MEGHALAYA RURAL BANK
Scheduled Bank Owned by Government

Volume 3 Issue 6

Date: 16-06-2026

Cybersecurity Digest

Bi-Weekly update by the O/o CISO of Meghalaya Rural Bank

# Attack Vector

To anyone concerned with cybersecurity, understanding what an attack vector is and how it works is crucial. An attack vector is the path or entry point that an attacker uses to gain unauthorized access to your system, network, or data. Once you define an attack vector, you identify the path or method that a threat actor could use to breach your system's security. Then you can take action to mitigate the potential security risks.

There are many different attack vectors, including phishing, malware, web application attacks, and even physical access to your server. Malicious actors might use a combination of attack vectors in order to disrupt your business systems, steal data, and/or cause data breaches.

**How Do Hackers Exploit Attack Vectors?**

Hackers use multiple threat vectors to exploit vulnerable systems, attack devices and networks, and steal data from individuals. There are two main types of hacker vector attacks: passive attacks and active attacks.

**Passive attack**

A passive attack occurs when an attacker monitors a system for open ports or vulnerabilities to gain or gather information about their target. Passive attacks can be difficult to detect because they do not involve altering data or system resources. Rather than cause damage to an organization's systems, the attacker threatens the confidentiality of their data.

**Active attack**

An active attack vector is one that sets out to disrupt or cause damage to an organization's system resources or affect their regular operations. This includes attackers launching attacks against system vulnerabilities, such as denial-of-service (DoS) attacks, targeting users' weak passwords, or through malware and phishing attacks.

## Some Common Attack Vectors in Cybersecurity

**Phishing:** It is a type of cyber attack in which user or victim is duped to click on harmful sites which are crafted in a way to feel authentic site. The most common mode of phishing is by sending spam emails that appear to be authentic and thus, taking away all credentials from the victim.

**Malware:** Malware is short for malicious software and refers to any software that is designed to cause harm to computer systems, networks or users. Malware are designed to gain access to computer systems, generally for the benefit of some third party, without the user's permission.

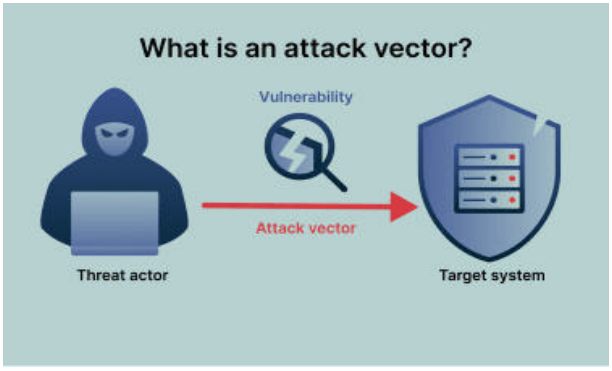
**MITM:** In Man-in-the-Middle (MITM) attacks there is an unwanted proxy in the network intercepting and modifying the responses. This proxy is called a Man in the middle.

**Denial of Service:** Denial-of-Service (DoS) is a cyber-attack on an individual Computer or Website with the intent to disrupt an organization's network operations by denying access to its users. It is done by flooding the targeted machine or resource with surplus requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

**Insider Attacks:** Insider Threats or Insider Attack are caused by insiders like former employees, business partners, contractors or security admins having access to the confidential information previously.


**Ransomware:** Ransomware is a form of malicious software that prevents computer users from accessing their data by encrypting it.

**SQL Injection:** SQL injection is a code injection technique attackers use to gain unauthorized access to a database by injecting malicious SQL commands into web page inputs.




**Why are Attack Vectors Exploited by Attackers**

Cybercriminals can make money from attacking your organization's software systems, such as stealing credit card numbers or online banking credentials. However, there are other more sophisticated ways to monetize their actions that aren't as obvious as stealing money.

Attackers may infect your system with malware that grants remote access to a command and control server. Once they have infected hundreds or even thousands of computers they can establish a botnet, which can be used to send phishing emails, launch other cyber attacks, steal sensitive data, or mine cryptocurrency.

Another common motivation is to gain access to personally identifiable information (PII), healthcare information, and biometrics to commit insurance fraud, credit card fraud or illegally obtain prescription drugs.

Competitors may employ attackers to perform corporate espionage or overload your data centers with a Distributed Denial of Service (DDoS) attack to cause downtime, harm sales, and cause customers to leave your business.

Money is not the only motivator. Attackers may want to leak information to the public, embarrass certain organizations, grow political ideologies, or perform cyber warfare on behalf of their government like the United States or China.

**How to Defend Against Common Attack Vectors**

To address common attack vectors, security controls must spread across the majority of the attack surface. The process begins by identifying all possible entry points into your private network - a delineation that will differ across all businesses.

The following cyber defense strategies will help you block frequently abused entry points and also highlight possible regions in your ecosystem that might be housing attack vectors.

**Create secure IoT credentials** - Most IoT devices still use their predictable factory default login credentials, making them prime targets for DDoS attacks.

**Use a password manager** - Password managers ensure login credentials are strong and resilient to brute force attacks.

**Educate employees** - To prevent staff from being a victim of social engineering and phishing tactics, they need to be trained on how to identify and report potential cybercriminal activity. Humans will always be the weakest points in every security program.

**Identify and shutdown data leaks** Most businesses are unknowingly leaking sensitive data that could facilitate data breaches. A data leak detection solution will solve this critical security issue.

**Detect and remediate all system vulnerabilities** - This should be done for both the internal and external vendor networks. Cyber risk remediation software can help you do this.

**Keep antivirus software updated** - Updates keep antivirus software informed of the latest cyber threats roaming the internet.

**Keep third-party software regularly updated** - Software updates contain critical patches for newly discovered attack vectors. Many cyber attackers have achieved success by abusing known vulnerabilities in out-of-date software.