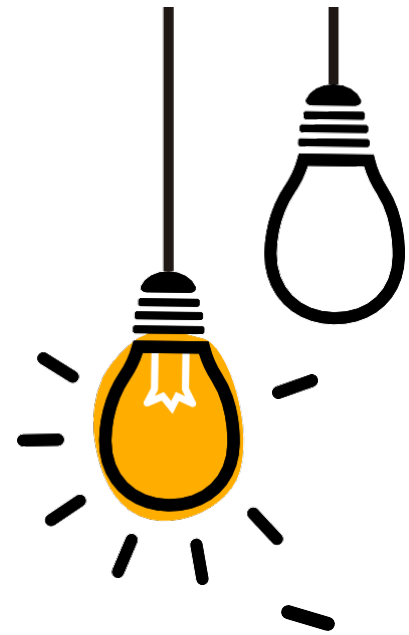
Solution:

- Implement data loss prevention (DLP) solutions to monitor and control the movement of sensitive data within and outside the organization.
- Encrypt sensitive data at rest and in transit to prevent unauthorized access in case of data leakage.
- Conduct regular security audits and risk assessments to identify vulnerabilities and gaps in data protection measures and take corrective actions.

25

Business Email Compromise (BEC)

BEC attacks target organizations to deceive employees into transferring funds, disclosing sensitive information, or performing actions beneficial to the attacker by impersonating executives or trusted entities.



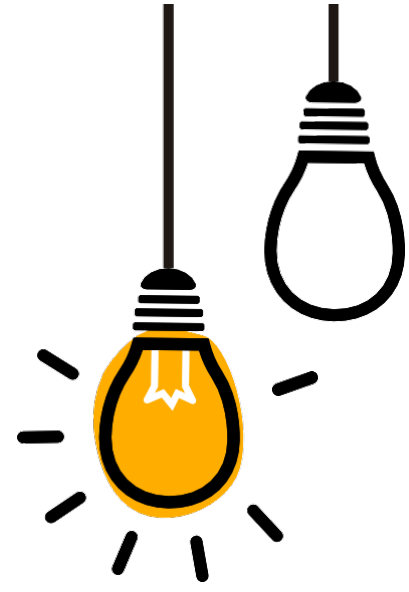
Solution:

- Implement email authentication mechanisms such as SPF, DKIM, and DMARC to detect and prevent email spoofing and impersonation.
- Establish verification procedures and authorization controls for financial transactions, sensitive information disclosure, and other critical actions.

26

Mobile Malware

Mobile malware refers to malicious software specifically designed to target mobile devices, such as smartphones and tablets, compromising their security and privacy.



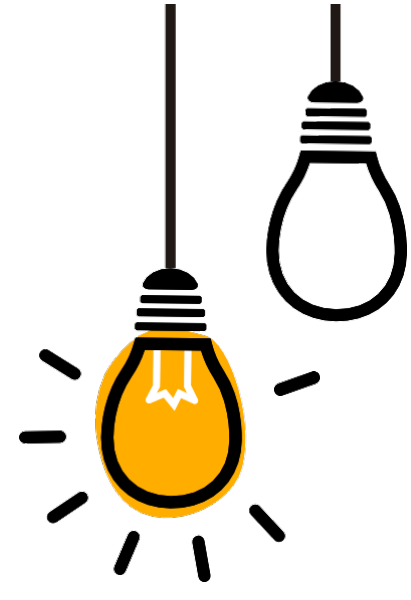
Solution:

- Download apps only from official app stores and reputable sources to minimize the risk of downloading malicious software.
- Keep mobile devices up to date with security patches and software updates to address known vulnerabilities and security flaws.
- Install mobile security solutions, such as antivirus and anti-malware apps, to detect and remove malicious software from devices.

27

AI-Powered Cyber Attacks

AI-powered cyber attacks leverage AI and ML algorithms to automate and enhance the capabilities of traditional cyber attacks, making them more sophisticated and evasive.



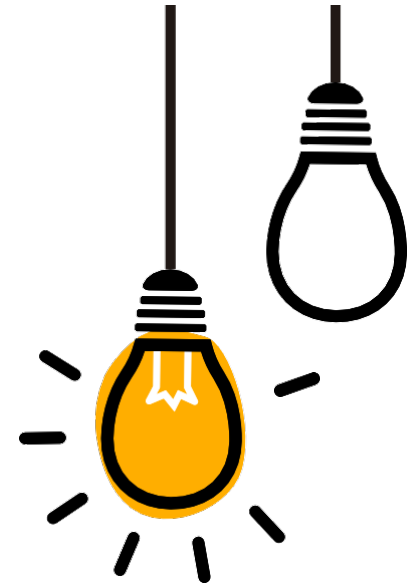
Solution:

- Employ AI-based security solutions to detect and respond to AI-powered cyber attacks in real-time.
- Enhance security awareness & training programs to educate employees about the risks and characteristics of AI-driven attacks.
- Collaborate with industry partners & researchers to develop AI-based defense mechanisms & countermeasures against evolving threats.

28

DNS Hijacking

DNS hijacking involves redirecting DNS queries to malicious servers controlled by attackers, enabling them to intercept and manipulate internet traffic, redirect users to phishing sites, or launch other malicious activities.



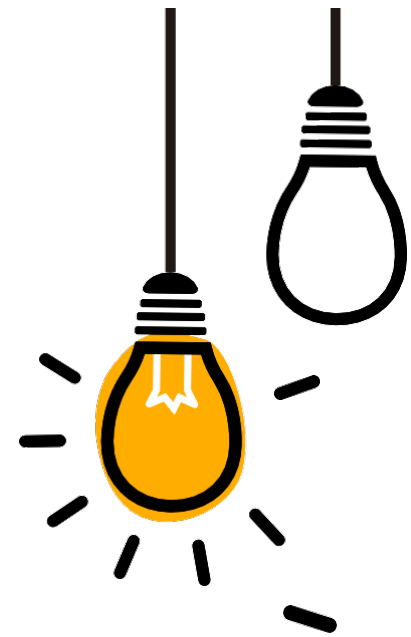
Solution:

- Use DNSSEC (Domain Name System Security Extensions) to cryptographically verify the authenticity of DNS responses and prevent DNS hijacking attacks.
- Implement DNS monitoring and logging to detect unauthorized changes to DNS records and identify potential hijacking attempts.
- Harden DNS server configurations and apply security best practices to mitigate the risk of DNS hijacking.

29

Physical Attacks on Infrastructure

Physical attacks on infrastructure involve sabotaging or damaging critical systems, facilities, or equipment through physical means, such as vandalism, theft, or tampering.



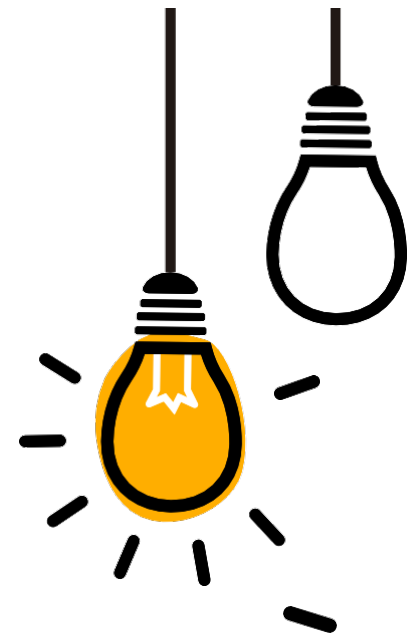
Solution:

- Implement physical security measures, such as access controls, surveillance cameras, and perimeter fencing, to protect critical infrastructure from unauthorized access and tampering.
- Conduct regular security assessments and audits to identify and remediate physical vulnerabilities in infrastructure components.

30

Cyber Espionage

Cyber espionage involves stealing sensitive information, intellectual property, or classified data from government agencies, corporations, or individuals for political, economic, or strategic purposes.



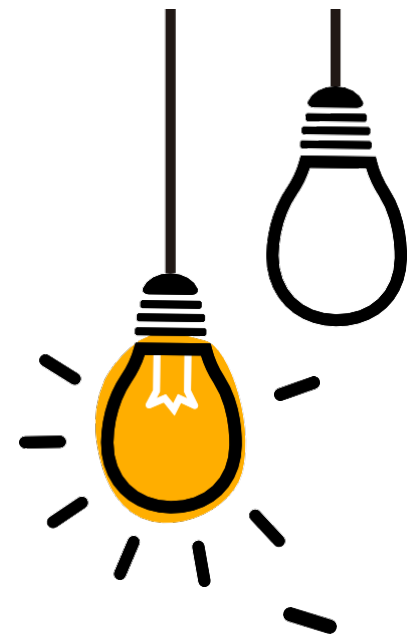
Solution:

- Implement robust network security measures, such as encryption, intrusion detection systems, and data loss prevention solutions, to protect sensitive information from unauthorized access.
- Monitor network traffic and user activity for indicators of compromise (IOCs) associated with cyber espionage activities, such as reconnaissance, data exfiltration, or lateral movement.

31

AI-Powered Deepfakes

AI-powered deepfakes use artificial intelligence algorithms to generate highly realistic fake images, videos, or audio recordings, often used for disinformation, fraud, or blackmail purposes.



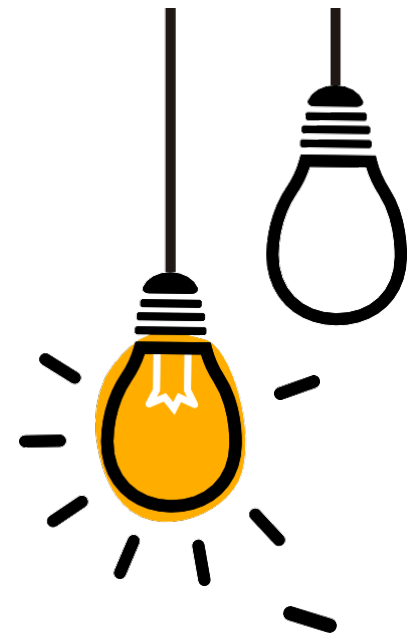
Solution:

- Develop and deploy AI-based detection tools and algorithms to identify and mitigate deepfake content across various online platforms and communication channels.
- Educate the public about the existence and potential dangers of deepfake technology to raise awareness and critical thinking skills.
- Collaborate with technology companies, research institutions, to establish standards and regulations for the responsible use of deepfake technology and combat its misuse.

32

File Encryption Trojans

File encryption trojans, also known as cryptoransomware, encrypt files on a victim's system and demand a ransom payment in exchange for the decryption key, extorting money from individuals or organizations.



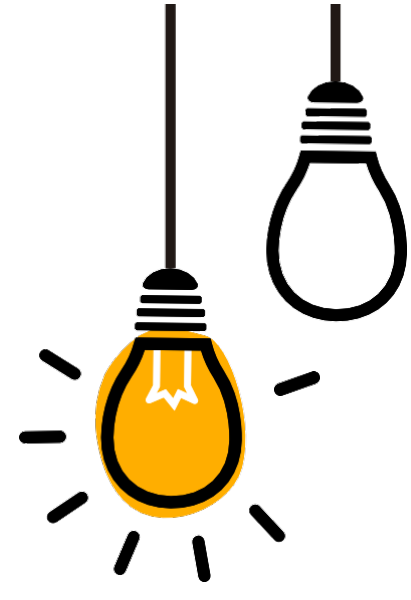
Solution:

- Implement robust backup and recovery procedures to regularly backup critical data and restore systems without paying ransom in the event of a cryptoransomware attack.
- Use endpoint security solutions, such as antivirus software and intrusion detection systems, to detect and block file encryption trojans before they can encrypt files.

33

Credential Stuffing Attacks

Credential stuffing attacks involve using large sets of stolen usernames and passwords to gain unauthorized access to user accounts across various online services and platforms, exploiting password reuse and weak authentication practices.

