MOST COMMON ATTACK VECTORS OF 2019

When it comes to data breaches, 2019 was neither the best of times nor the worst of times. It was more a sign of the times. Billions of people were affected by data breaches in 2019, with 4.1 billion records exposed in the first half of 2019 alone. The losses surpassed tens of millions of dollars.

SECURITY TERMINOLOGY

ATTACK VECTOR

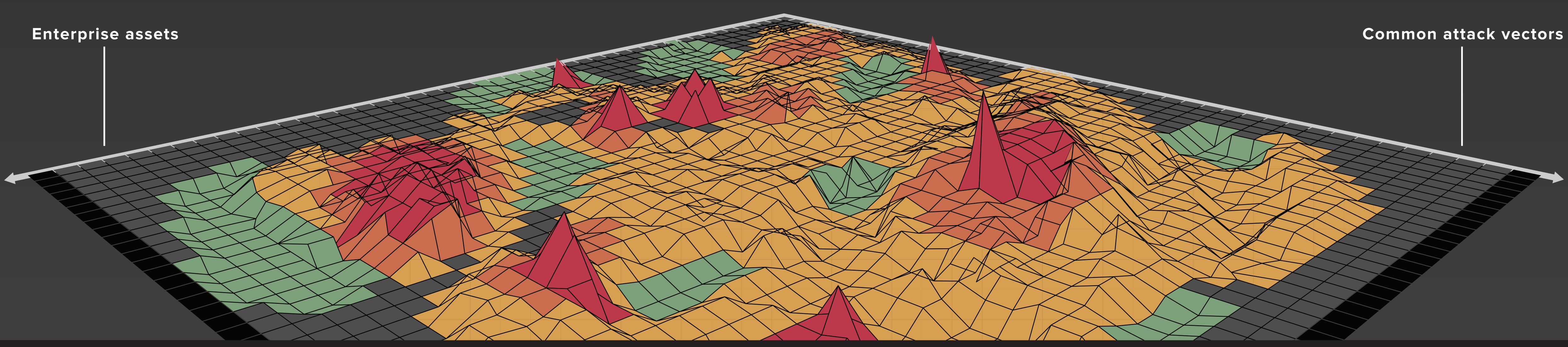
The method or way by which an adversary can breach an entire network/system by exploiting system vulnerabilities or weaknesses.

ATTACK SURFACE

All of the points on a network where attacks can occur.. This is where an unauthorized person (the "attacker") can try to manipulate or extract data using a myriad of breach methods.

SECURITY BREACH

Any security incident in which sensitive, protected, or confidential data is accessed or stolen by an unauthorized party, jeopardizing an organization's brand, customers, and assets.



COMPROMISED CREDENTIALS

User credentials, such as usernames and passwords, are exposed to unauthorized entities, typically when unsuspecting users fall prey to phishing attempts and enter their login credentials on fake websites.

Privileged access credentials, which give administrative access to devices and systems, typically pose a higher risk to the enterprise than consumer credentials.

TAKE ACTION

- Enact effective password policies that ensure suitable password strength.
- Do not reuse the same password to access multiple apps and systems.
- Use two-factor authentication.

WEAK AND STOLEN CREDENTIALS

Weak passwords and password reuse make credential exposure a gateway for initial attacker access and propagation. Malware attacks such as Mirai highlight this threat not only for managed devices but also IoT connected devices.

Apps and protocols sending login credentials over your network pose a significant security threat. An attacker connected to your network can easily locate and utilize these credentials for lateral movement.

TAKE ACTION

- Identify instances of password re-use and sharing across your enterprise.
- Track employee password hygiene to pinpoint high risk users and their devices.

MALICIOUS INSIDERS

A malicious insider is an employee who exposes private company information and/or exploits company vulnerabilities. Malicious insiders are often unhappy employees.

Users with access to sensitive data and networks can inflict extensive damage through privileged misuse and malicious intent.

TAKE ACTION

- Identify instances of password re-use and sharing across your enterprise.
- Track employee password hygiene to pinpoint high risk users and their devices.

MISSING/POOR ENCRYPTION

Data encryption translates data into another form to protect digital data confidentiality and once encrypted, it is accessible only by using a secret key. Strong encryption must be applied to data at rest, in-motion, and where suitable, in-processing.

Missing/poor encryption leads to sensitive information including credentials being transmitted either in plaintext or using weak cryptographic ciphers or protocols.

TAKE ACTION

- Don't rely solely on weak encryption or assume that following compliance means that the data is securely encrypted.
- Ensure that sensitive data is encrypted at rest, in-transit, and in processing.

MISCONFIGURATION

Misconfiguration is when there is an error in system configuration.

Misconfigured devices and apps present an easy entry point for an attacker to exploit.

TAKE ACTION

- Put procedures and systems in place that tighten your configuration process and use automation wherever possible.
- Monitor application and device settings and compare these to recommended best practices.

RANSOMWARE

Ransomware is a form of cyber-extortion in which users are unable to access their data until a ransom is paid. Users are shown instructions for how to pay a fee to get the decryption key.

The costs of a ransomware attack can range from a few hundred dollars to thousands, payable to cybercriminals in Bitcoin.

TAKE ACTION

- Keep your operating system patched and up to date.
- Don't install software or give it administrative privileges unless you know exactly what it is and what it does.

PHISHING

Phishing is a cybercrime tactic in which the targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

Phishing is one of the most effective social engineering attack vectors.

TAKE ACTION

- Measure web browsing and email click-through behavior for users and devices to get valuable risk insights.
- When in doubt, don't click.

TRUST RELATIONSHIPS

Trust relationships refer to a certain level of trust that exists between users and systems. The two domains in a trust relationship are the trusted domain (the domain that authenticates the user the first time), and the trusting domain (the domain that relies on the trusted domain to authenticate users and gives access to its resources without re-authenticating the user).

A common breach scenario example is when credentials are cached on the trusted client, which then gets breached, wreaking havoc.

TAKE ACTION

- Manage trust relationships to help you limit or eliminate the impact or damage an attacker can inflict.

Balbix

Learn more about most common breach methods

Read about the 10 common blind spots in your cybersecurity posture