CyberVigilance™

A PROTEUS TECHNOLOGIES CYBER SOLUTION

#ACTB4URHACKD

"It's amazing how much manipulation is going on in parasites" - Jacob Koella

Advanced Persistent Threats (APTs) are a parasitical form of cyberattack that infiltrate systems to establish a foothold, then stealthily exfiltrate data and intellectual property over an extended period of time. Attackers use these capabilities to compromise and eavesdrop on targeted systems.

Slow and Low That Is the Tempo

In a simple attack, an attacker tries to get in and out of the targeted infrastructure as quickly as possible in order to avoid detection by the network's intrusion detection system (IDS). In an APT attack, however, the goal is not to get in and out but to achieve ongoing access.

Once the attacker is on the system, the persistence strategy is one of "slow and low" to move laterally through the network and blend in with normal traffic allowing continuous monitoring and data extraction while avoiding detection. No single layer of intrusion prevention or anomaly detection is enough to stop a determined attacker and multiple layers of security must be employed to defend against today's attacks and those that have yet to appear.

Act Before You're Hacked

Contact PROTEUS at CV@proteuseng.com to find out how our CyberVigilance™ services can help YOU deploy an effective approach to defend against APTs that includes detection capabilities, an incident response and recovery plan, as well as routine security awareness and training.

PROTEUS TECHNOLOGIES
Outsmart.