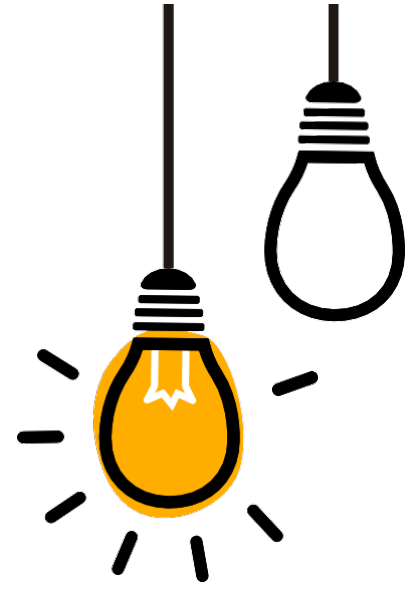


Solution:

- Enforce strong password policies and encourage users to use unique, complex passwords for each online account to mitigate the impact of credential stuffing attacks.
- Implement multi-factor authentication (MFA) mechanisms, such as SMS codes, authenticator apps, or biometric authentication, to add an extra layer of security and prevent unauthorized access to accounts.

34

Bluetooth Impersonation Attacks



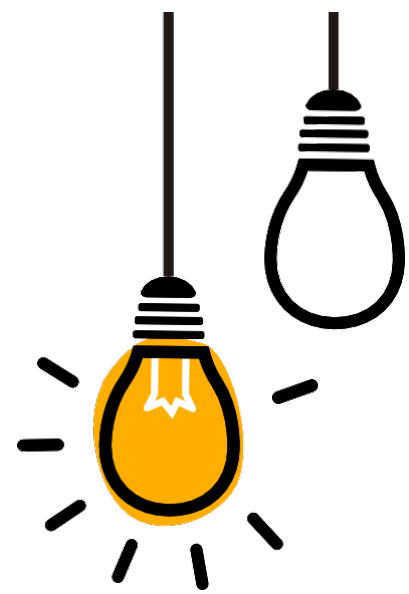
Bluetooth impersonation attacks involve impersonating legitimate Bluetooth devices to establish unauthorized connections and gain access to target systems or services.

Solution:

- Keep Bluetooth-enabled devices updated with the latest firmware and security patches.
- Disable unnecessary Bluetooth services and configure devices to require manual approval for pairing.
- Monitor Bluetooth traffic and employ intrusion detection systems to detect and mitigate impersonation attacks.

35

USB-Based Attacks



USB-based attacks involve exploiting vulnerabilities in USB devices or ports to infect computers, steal sensitive information, or deliver malware payloads, exploiting the convenience and ubiquity of USB technology.

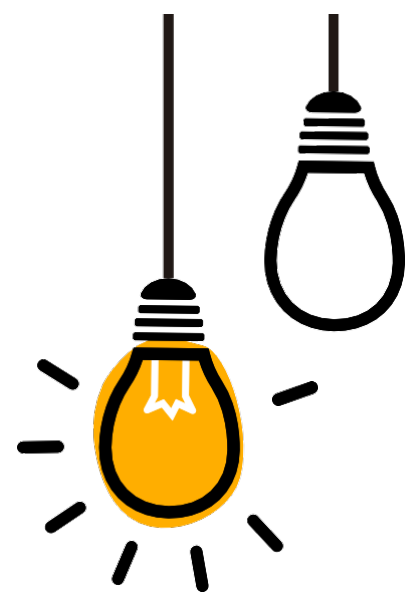
Solution:

- Disable autorun and autoplay features on computers and devices to prevent automatic execution of malicious code when USB devices are connected.
- Use endpoint security solutions, such as antivirus software and intrusion detection systems, to scan USB devices for malware and block malicious activities.

36

Formjacking Attacks

Formjacking attacks involve injecting malicious code into e-commerce websites to steal payment card details entered by users during online transactions, compromising their financial information.



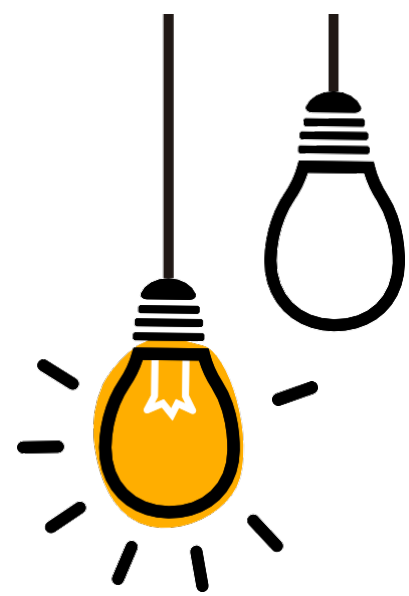
Solution:

- Implement web application firewalls (WAFs) to detect and block formjacking attempts by filtering malicious requests and scripts.
- Encrypt sensitive data, such as payment card details, during transmission to prevent interception by attackers conducting formjacking attacks.

37

Watering Hole Attacks

Watering hole attacks involve compromising legitimate websites frequented by targeted individuals or organizations and injecting malicious code to infect visitors' devices with malware, exploiting trust and familiarity.



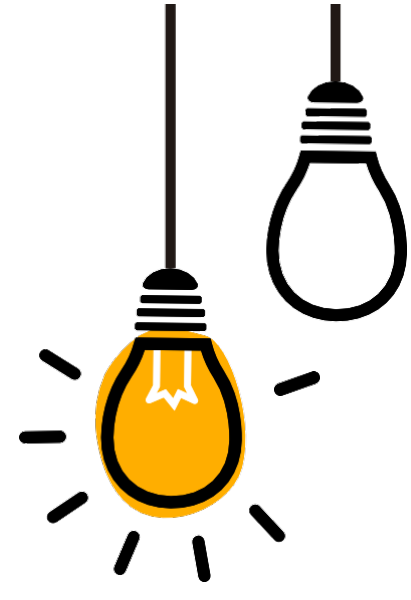
Solution:

- Use web content filtering and reputation-based security solutions to block access to known malicious websites and prevent users from inadvertently visiting compromised sites.
- Implement browser isolation or sandboxing techniques to contain and mitigate the impact of potential malware infections resulting from watering hole attacks.

38

Supply Chain Compromise

Supply chain compromise involves infiltrating and tampering with the software supply chain, infecting legitimate software or components distributed to end users with malware or backdoors, compromising their security.



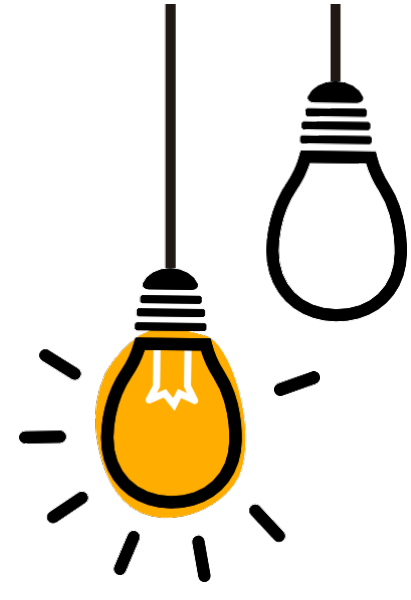
Solution:

- Vet and verify the security practices of software vendors and third-party suppliers to ensure the integrity and trustworthiness of software and components integrated into the supply chain.
- Implement code signing and digital certificates to verify the authenticity and integrity of software updates and components distributed through the supply chain.

39

Voice Phishing (Vishing)

Voice phishing (vishing) attacks involve using phone calls or voice messages to deceive individuals into disclosing sensitive information, such as passwords, personal identification numbers (PINs), or financial details, over the phone.

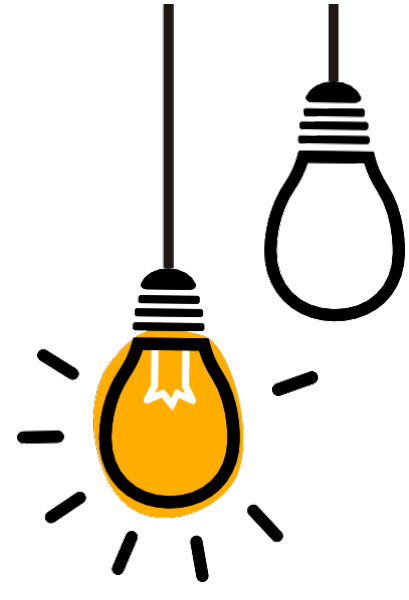


Solution:

- Implement caller ID authentication and verification mechanisms to validate the identity of callers and detect spoofed or fraudulent phone numbers used in vishing attacks.
- Encourage individuals to verify the legitimacy of unexpected or suspicious calls by contacting the organization or individual directly through official channels before disclosing sensitive information.

40

Deep Packet Inspection (DPI) Evasion



Deep Packet Inspection (DPI) evasion techniques involve circumventing network security measures, such as firewalls or intrusion detection/prevention systems, by obfuscating or encrypting malicious traffic to evade detection.

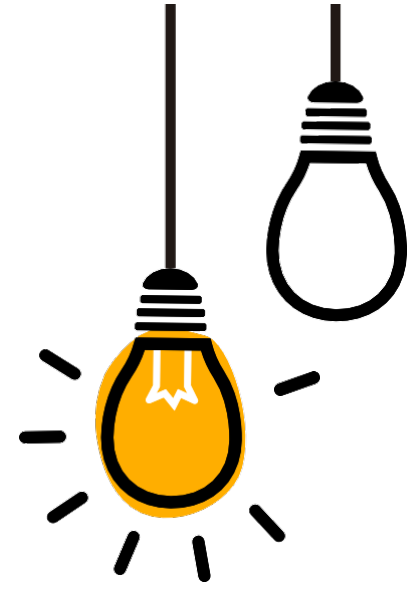
Solution:

- Deploy advanced threat detection and analysis tools capable of decrypting and inspecting encrypted traffic for signs of malicious activity while maintaining privacy and compliance with data protection regulations.
- Implement network segmentation and access controls to restrict the flow of traffic between network segments and prevent lateral movement by attackers

41

Browser-based Cryptojacking

Browser-based cryptojacking involves leveraging JavaScript-based cryptocurrency mining scripts embedded in websites to hijack visitors' CPU resources and mine cryptocurrency without their consent or knowledge.

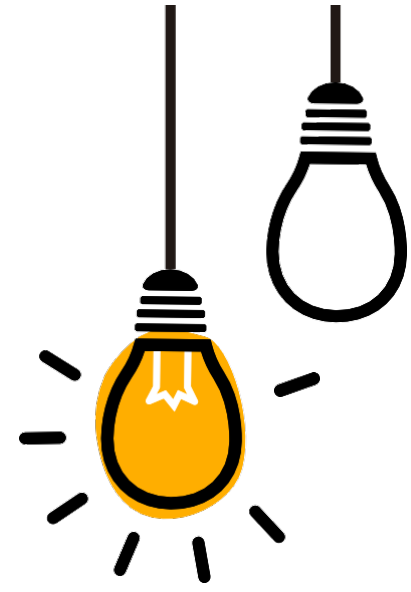


Solution:

- Use browser extensions or security tools to detect and block cryptojacking scripts running in web browsers and prevent unauthorized cryptocurrency mining activity.
- Educate website owners about the risks of hosting cryptojacking scripts on their sites and encourage them to implement measures, such as CSP or script-blocking techniques, to mitigate the threat.

42

Simultaneous Multithreading (SMT) Side-Channel Attacks



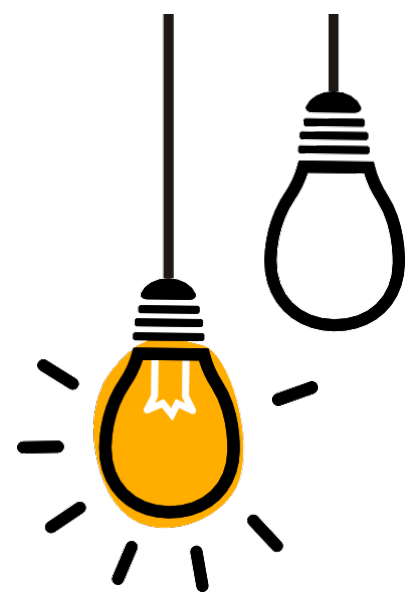
Simultaneous Multithreading (SMT) side-channel attacks exploit hardware vulnerabilities and microarchitectural flaws in processors to leak sensitive information across CPU cores sharing the same physical core resources.

