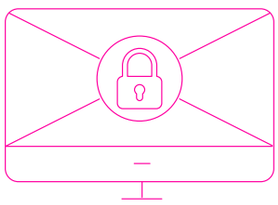
cynet

Top 10 Cyber Threats

Here are the top threats we expect to see in 2023

REQUEST A FREE TRIAL

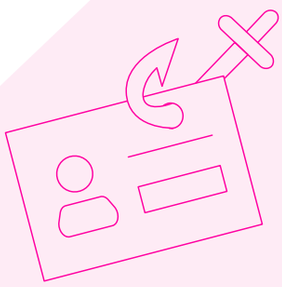


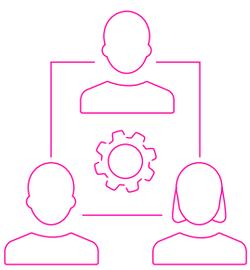
1: Ransomware Extortions

Ransomware encrypts files on a device and then demands a ransom for the encryption key. Criminals typically use multi-stage attacks to gain access to the corporate environment, escalate privileges, move laterally and ultimately deploy ransomware across multiple computers on the corporate network.

2: Social Engineering / Phishing

Tricking users into divulging credentials, click on malicious links or opening weaponized documents continues to be the primary means of gaining access to computer and networks. This is usually done via email, but can also be done via social networks, mobile SMS, games, and other channels.



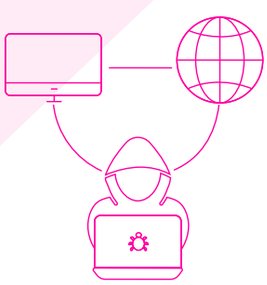


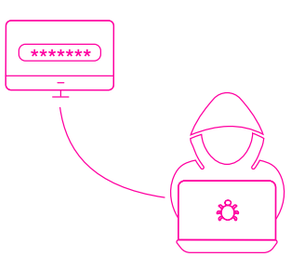
3: Lateral Movement

Gaining initial access to a device or network is the starting point of an advanced persistent threat (APT) attack. Once initial access is gained, the attacker then attempts to quietly move through the network to seek out more privileged accounts and valuable corporate data.

4: Man-in-the-Middle (MitM) Attack

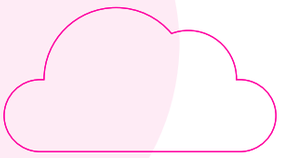
MitM attacks intercept and alter the communication between parties. This can be used to steal sensitive information, employ social engineering, or inject malicious code into the communications.





5: Account Takeover

When attackers gain control of an online account using stolen credentials, it is known as an account takeover. The attacker can use social engineering or malware to steal the credentials directly from the user or acquire them from another criminal.

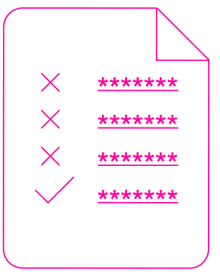


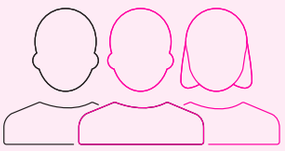
6: Cloud & SaaS Misconfiguration Vulnerabilities

Cloud and SaaS applications provide tremendous benefits and shift some security responsibilities to the application providers. Each app can have hundreds of settings, are accessed by multiple employees with different levels of privileges and are continuously changing. Cybercriminals exploit misconfigurations to gain access to these valuable targets.

7: Brute Force

These are generally known as trial-and-error attacks where the attacker uses multiple usernames and/or passwords until the correct one is found. Sometimes this can take the form of credential stuffing where attackers use credentials from one breach to gain access to another account.



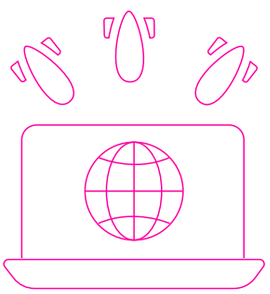


8: Insider Threats

Rogue employees, vendors and partners can leverage their legitimate access privileges to steal data and do harm, purposely or through negligence. Sometimes employees are approached by 3rd parties to steal valuable corporate information. Insider threats can take the form of espionage, terrorism, blackmail and sabotage.

9: Supply Chain Attacks

Criminals can gain access to your systems by successfully infiltrating your 3rd party providers or partners with access to your systems and data. Because your providers and partners are trusted, it's easier for attackers to slip through your defenses masquerading as legitimate users. Attackers can also leverage trusted 3rd parties to deploy malware in trusted applications.



10: DoS and DDoS

Attackers overload web servers with traffic so it becomes inaccessible to legitimate users. A Denial of Service (DOS) attack comes from a single location, whereas a Distributed Denial of Service (DDoS) attack comes from multiple locations, making it much more difficult to detect and block. Sometimes these attacks are used to distract the security team while other attacks are taking place.

REQUEST A FREE TRIAL