# The Changing Threat Landscape: Criminals Leveraging Both Broad-based and Targeted Attacks

## Security Fundamentals

- Use Strong Passwords
- Apply Updates Regularly
- Use Anti-Virus Software
- Consider the Cloud
- Invest in Newer Products

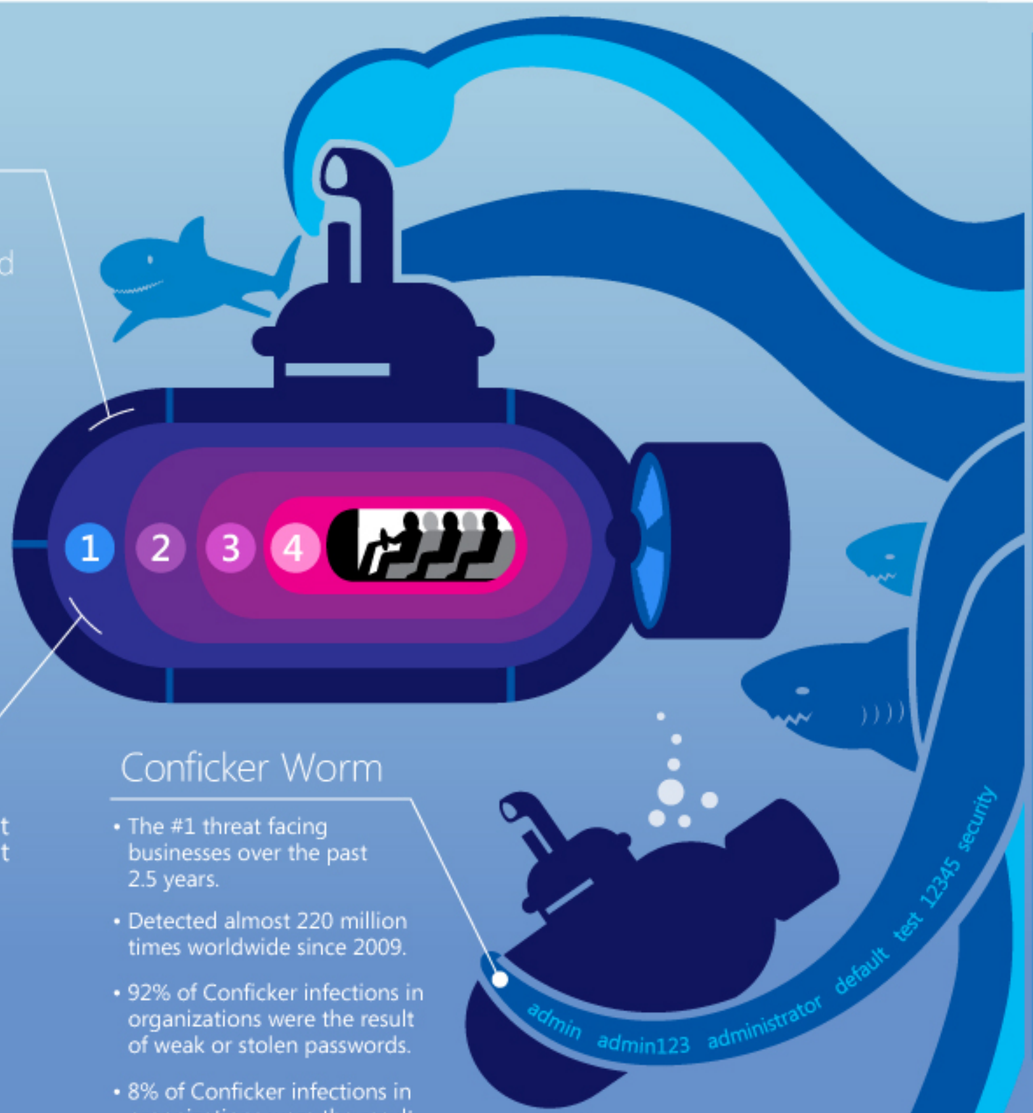
## Holistic Approach

**1 Prevention**
Ensure you have implemented the security fundamentals.

**2 Detection**
Regularly monitor and conduct advanced analysis within your organization to identify threats.

**3 Containment**
If the attacker is successful at breaching, contain the threat so that it does not spread.

**4 Recovery**
Have a well-conceived recovery plan supported by suitably skilled response capability.




## Conficker Worm

- The #1 threat facing businesses over the past 2.5 years.
- Detected almost 220 million times worldwide since 2009.
- 92% of Conficker infections in organizations were the result of weak or stolen passwords.
- 8% of Conficker infections in organizations were the result of vulnerabilities for which an update exists.

## Targeted Attacks

Focus on individuals or organizations. A specific target in mind.

Majority of people are unlikely to encounter such a threat.

### Attack Motives
Targets are chosen because of who they are or what they represent.

### Common Tactics
- Weak Passwords
- Unpatched Vulnerabilities
- Social Engineering

## Broad-based Attacks

Broad-based attacks reach a large number of people in hopes of compromising as many systems as possible.

Majority of cyber criminal activity is taking place.

### Attack Motives
Typically this tactic is used to steal identities and money.

### Common Tactics
- Weak Passwords
- Unpatched Vulnerabilities
- Social Engineering