Solution:

- Apply microcode updates, firmware patches, and software mitigations provided by CPU vendors to address known vulnerabilities and protect against SMT side-channel attacks targeting processor microarchitectures.

43

Firmware Vulnerabilities



Firmware vulnerabilities refer to security weaknesses and exploitable flaws present in the low-level software embedded in hardware devices, such as BIOS, UEFI, or device firmware, which can be exploited to compromise system integrity and security.

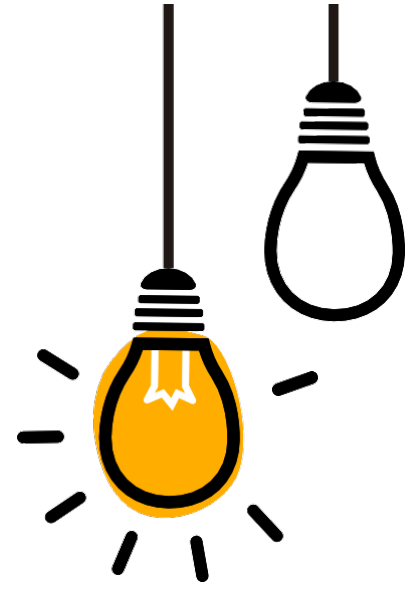
Solution:

- Regularly update firmware and apply security patches provided by device manufacturers to mitigate known vulnerabilities and address security flaws present in firmware code.
- Implement secure boot mechanisms, firmware integrity verification, and code signing to prevent tampering, unauthorized modification

44

Mobile App Spoofing

Mobile app spoofing involves creating fake or malicious applications that impersonate legitimate apps to deceive users into downloading and installing them, potentially leading to data theft, financial fraud, or device compromise.

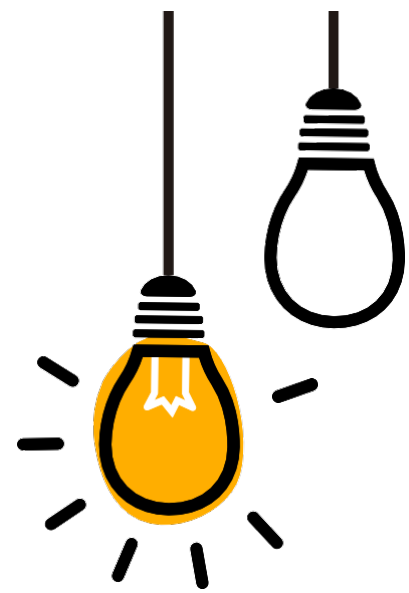


Solution:

- Download mobile apps only from official app stores, such as Google Play Store or Apple App Store, to minimize the risk of installing counterfeit or malicious applications.
- Enable app verification settings and security features on mobile devices to detect and block the installation of untrusted or potentially harmful apps from unknown sources.

45

Cloud Service Misconfiguration



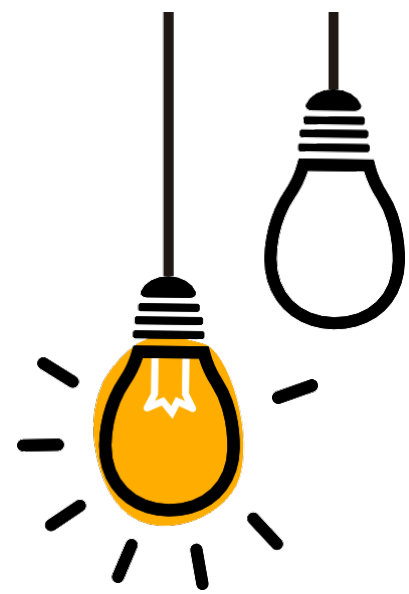
Cloud service misconfiguration occurs when cloud resources, storage buckets, databases, or server instances are improperly configured, exposing sensitive data, assets, or infrastructure to unauthorized access, data breaches, or exploitation.

Solution:

- Conduct regular cloud security assessments, configuration audits, and compliance checks to identify and remediate misconfigurations, vulnerabilities, or security gaps in cloud infrastructure and services.

46

Data Exfiltration through Stenography



Data exfiltration through steganography involves concealing sensitive information or covert communications within digital images, audio files, or other media objects to evade detection and exfiltrate data from compromised systems or networks.

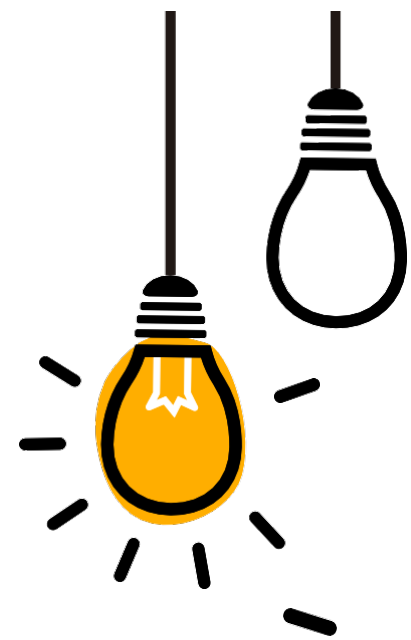
Solution:

- Deploy network monitoring, data loss prevention (DLP), and advanced threat detection solutions capable of analyzing multimedia content, inspecting file attributes, and detecting steganographic payloads or covert communications.

47

Adversarial Machine Learning Attacks

Adversarial machine learning attacks manipulate or deceive machine learning models by exploiting vulnerabilities in the model's training data or algorithms.



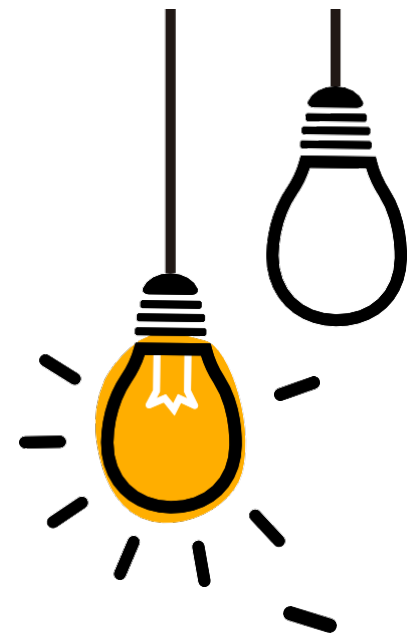
Solution:

- Regularly update and retrain machine learning models with diverse and representative datasets.
- Implement robust validation techniques to detect and filter out adversarial inputs.
- Employ adversarial training and model ensembling to enhance model resilience against attacks.

48

App Store Fraud

App store fraud involves manipulation of app rankings, reviews, or downloads to deceive users or game algorithms for financial gain or reputation.



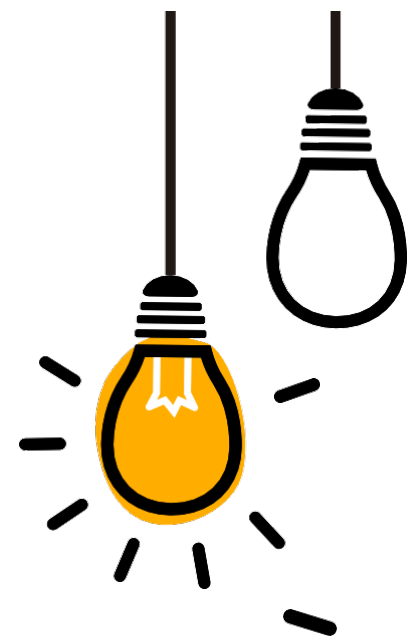
Solution:

- Implement strict review processes and fraud detection mechanisms in app store platforms.
- Educate users about the risks of downloading apps from untrusted sources.
- Collaborate with app store operators and cybersecurity experts to investigate and remove fraudulent apps.

49

Insufficient Security Patching

Insufficient security patching refers to the failure to apply timely updates, patches, or fixes to address known vulnerabilities and security flaws in software, systems, or devices, exposing them to exploitation by attackers.

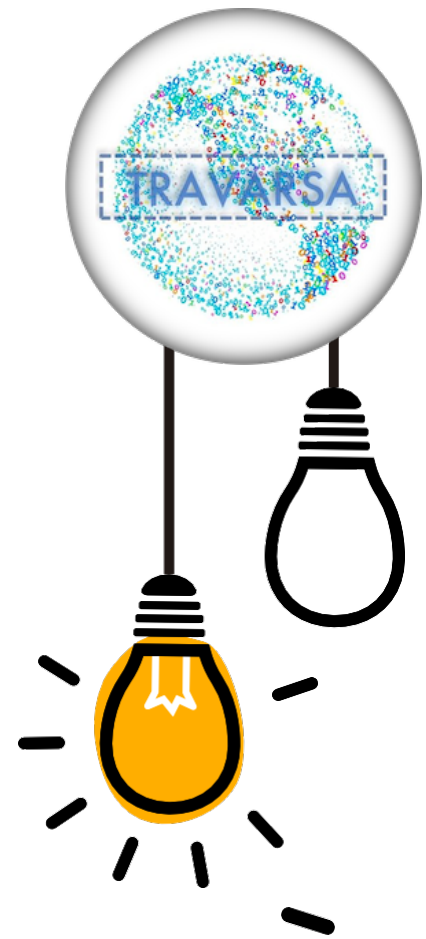


Solution:

- Implement automated patch management solutions, vulnerability scanners, and configuration management tools to identify, prioritize, and apply security patches promptly across IT infrastructure, minimizing the window of exposure to known vulnerabilities.

50

Automated Brute Force Attacks



Automated brute force attacks systematically guess passwords or authentication credentials using automated tools to gain unauthorized access to accounts or systems.

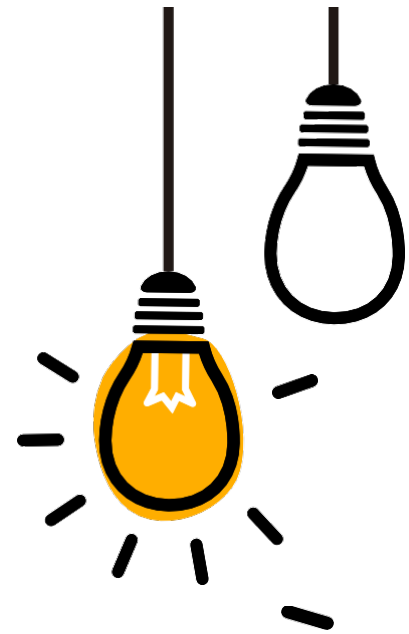
Solution:

- Enforce strong password policies and multifactor authentication to mitigate the risk of successful brute force attacks.
- Implement account lockout mechanisms and rate limiting to prevent repeated login attempts.
- Monitor login attempts and detect suspicious patterns indicative of brute force attacks.

51

Blockchain Vulnerabilities

Blockchain vulnerabilities refer to weaknesses or flaws in blockchain networks or protocols that can be exploited by attackers to compromise the integrity, confidentiality, or availability of decentralized systems.



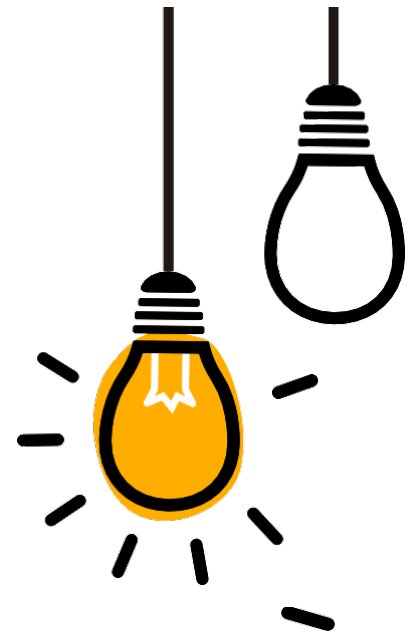
Solution:

- Conduct regular security audits and penetration testing of blockchain networks.
- Follow best practices for secure smart contract development and deploy decentralized governance mechanisms.
- Enhance network resilience by diversifying validator nodes and implementing robust consensus protocols.

