Honeypots are decoy systems configured to be intentionally vulnerable and designed to gather information about attackers and their methods.

**TYPES OF HONEYPOTS**
- Pure Honeypots: Set up as full-fledged production systems.
- High-Interaction Honeypots: Imitate production system activities, so to an attacker, they look like a full production system.
- Low-Interaction Honeypots: Simulate only the services frequently requested by attackers.

**WHY USE HONEYPOTS?**
- Collect new and emerging malware
- Identify the source of attacks
- Determine attack vectors
- Build a profile of the target industry if using specific industry domains

Alert Logic deploys honeypots in public cloud infrastructures around the world to observe the types and frequencies of attacks, and how the attacks vary geographically.

**USA**
- **Origin of Attack**
  Attacks on US targets most frequently come from China, the US, India and Russia.
- **Type of Malware**
  94% of malware observed was credential-stealing malware.
- **Attack Vector**
  The US had the highest proportion of attacks on HTTP, perhaps because of higher web adoption.

**EUROPE**
- **Origin of Attack**
  Attacks against Northern Europe were most often from neighbors to the East; Western Europe’s primary attackers were from China and North and South America.
- **Type of Malware**
  Northern Europe had more known malware than what was used in Western Europe.
- **Attack Vector**
  While Microsoft DS was the most popular, attacks in Europe were equally spread among other services.

**ASIA**
- **Origin of Attack**
  Attacks against the Asian/Pacific region most frequently originated in the US.
- **Type of Malware**
  Conficker (credential-stealing malware) is the most popular malware for attacks in Asia. Financial institutions have been the hardest hit.
- **Attack Vector**
  Microsoft DS is the overwhelming most popular attack vector, and a good target for accessing files and infecting systems.