ARTICLE :

Four Reasons DDoS Attacks Target Banks and E-Commerce Sites

Banks and e-commerce sites have long been the target of malicious cyberattacks. Though cybersecurity efforts continue to improve, attempts to stay ahead of newer, emerging threats is an ongoing process.

Some of the reasons that attackers target banks and e-commerce sites might seem obvious, but some are a little more subtle. In many cases, you might wonder, "why me?" but the rationale might not be what you think.

Attacker Motivation #1: Extortion
Extortion, at least in the realm of DDoS attacks, is not aimed at stealing personal information, it's more about shutting down online systems and blocking customer access to online resources.

Attacker Motivation #2: Hacktivism
Hacktivist groups like Anonymous wage campaigns against major banks and corporations like Exxon Mobil, BP, or any corporation that operates under controversy. In most cases, the hackers are using these platforms to further their viewpoints.

Today, most hacktivist efforts center around a government, an organization, or a country that is experiencing conflict. They cause destruction and then leverage the news media to bring attention to their cause.

Attacker Motivation #3: Showcase Skillset
Hackers frequently use attacks as a way to up their status in the hacker community. They show off their prowess on the dark web to market themselves to various factions who may or may not have a malicious agenda.

On one side of the coin, the attacker might simply be trying to call attention to vulnerabilities in the system, ostensibly to help the company in question. In other situations, the motivation could be to promote their skills to other malicious actors as the "business" of DDoS can be very profitable.

Attacker Motivation #4: Disgruntled IT Employees
Not every IT employee that is fired decides to wage cyberwar against their former employer, but some will. Revenge is the primary motive. Some threats come with specific demands, some are merely to upset the status quo, but the reality is that these people often have access to a lot of information and systems that can be manipulated for various purposes.

One of the most significant examples in recent years is John Kelsey Gammell, who waged a year-long attack against Washburn Computer Group as well as several banks and two other companies at which he had been previously employed.

How You Can Protect Your Company and Its Systems
The fear of external unknowns and internal cybersecurity vulnerabilities is genuine. When your system is down, it can derail your IT team for weeks and seriously impact your business continuity.

How is your company protecting itself against cyberattacks? Are you prepared to respond? Learn more about DDoS Risk Assessments today: reach out to speak to a security specialist about what you can do.