52

Whaling Attacks

Whaling attacks, also known as CEO fraud or Business Email Compromise (BEC), target high-profile individuals or executives within organizations, impersonating them to deceive employees into transferring funds, disclosing sensitive information, or performing fraudulent actions.

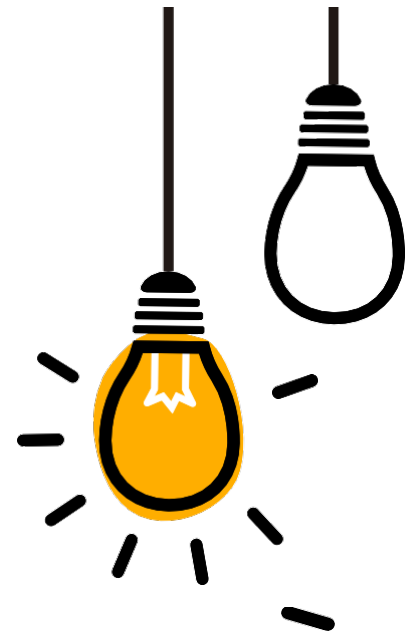


Solution:

- Implement email authentication protocols such as SPF, DKIM, and DMARC to verify sender authenticity, detect email spoofing, and prevent domain impersonation attacks used in whaling campaigns.

53

Logic Bombs



Logic bombs are malicious code snippets or software components embedded within legitimate applications, scripts, or systems, programmed to execute a destructive action or trigger a malicious payload when specific conditions or triggers are met.

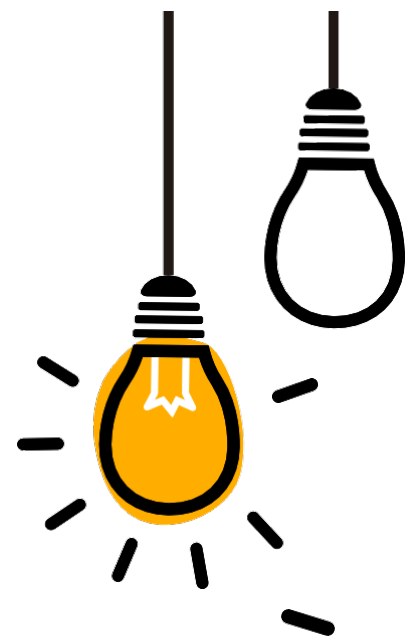
Solution:

- Implement code reviews, static analysis, and secure coding practices to identify and remove suspicious or malicious code fragments, including potential logic bombs, from software applications, scripts, or automated workflows.

54

File Encryption Ransomware

File encryption ransomware is a type of malicious software that encrypts files or entire systems, rendering them inaccessible to users until a ransom is paid to the attackers, who promise to provide the decryption key upon payment.



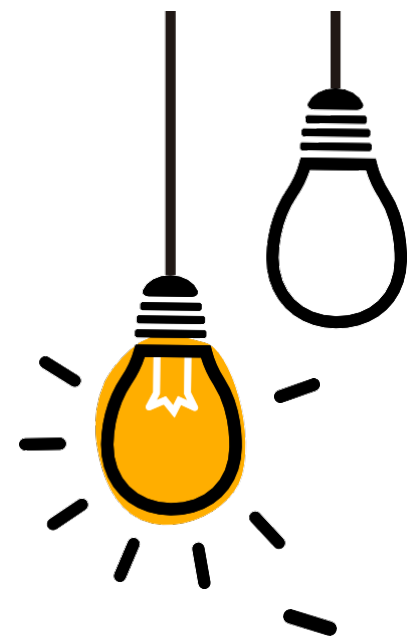
Solution:

- Implement robust backup and disaster recovery procedures to regularly backup critical data and systems, enabling organizations to restore files from unaffected backups in the event of file encryption ransomware infections, reducing the incentive to pay ransoms to attackers.

55

Biometric Spoofing

Biometric spoofing, also known as biometric presentation attacks, involves the use of fake biometric data, such as fingerprints, facial images, or iris scans, to deceive biometric authentication systems and gain unauthorized access to secured devices, applications, or facilities.

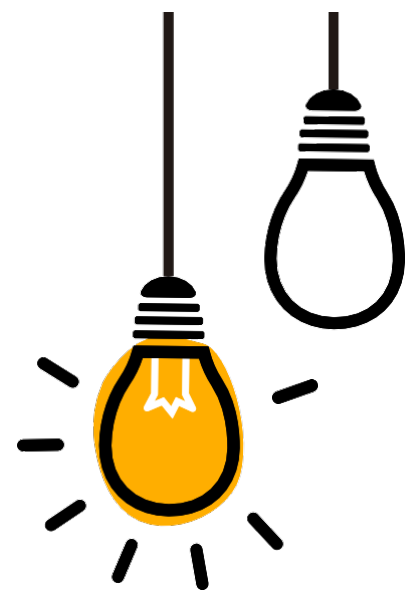


Solution:

- Employ liveness detection, biometric anti-spoofing techniques, and multi-factor authentication (MFA) to enhance the resilience of biometric systems against presentation attacks, ensuring the authenticity and integrity of biometric data captured during authentication.

56

Eavesdropping (Passive Surveillance)



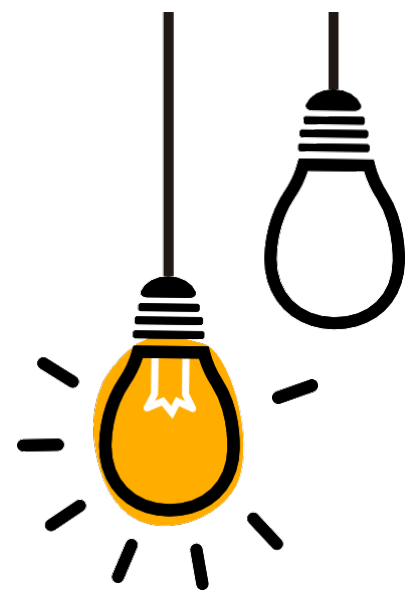
Eavesdropping, also known as passive surveillance, involves unauthorized interception and monitoring of communications, such as network traffic, phone calls, or wireless transmissions, with the aim of gathering sensitive information or intelligence without the knowledge or consent of the parties involved.

Solution:

- Encrypt sensitive communications using strong encryption protocols, such as SSL/TLS for web traffic, VPNs for remote access, and end-to-end encryption for messaging applications, to protect data confidentiality and prevent eavesdropping attacks.

57

Voice Assistant Exploitation



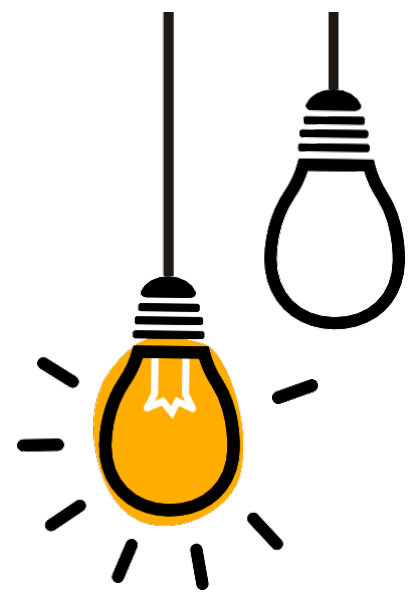
Voice assistant exploitation refers to cyber attacks targeting voice-activated virtual assistants, such as Amazon Alexa, Google Assistant, or Apple Siri, to manipulate devices, extract sensitive information, or compromise user privacy through voice commands or audio interactions.

Solution:

- Secure voice assistant devices with strong authentication mechanisms, voice recognition training, and privacy settings to prevent unauthorized access, restrict voice commands, and enhance user control over voice assistant interactions and data sharing.

58

Malvertising (Malicious Advertising)



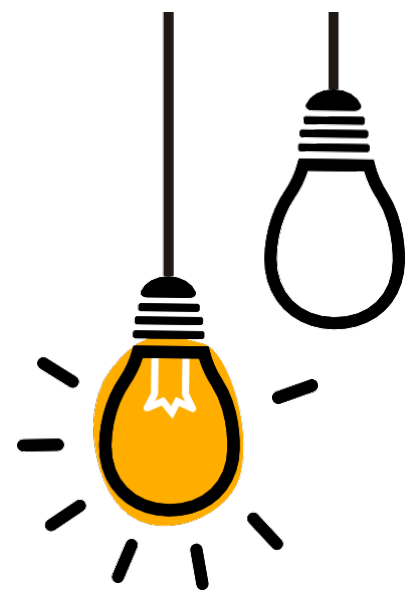
Malvertising, short for malicious advertising, involves the distribution of malicious code, exploit kits, or phishing scams through online advertisements displayed on legitimate websites, exploiting vulnerabilities in ad networks, ad exchanges, or web browsers to compromise visitor devices.

Solution:

- Deploy ad-blocking software, browser extensions, or network-level filtering solutions to block malicious ads, prevent drive-by downloads, and mitigate the risk of malvertising infections when visiting websites with potentially compromised advertising content.

59

5G Network Vulnerabilities



5G network vulnerabilities refer to security weaknesses, risks, or exposures inherent in 5th generation cellular networks, including infrastructure components, protocols, or deployment architectures, which adversaries may exploit to launch cyber attacks, intercept communications, or compromise network integrity.

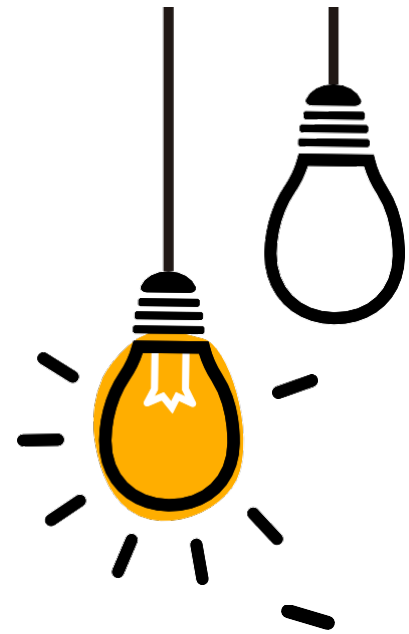
Solution:

- Enhance 5G network security through encryption, authentication, and access control mechanisms, leveraging technologies such as 5G-AKA (Authentication and Key Agreement), network slicing isolation, and secure virtualized infrastructure

60

Credential Theft via Keylogging

Credential theft via keylogging involves capturing and recording user keystrokes, login credentials, or sensitive information entered via keyboards, virtual keyboards, or touchscreen interfaces, compromising user privacy and security.



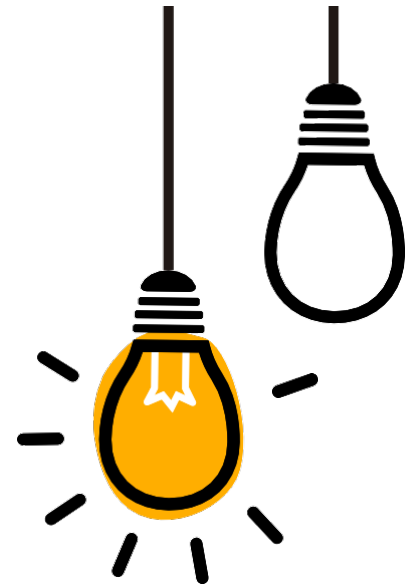
Solution:

- Deploy endpoint security solutions, anti-malware tools, and intrusion detection systems capable of detecting and blocking keylogging activities, preventing the installation or execution of keyloggers on compromised systems.

