What can organizations do immediately to put them in a better position to investigate an APT breach?

Shawn Carpenter

- Currently Principal Forensics Analyst at NetWitness Corporation (~3.5 years)
- ManTech, Cyber Threat Analysis Division (CTAD), Diplomatic Security, US Dept. of State (2 years)
- Sandia National Laboratories, Cyber Monitoring and Analysis / Information Design Assurance Red Team (7 years)
- US Navy

INTELLIGENCE - Establish a dedicated threat intelligence group

- Threat intelligence – it is a full time job collecting, analyzing/correlating, maintaining and successfully leveraging
- Cultivate trusted relationships with other organizations; forums for open sharing of threat intel
- DNS logging, regular analysis of collected data & a system in place to blackhole domains

PREPARATION - Be prepared for the inevitable APT compromise…

- Identify what systems house your organization's most sensitive/critical data. Your answer shouldn't be "everything"
- Identify individuals that may be targeted based on their roles in the organization or access to sensitive information
- **Build relationships** with departments/groups that are crucial in rapid incident response
- Honeypot – server(s) maintained on corporate infrastructure with legitimate and convincing looking materials, but not disclosed to user population; increased logging/monitoring to ferret out interesting traffic
- Full packet capture solution at gateway and strategic points in network infrastructure

Quality, not Quantity

- Regularly audit all of your IDS signatures
- Regularly examine emails quarantined by your security infrastructure
- Infrastructure in place to quickly identify affected machines/users & correlate
- Solid incident response procedures in place
- People - Experienced analysts with critical skill sets

Thanks!

Contact information:

shawn(at)netwitness.com

Twitter: @shawn_carpenter

703.889.8950