Raytheon

Customer Success Is Our Mission

Castle Warrior

Monty McDougal
Principle Security Engineer
Information Security Solutions (ISS)

Why Build Network Castles?

- Castle Walls keep out the roving hordes
  - If nothing else we need to filter the noise level down
  - It is fairly low cost to defend against the threat from the horde
- Castle Walls will not defend against skilled attackers
  - They will subvert them using a more sophisticated attack method
- Never underestimate the horde's ability to learn new skills!
  - Advanced attacks today will become the norm over time

Your Firewall Will No Longer Protect You…

Assume Attackers Will Get In

- Attackers are going to get inside the walls
  - Software is inherently vulnerable to human coding error
  - It is time to consider an Intruder Tolerance model
    - Risk Management vs. Risk Avoidance
- It is impossible to keep threats out
  - Zero day, polymorphic and/or targeted threats are real hard to stop
  - Attacks against end-points perpetuate this problem
    - Mail clients, browsers, desktop applications, remote access, client devices, Web 2.0
  - Insider threats (how are users and administrators vetted?)
  - Supply chain threats (who provides your hardware and services?)
- We should still make it hard for them to get in…

End-Point Devices And End-Users Are Achilles Heel…

Turn Thy Castle Around

- Castle walls can be used offensively too
  - Use walls to stop attackers from exiting
  - Channel the enemy into points which are closely watched
- Ingress vs Egress rules
  - Traditional controls have been focused on what has entering the kingdom (network)
  - It is time to start watching what is leaving to see if it is the crown jewels
- Slow data exfiltration and monitor data flows
  - Use the walls to create situational awareness & choke points

Watching Outbound Net Flows Is A Necessity

Watch For Secret Tunnels

- Why watching the door if attackers are not using it!

- If the attackers uses a secret tunnel you don't know about they can bypass your controls
  - – Masquerading as legitimate traffic allowed to pass through the gates
    - HTTP/HTTPS, DNS, email, etc.
  - – Going over/under the walls and bypassing the gate all together
    - VPNs, rogue modems, rogue wireless, thumb drives, hand-held devices, etc.
  - – Watch for lateral moving traffic
    - Attackers may not be going out the same way they came in

Aggressively Watching For Anomalies Is Required

Know Thy Castle

- Defenders have one major advantage… It is their Castle!
- Defenders can leverage this to choose the battlefield
  - Force attackers into vulnerable positions that can be monitored
  - Set traps and monitor them for intrusion
- Watch for and aggressively investigate anomalies
  - At the network level and the host level
- Assuming the defender has a proper baseline, they know what is the normal state of their castle
  - Strong host-based lockdown and configuration management
  - Use whitelists as opposed to blacklists

Whitelisting And Strong CM Offer A Glimmer Of Hope

Aggressively Defend Thy Castle

- Even if we assume attackers can get into the Castle, we should kill them with extreme prejudice for being there!
- Limit the window of time an attacker has inside the walls
  - Focus on real time detection capabilities
  - Speed up the response times
- Deception and misdirection of the enemy may slow their attacks or allow you to learn their tactics (e.g. honeynets)
- If only we could ride out and burn our attackers Castle down…

Re-Tool To Respond Faster And More Aggressively

Parting Thought…

When was the last time you took a hard look at your Castle from the inside out?

About the Author & Raytheon ISS

- Monty McDougal – Principal Security Engineer
  - CISSP, ISSEP, ISSAP
  - GCFA, GCIH, GCUX, GCWN, GREM, GSEC, GAWN-C
  - Expert in Information Security and Incident Response

- Contact Info
  - Monty_McDougal@raytheon.com
  - 972.205.8650

- Raytheon – Information Security Solutions (ISS)
  - http://www.raytheon.com/businesses/riis/iss/index.html