61

Backdoor Attacks

Backdoor attacks involve the insertion of unauthorized access points into software, systems, or networks, enabling attackers to bypass security controls and gain persistent access for malicious purposes.



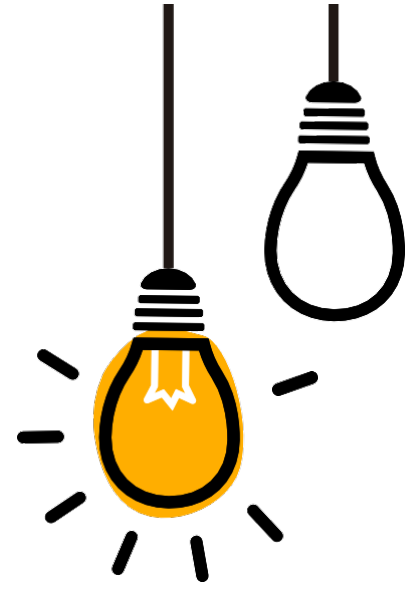
Solution:

- Conduct regular security assessments, code reviews, and vulnerability scans to identify and remove backdoors from software or systems before deployment.
- Implement network segmentation, intrusion detection/prevention systems (IDS/IPS), and endpoint protection measures to detect and block unauthorized access attempts through backdoors.

62

Smart Contract Vulnerabilities

Smart contract vulnerabilities are weaknesses or flaws in blockchain-based smart contracts, allowing attackers to exploit coding errors, logic flaws, or design weaknesses to steal cryptocurrency, manipulate transactions, or disrupt operations.

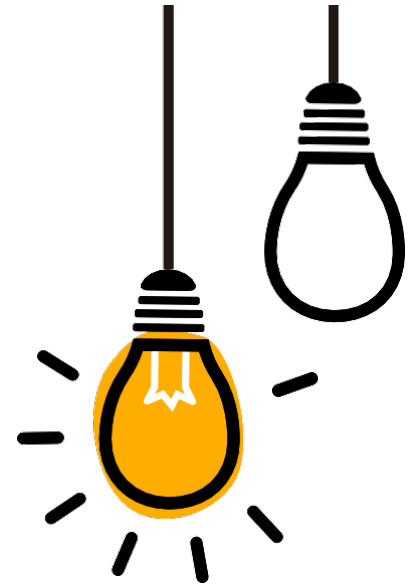


Solution:

- Conduct thorough code reviews, static analysis, and formal verification of smart contracts to identify and remediate vulnerabilities before deployment on blockchain networks.
- Utilize security best practices and design patterns for smart contract development, including input validation, access controls, and fail-safe mechanisms.

63

Typosquatting Attacks



Typosquatting attacks involve registering domain names similar to legitimate websites or brands but containing typographical errors or misspellings, with the intent to deceive users and exploit their mistakes for malicious purposes.

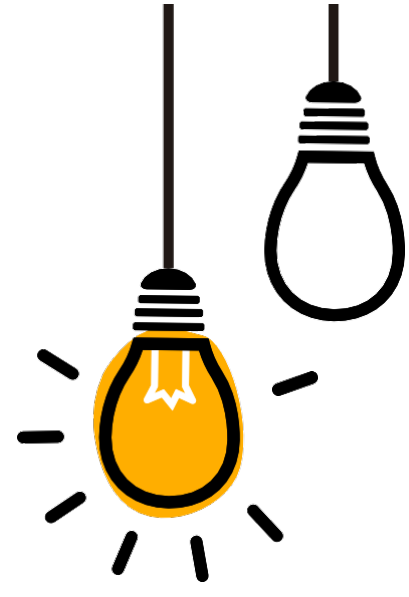
Solution:

- Educate users about the risks of typosquatting attacks, advising them to double-check URLs, verify website authenticity, and avoid clicking on suspicious links or visiting unfamiliar domains to minimize the likelihood of falling victim to such attacks.

64

Zero-Click Exploits

Zero-click exploits are cyber attacks that require no user interaction or engagement to compromise a target device or system, exploiting vulnerabilities in software, protocols, or hardware components to execute arbitrary code or gain unauthorized access silently.



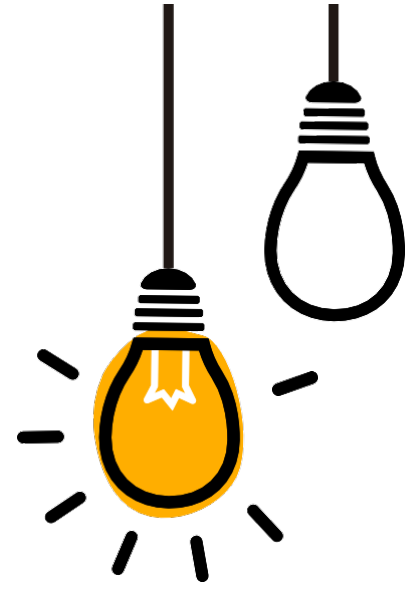
Solution:

- Utilize exploit prevention mechanisms, such as address space layout randomization (ASLR), data execution prevention (DEP), or control-flow integrity (CFI), to thwart memory-based attacks and disrupt exploit chains used in zero-click exploitation techniques.

65

Rogue Software

Rogue software, also known as scareware or fake antivirus, refers to malicious software or applications that masquerade as legitimate security tools or utilities, deceiving users into purchasing unnecessary software licenses or providing sensitive information.

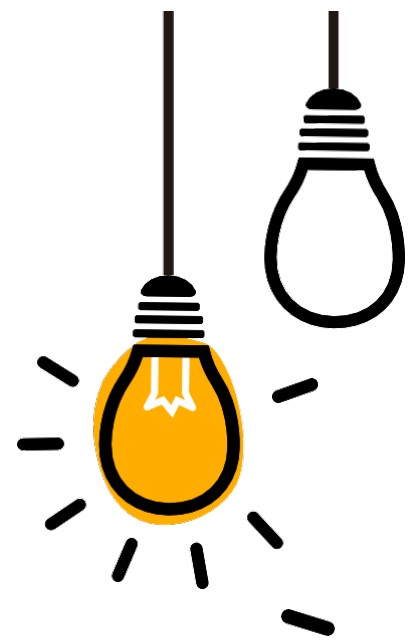


Solution:

- Educate users about common tactics used by rogue software, advising them to verify the authenticity of security alerts, avoid downloading software from untrusted sources, and conduct research before purchasing or installing security products.

66

USB Rubber Ducky Attacks



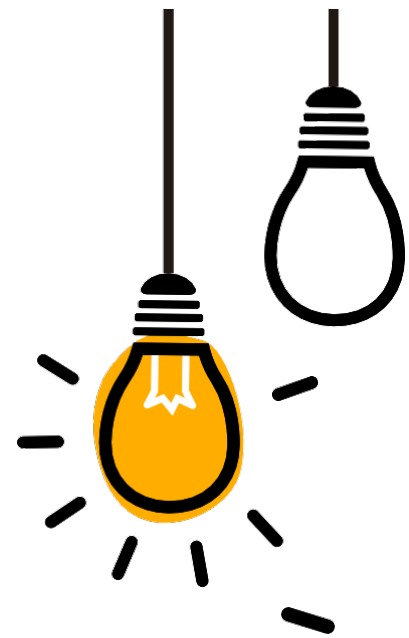
deceivingUSB Rubber Ducky attacks involve the use of specially crafted USB devices, such as keystroke injection tools or HID (Human Interface Device) emulators, to mimic keyboard input and execute malicious commands or payloads on target systems.

Solution:

- Implement endpoint security policies to disable auto-run functionality, restrict USB device access, and enforce device whitelisting to prevent unauthorized USB Rubber Ducky devices from executing malicious payloads on endpoint systems.

67

Remote Code Execution (RCE) Vulnerabilities



Remote Code Execution (RCE) vulnerabilities allow attackers to execute arbitrary code or commands on target systems remotely, often resulting from security flaws in software applications, web servers, or network protocols that enable unauthorized code execution.

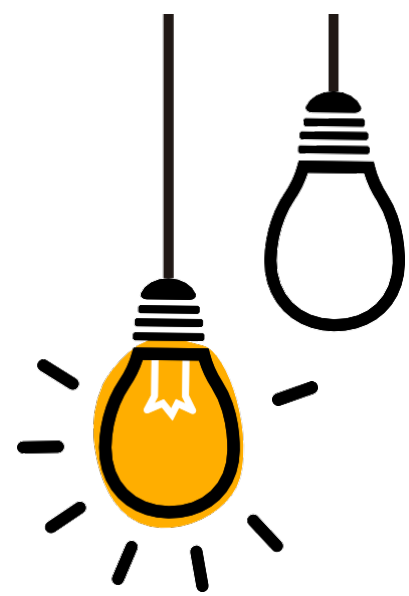
Solution:

- Apply security patches, updates, and software fixes promptly to address known RCE vulnerabilities and prevent attackers from exploiting security flaws to execute arbitrary code or commands on vulnerable systems.

68

Router Exploitation

Router exploitation involves the compromise of network routers, gateways, or access points by attackers to gain unauthorized access, intercept traffic, or launch various types of cyber attacks targeting connected devices and users.



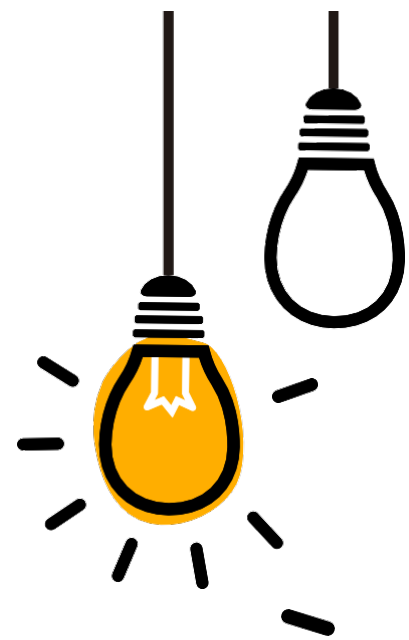
Solution:

- Update router firmware regularly, apply security patches, and change default passwords to mitigate known vulnerabilities and strengthen the security posture of network infrastructure against router exploitation.
- Configure router settings securely, disable unnecessary services, enable firewall protection, and implement strong authentication mechanisms,

69

Bluetooth Attacks

Bluetooth attacks exploit vulnerabilities in Bluetooth-enabled devices, such as smartphones, laptops, or IoT devices, to gain unauthorized access, steal data, or compromise device functionality through wireless communication channels.

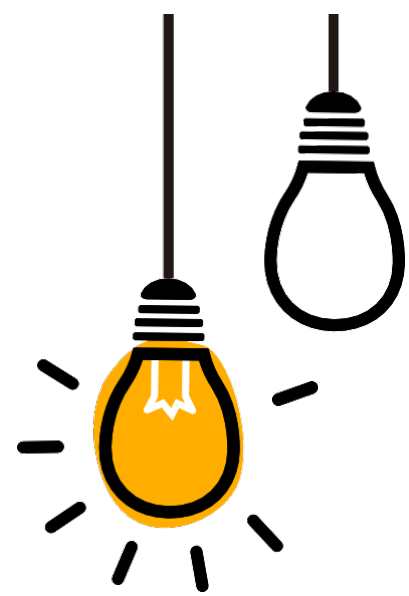


Solution:

- Keep Bluetooth-enabled devices updated with the latest firmware and security patches to mitigate known vulnerabilities and strengthen Bluetooth security against exploitation by attackers.
- Disable Bluetooth functionality when not in use, enable Bluetooth visibility settings judiciously, and avoid pairing with unknown or untrusted devices.

70

Data Interception (Data-in-Transit Attacks)



Data interception, also known as data-in-transit attacks, involves the unauthorized interception, eavesdropping, or monitoring of data as it travels across networks, communication channels, or wireless connections, potentially exposing sensitive information to unauthorized parties.

