The Art of Cyber Security: The Threat Landscape and Tactics

1 Who really are the adversaries?

- Professional criminal gangs
- Lone hackers, cyber criminals, script kiddies
- Foreign governments
- Political activists
- Insiders
- Competitors

2 The most common tactics

- Steal credit cards, paypal logins
- Ransomware
- Industrial espionage
- Database breach
- Botnets, fast flux, domain flux
- Spam
- Keyloggers
- Rootkits
- Man in the browser

3 The economy

- Bitcoin transactions change cyber landscape by enabling anonymous transactions

Economy can have fairly deep hierarchies, for example:

- Hacker steals 1000 Fullz (credit card and CCV and name and address)
- Sells on Tor forum for 1 BTC
- Buyer sells groups of 20 to cashiers

4 Planning strategies

With the advent of machine learning, strategies are more intelligent based on large scale analytics

- Open source intelligence (OSINT)
- Sentiment analysis
- Targeted advertising
- Identifying criminals and threats

5 Spies - Can ”we” stay anonymous

VPNs can be used to hide your IP address, or TOR can be used to increase anonymity

6 Security Operations Center (SOCs)

Teams proactively monitor the infrastructure

Tools/communities:

- Alien Vault
- Snort
- SNAIL
- OSEC
- OTX
- Logrhythm

7 Security Information and Event Management

Third party monitoring (£8k/year)
Log rhythm:

- Create rules for alert types
- People review alerts and report back
- Cost depends on the level of monitoring they want

8 High Availability Pair

2 firewalls in active-active pair (means e.g. VOIP availability during updates) Network/switches updated out of hours

1. Verify HA functionality before an upgrade