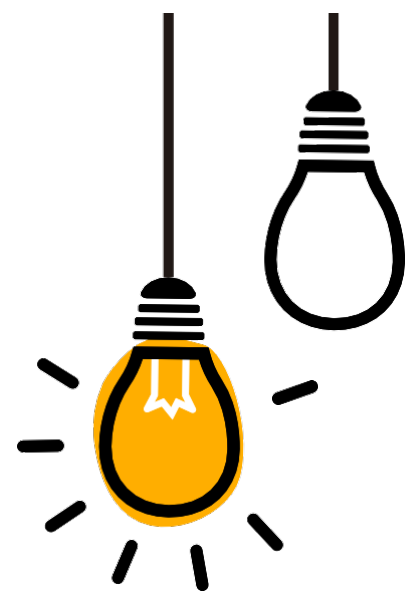
Solution:

- Encrypt data transmissions using strong encryption protocols, such as SSL/TLS for web traffic, IPsec for VPN connections, or end-to-end encryption for messaging applications, to protect data confidentiality and integrity against interception or eavesdropping by attackers.

71

Virtual Private Network (VPN) Exploitation

VPN exploitation involves exploiting vulnerabilities in VPN services or protocols to bypass network security controls, intercept encrypted traffic, or compromise VPN endpoints for unauthorized access or data exfiltration.



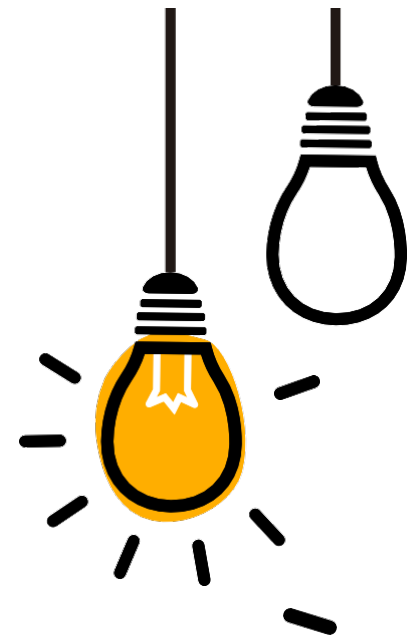
Solution:

- Implement multi-factor authentication (MFA), certificate-based authentication, or strong pre-shared keys (PSKs) to enhance VPN security, prevent unauthorized access, and mitigate the risk of VPN exploitation by adversaries.
- Keep VPN software and firmware updated with the latest security patches and configurations to mitigate known vulnerabilities

72

Malware-as-a-Service (MaaS)

Malware-as-a-Service (MaaS) refers to the commercialization of malware, where cybercriminals offer malicious software, tools, or services for sale or rent to other malicious actors, enabling them to launch cyber attacks without the need for technical expertise or infrastructure.

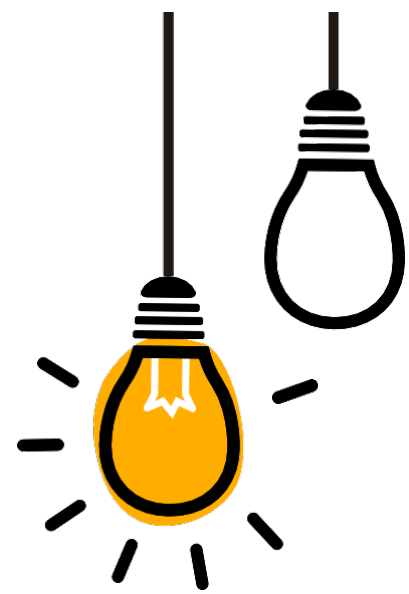


Solution:

- Enhance threat intelligence sharing, collaboration with law enforcement agencies, and public-private partnerships to disrupt and dismantle MaaS operations, identify and apprehend MaaS providers, and mitigate the proliferation of malware-as-a-service offerings in the cybercriminal underground.

73

Browser Extension Vulnerabilities



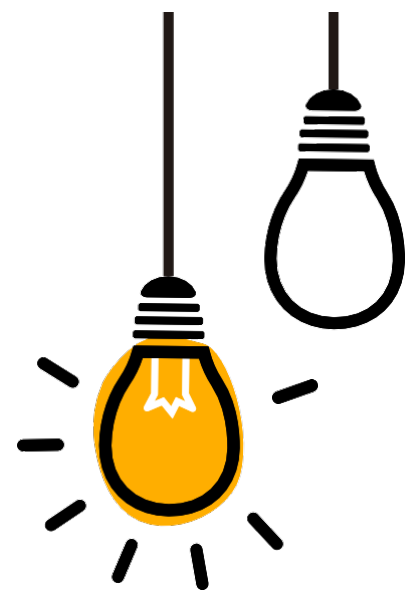
Browser extension vulnerabilities are security weaknesses in third-party browser extensions that can be exploited by attackers to compromise browser security and execute arbitrary code.

Solution:

- Regularly update browser extensions with the latest security patches.
- Limit the use of browser extensions to trusted sources and review extension permissions before installation.
- Implement browser isolation techniques to contain the impact of compromised extensions.

74

Cache Poisoning



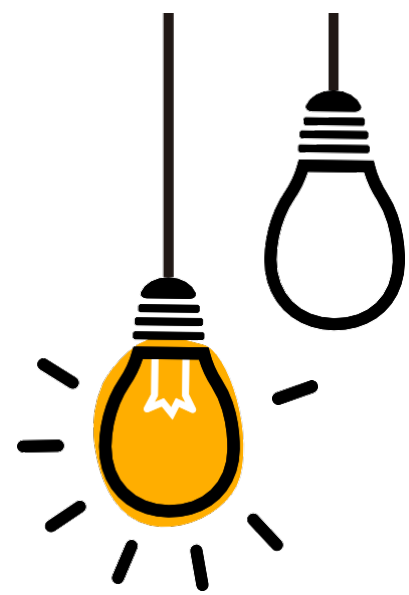
Cache poisoning is a cyber attack where attackers inject false data into a cache to compromise the integrity of cached information or redirect users to malicious websites.

Solution:

- Implement proper input validation and sanitization to prevent injection of malicious content into cache systems.
- Use cryptographic hashing and integrity checks to verify the authenticity and integrity of cached data.
- Regularly monitor cache contents for anomalies and unexpected changes.

75

Caller ID Spoofing



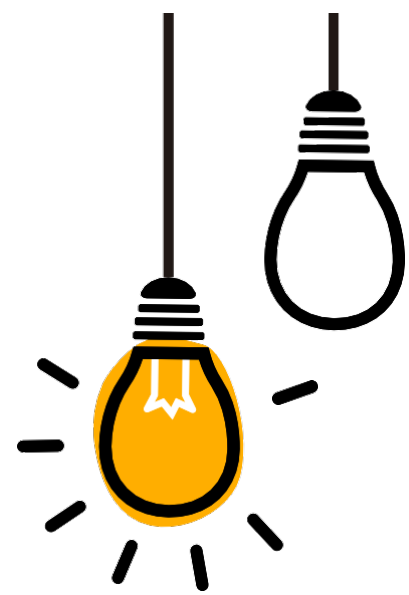
Caller ID spoofing is a technique used by attackers to falsify the caller ID information displayed on a recipient's phone, often to deceive or defraud individuals.

Solution:

- Implement caller authentication mechanisms such as STIR/SHAKEN protocols to verify the authenticity of caller ID information.
- Educate users about the risks of trusting caller ID information and encourage skepticism when receiving unexpected calls.
- Deploy anti-spoofing technologies and call blocking solutions to detect and prevent caller ID spoofing attempts.

76

Camfecting



Camfecting is the unauthorized access and control of a victim's webcam or camera-enabled device by hackers, often for spying or surveillance purposes.

Solution:

- Cover or disconnect webcams when not in use to prevent unauthorized access.
- Regularly update device firmware and security patches to mitigate known vulnerabilities exploited by camfecting attacks.
- Utilize endpoint security solutions with webcam protection features to detect and block unauthorized access attempts.

77

Car Hacking

Car hacking involves exploiting vulnerabilities in modern vehicles' electronic control units (ECUs) or onboard computer systems to gain unauthorized access and manipulate vehicle functions.

Solution:

- Implement secure coding practices and conduct security assessments of vehicle firmware and software.
- Segment vehicle networks and implement network segmentation to isolate critical systems from non-essential functions.
- Deploy intrusion detection and prevention systems (IDPS) to detect and block suspicious activities or unauthorized access attempts in vehicle networks.

78

Certificate Transparency Abuse

Certificate transparency abuse refers to the exploitation of weaknesses in certificate transparency logs to issue fraudulent digital certificates or evade detection.

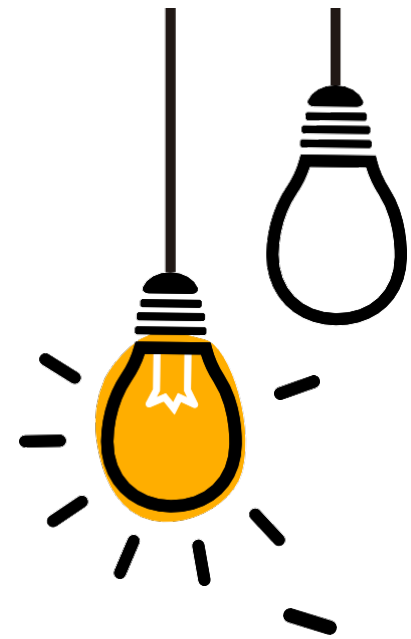
Solution:

- Monitor certificate transparency logs for suspicious or unauthorized certificate issuance activities.
- Enforce strict certificate validation policies and reject certificates not compliant with certificate transparency requirements.
- Educate CAs & domain owners about the importance of maintaining transparency logs and promptly reporting anomalies or unauthorized certificate issuances.

79

Clipboard Hijacking

Clipboard hijacking is a type of cyber attack where malware or malicious scripts intercept and modify clipboard content, often to steal sensitive information such as passwords or cryptocurrency addresses



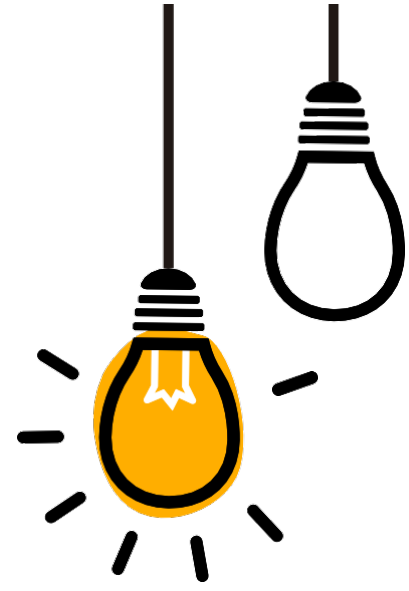
Solution:

- Use endpoint security solutions with clipboard monitoring capabilities to detect and block malicious clipboard manipulation.
- Avoid copying sensitive information to the clipboard when unnecessary and utilize secure password managers or cryptographic solutions for sensitive data handling.
- Regularly scan devices for malware and keep security software updated to prevent clipboard hijacking infections.

80

Click Injection Fraud

Click injection fraud is a form of mobile ad fraud where attackers manipulate mobile apps to generate fake ad clicks attributed to legitimate user interactions, leading to financial losses for advertisers.

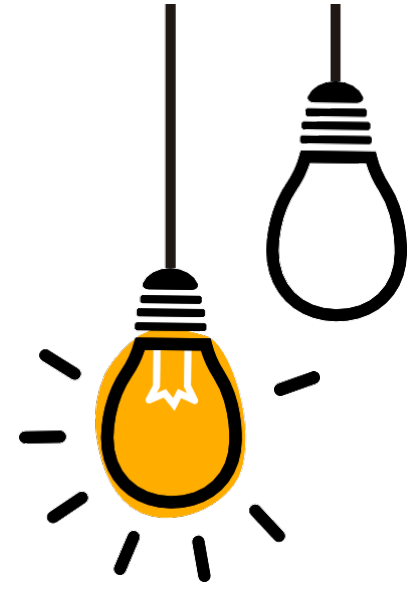


Solution:

- Employ fraud detection algorithms to identify abnormal click patterns and flag suspicious activities indicative of click injection fraud.
- Implement secure app development practices to prevent attackers from exploiting vulnerabilities in mobile apps to manipulate ad clicks.

81

Command Injection



Command injection is a type of cyber attack where attackers exploit vulnerabilities in web applications or operating systems to execute arbitrary commands on the underlying system.

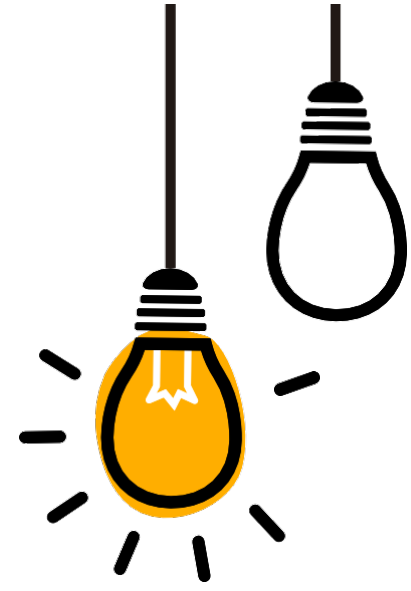
Solution:

- Implement input validation and output encoding techniques to sanitize user inputs and prevent malicious command injection.
- Utilize parameterized queries and prepared statements to interact with databases securely and mitigate the risk of SQL injection attacks, a common vector for command injection.
- Regularly update software and patch known vulnerabilities to prevent attackers from exploiting outdated or unpatched systems.

82

Container Escapes

Container escapes occur when attackers exploit vulnerabilities in containerization platforms or misconfigurations to break out of containerized environments and gain unauthorized access to the underlying host system.



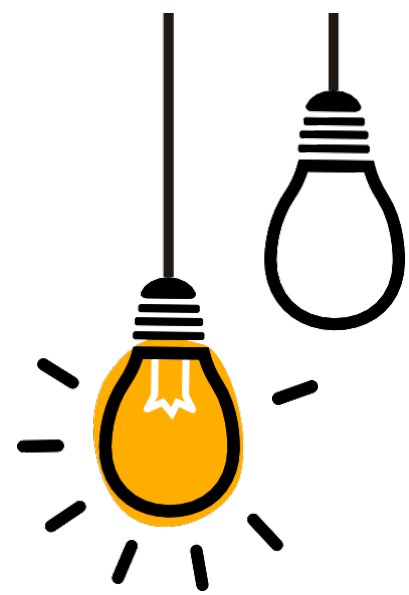
Solution:

- Harden container configurations and limit privileges to reduce the attack surface and mitigate the risk of container escapes.
- Utilize container security tools and runtime protection mechanisms to monitor container activities and detect anomalous behavior indicative of escape attempts.

83

Content Security Policy (CSP) Bypass

Content Security Policy (CSP) bypass is a technique used by attackers to circumvent security policies implemented by web applications, allowing them to execute malicious scripts or inject unauthorized content.



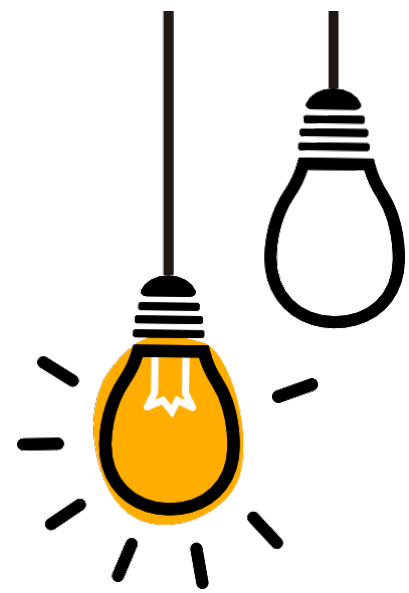
Solution:

- Implement a robust CSP with strict directives to control the sources from which content can be loaded and executed within web pages.
- Utilize subresource integrity (SRI) to verify the integrity of external resources and prevent unauthorized modifications or tampering.

84

Data Destruction Attacks

Data destruction attacks involve the deliberate destruction or deletion of data assets, rendering them permanently inaccessible or irrecoverable, often causing significant disruption to businesses or individuals.



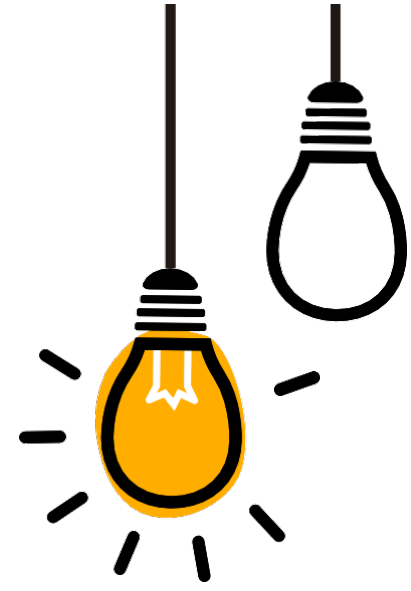
Solution:

- Implement data backup and disaster recovery strategies to regularly backup critical data and systems and facilitate rapid recovery in the event of a data destruction attack.
- Utilize access controls and encryption to protect sensitive data from unauthorized access or tampering by malicious actors.
- Deploy endpoint security solutions with DLP capabilities to monitor and prevent unauthorized attempts

85

Dark Web Marketplaces

Dark web marketplaces are hidden online platforms where illegal goods and services, including drugs, stolen data, malware, and hacking tools, are bought and sold anonymously using cryptocurrencies.



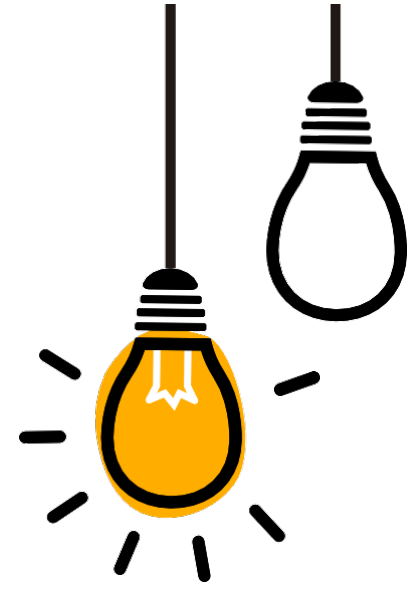
Solution:

- Collaborate with law enforcement agencies and cybersecurity experts to monitor and investigate dark web activities and identify individuals or groups involved in illegal trading.
- Educate users about the risks associated with accessing or transacting on dark web marketplaces and discourage engagement in illegal activities.

86

Digital Certificate Spoofing

Digital certificate spoofing involves the creation or manipulation of digital certificates to impersonate legitimate entities or websites, allowing attackers to conduct phishing, man-in-the-middle, or other malicious activities.



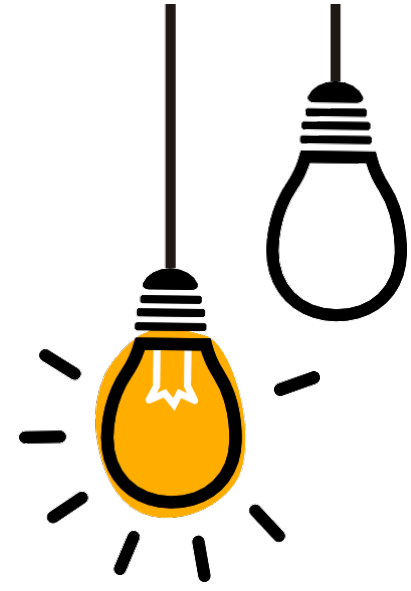
Solution:

- Deploy certificate revocation mechanisms such as certificate revocation lists (CRLs) or online certificate status protocol (OCSP) to verify the validity of digital certificates and detect spoofed certificates.
- Utilize certificate transparency logs and monitoring tools to detect unauthorized certificate issuances or suspicious changes to certificate metadata.

87

DNSSEC Misconfigurations

DNSSEC misconfigurations occur when domain name system security extensions (DNSSEC) are improperly configured, leading to vulnerabilities that could be exploited by attackers to conduct DNS spoofing or cache poisoning attacks.

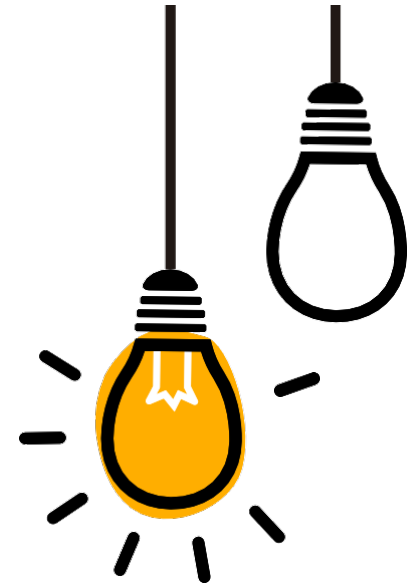


Solution:

- Implement proper DNSSEC deployment practices and adhere to DNSSEC configuration best practices provided by authoritative bodies and standards organizations.
- Regularly audit DNSSEC configurations and monitor DNS traffic for signs of DNSSEC-related anomalies or security incidents.

88

Domain Generation Algorithm (DGA) Attacks



Domain Generation Algorithm (DGA) attacks involve the use of algorithms to generate a large number of domain names that malware can use to establish command and control (C&C) communication channels with botnets, making it difficult for security systems to block or detect malicious traffic.

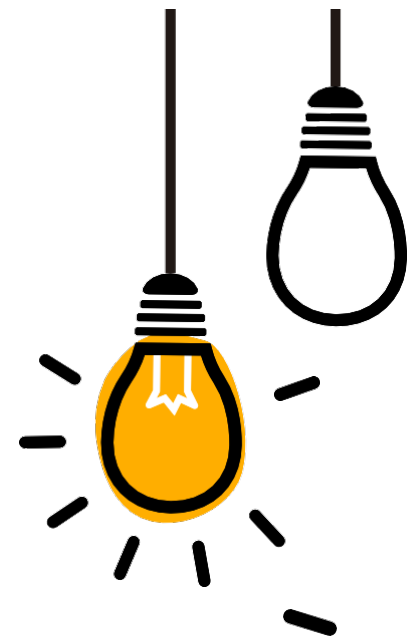
Solution:

- Implement DNS sinkholing techniques to redirect traffic from known malicious domains to a controlled server for analysis and mitigation.

89

Email Spoofing

Email spoofing is a technique used by attackers to forge the sender's email address, making it appear as if the email originated from a legitimate source, often to deceive recipients into divulging sensitive information or performing malicious actions.



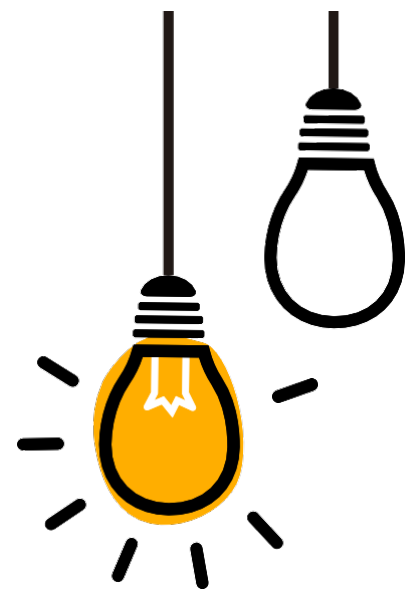
Solution:

- Implement email authentication mechanisms such as SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance) to verify the authenticity of email senders and detect spoofed emails.
- Utilize email filtering solutions and anti-phishing tools

90

Emulation Detection Evasion

Emulation detection evasion refers to techniques used by malware to detect and evade analysis environments, such as sandboxes or virtual machines, by identifying specific emulation artifacts or behaviors and altering their execution to avoid detection or analysis.

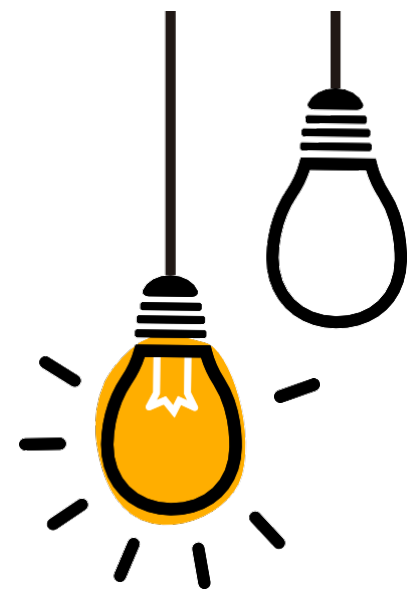


Solution:

- Employ dynamic analysis techniques such as memory introspection and code emulation to detect and analyze malware behavior without relying solely on emulation environments.
- Implement stealthy emulation environments that simulate realistic user interactions and system behaviors to deceive malware into revealing its true intent.

91

Exploitation of Zero-Day Vulnerabilities



Exploitation of zero-day vulnerabilities involves attackers exploiting previously unknown security vulnerabilities in software or hardware systems to gain unauthorized access, execute arbitrary code, or perform other malicious actions before vendors release patches or security updates.

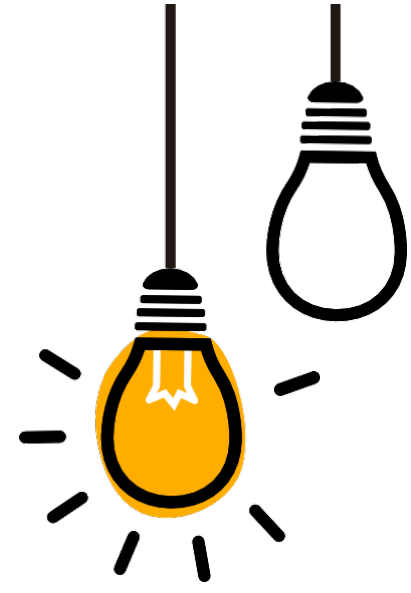
Solution:

- Implement intrusion detection and prevention systems (IDPS) to detect and block suspicious network traffic associated with zero-day exploitation attempts.
- Utilize threat intelligence feeds and vulnerability scanning tools to identify systems potentially vulnerable to zero-day exploits and prioritize patching or mitigation efforts.

92

GPS Spoofing

GPS spoofing is a cyber attack where attackers manipulate GPS signals to deceive GPS receivers, causing them to provide inaccurate location information, which can lead to navigation errors, disruptions in critical infrastructure, or physical harm.

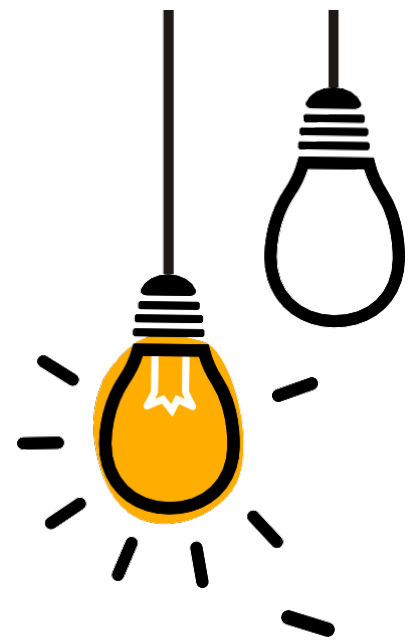


Solution:

- Implement cryptographic authentication and integrity verification mechanisms in GPS signals to detect and prevent GPS spoofing attacks.
- Utilize GPS receivers with anti-spoofing capabilities and multi-constellation support to improve resilience against signal manipulation and interference.

93

HTTP Parameter Pollution (HPP)



HTTP Parameter Pollution (HPP) is a web security vulnerability where attackers manipulate HTTP request parameters to bypass input validation mechanisms, inject malicious payloads, or alter application behavior, leading to various attacks such as SQL injection or cross-site scripting (XSS).

Solution:

- Implement server-side input validation and sanitization to ensure that only expected and properly formatted parameters are processed by web applications.
- Utilize secure coding practices and frameworks that automatically handle parameter encoding and validation to mitigate the risk of HPP vulnerabilities.

94

Insecure Deserialization

Insecure deserialization is a vulnerability where untrusted data is deserialized by an application, potentially leading to remote code execution, denial of service (DoS), or data tampering attacks if the deserialization process is not properly secured.

Solution:

- Implement input validation and integrity checks on serialized data to prevent tampering or exploitation of deserialization vulnerabilities.
- Utilize serialization libraries and frameworks with built-in security features such as whitelisting or sandboxing to mitigate the risk of insecure deserialization.

95

Internet Routing Attacks

Internet routing attacks involve the manipulation of routing protocols or the Border Gateway Protocol (BGP) to redirect traffic, hijack IP addresses, or disrupt network connectivity, potentially leading to service outages, data interception, or traffic interception.

Solution:

- Implement BGP security mechanisms such as Resource Public Key Infrastructure (RPKI) and BGP Route Origin Validation (ROV) to authenticate route announcements and prevent route hijacking.
- Utilize network monitoring tools to detect anomalies or suspicious routing behavior and respond promptly to mitigate the impact of routing attacks.

96

IoT Ransomware

IoT ransomware is a type of malware that targets Internet of Things (IoT) devices, encrypting device data or locking device functionality, and demanding a ransom payment in exchange for decryption keys or device control.

Solution:

- Segment IoT networks from critical infrastructure and enterprise networks to contain the spread of ransomware infections and limit the impact on business operations.
- Regularly update IoT device firmware and apply security patches provided by device manufacturers to mitigate known vulnerabilities exploited by ransomware.

97

IoT Replay Attacks

IoT replay attacks involve capturing and replaying legitimate communication between IoT devices and backend servers to impersonate authorized users, bypass authentication mechanisms, or perform unauthorized actions.

Solution:

- Implement secure communication protocols such as Transport Layer Security (TLS) with mutual authentication to prevent replay attacks and ensure the integrity and confidentiality of IoT device communications.
- Utilize time-based or nonce-based authentication tokens to prevent replay of outdated or previously used authentication credentials.

98

Key Recovery Attacks

Key recovery attacks involve attempts to retrieve encryption keys from compromised or insecurely stored key repositories, enabling attackers to decrypt sensitive data, impersonate legitimate users, or perform unauthorized actions.

Solution:

- Implement strong encryption algorithms and key management practices to protect encryption keys and prevent unauthorized access or disclosure.
- Utilize hardware security modules (HSMs) or trusted execution environments (TEEs) to securely store encryption keys and perform cryptographic operations, reducing the risk of key recovery attacks.

99

Live Migration Attacks

Live migration attacks target virtualized environments where live migration technologies are used to move virtual machines (VMs) between physical hosts, exploiting vulnerabilities in migration protocols or hypervisor configurations to gain unauthorized access or disrupt VM operations.

Solution:

- Implement network segmentation and access controls to restrict live migration traffic and prevent unauthorized VM migrations between hosts.
- Utilize encryption and authentication mechanisms to secure live migration traffic and protect VM images and data during migration operations.

100

Memory Scraping Malware

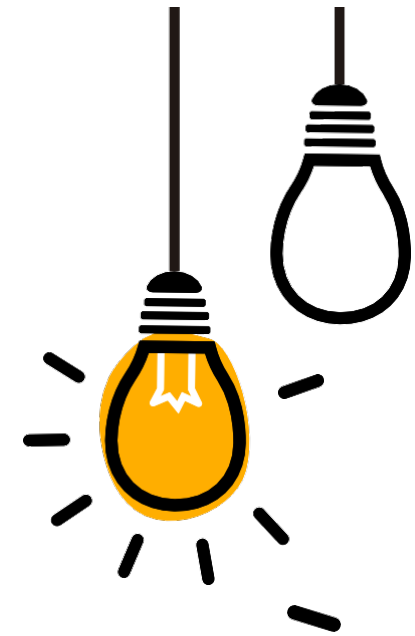
Memory scraping malware, also known as RAM scrapers, target the volatile memory (RAM) of compromised systems to harvest sensitive data such as credit card numbers, passwords, or encryption keys from running processes or application memory spaces.

Solution:

- Implement endpoint security solutions with memory protection features to detect and block memory scraping malware infections and prevent unauthorized access to sensitive data in system memory.
- Utilize application whitelisting and code signing to prevent the execution of unauthorized or untrusted processes that may attempt to scrape memory contents.

100
Topics Covered

5G Network Vulnerabilities
Advanced Persistent Threats (APTs)
Adversarial Machine Learning Attacks
AI-Powered Cyber Attacks
AI-Powered Deepfakes
App Store Fraud
Automated Brute Force Attacks
Backdoor Attacks
Biometric Spoofing
Blockchain Vulnerabilities
Bluetooth Attacks
Bluetooth Impersonation Attacks
Browser Extension Vulnerabilities
Browser-based Cryptojacking
Business Email Compromise (BEC)
Cache Poisoning
Caller ID Spoofing
Camfecting
Car Hacking
Certificate Transparency Abuse
Click Injection Fraud
Clipboard Hijacking
Cloud Service Misconfiguration
Command Injection
Container Escapes
Content Security Policy (CSP) Bypass
Credential Phishing
Credential Stuffing Attacks
Credential Theft via Keylogging
Cross-Site Request Forgery (CSRF)
Cross-Site Scripting (XSS) Attacks
Cryptojacking
Cyber Espionage
Dark Web Marketplaces
Data Breaches
Data Destruction Attacks
Data Exfiltration through Stenography
Data Interception
Data Leakage
Data Manipulation Attacks
Deep Packet Inspection (DPI) Evasion
Digital Certificate Spoofing
Distributed Denial of Service (DDoS) Attacks
DNS Hijacking
DNS Tunneling
DNSSEC Misconfigurations
Domain Generation Algorithm (DGA) Attacks
Eavesdropping
Email Spoofing
Emulation Detection Evasion
Exploitation of Zero-Day Vulnerabilities
File Encryption Ransomware
File Encryption Trojans
Fileless Malware
Firmware Vulnerabilities
Formjacking Attacks
GPS Spoofing
HTTP Parameter Pollution (HPP)
Identity Theft
Insecure Deserialization
Insider Threats
Insufficient Security Patching
Internet Routing Attacks
IoT Botnets
IoT Firmware Vulnerabilities
IoT Ransomware
IoT Replay Attacks
Key Recovery Attacks
Live Migration Attacks
Logic Bombs
Malvertising
Malware
Malware-as-a-Service (MaaS)
Man-in-the-Middle (MitM) Attacks
Memory Scraping Malware
Mobile App Spoofing
Mobile Malware
Phishing Attacks
Physical Attacks on Infrastructure
Ransomware
Remote Code Execution (RCE) Vulnerabilities
Rogue Software
Router Exploitation
Side Channel Attacks
SIM Swapping
Simultaneous Multithreading (SMT) Side-Channel Attacks
Smart Contract Vulnerabilities
Social Engineering Attacks
Supply Chain Attacks
Supply Chain Compromise
Typosquatting Attacks
USB Rubber Ducky Attacks
USB-Based Attacks
Virtual Private Network (VPN) Exploitation
Voice Assistant Exploitation
Voice Phishing (Vishing)
Watering Hole Attacks
Whaling Attacks
Zero-Click Exploits
Zero-Day Exploits



Was this helpful to you?

SCAN NOW TO READ MORE

Be sure to save this post
for later reading

Follow us for more: