

Auto-adapting Stealth Communication Channels

Daniel J. Burroughs
University of Central Florida

About myself

- Assistant Professor at UCF
- Research includes
 - Correlation of distributed network sensors
 - Law enforcement data sharing network

Correlation of IDS/Sensors

- Previous research project I worked on
 - Presented at DefCon 9 & 10
 - Used Bayesian Multiple Hypothesis Tracking to analyze reports from multiple IDS scattered throughout a large network
 - Attempt to determine if events being detected are related or not

Escalation of the Situation

- That got me thinking
 - How would you defeat such a system (if it worked)
 - How could you avoid detection
- Not the detection of an attack, but the ongoing communication
 - Or, how could you secretly communicate on a network

Here's the question

- How do you communicate on a network without letting anyone know that you are doing it?
- First thing to figure out
 - How do they detect what is going on?
 - IDS
 - Firewalls
 - Observers

IDS

- Two basic forms of detection
 - Anomaly and Signature
- Signature Detection
 - Known attacks / events
 - Only way to avoid is to use an unknown method or an ever changing method
- Anomaly detection
 - Doesn't detect misuse – detects unusual behavior
 - Only chance someone has at detecting an unknown attack / event

Anomaly Detection Avoidance

- If we use a “random” or “changing” communication channel, signature detection can be avoided
- How do we avoid looking unusual?
- Detection of the network baseline
 - First stage:
Discover what the network looks like
 - What traffic is allowed?
 - What does normal traffic look like?
 - Do this passively

Detection of Entropy in the Network

- Some aspects of the network traffic are going to have a low entropy, other will have a high entropy
- Information can best be hidden in a high entropy data stream
- Lots of available channels
 - Timing
 - Checksums
 - All the other data in a packet

Overall Concept

- Detect existing network baseline conditions
 - What does normal look like?
- Select potential communications channels
 - Determination of highly random information on network
 - Pruning of information channels
 - Communicating the method to the receiver
- Maintain an (almost) undetectable presence
 - Monitoring and updating to stay hidden

University of Central Florida

- Established in 1963
- Part of the Florida State University System
- Located 13 miles east of Orlando
- 42,837 Students
- 5,500 in Engineering and Computer Science



Information Systems Technology

- IST
 - Undergraduate program in the College of Engineering
 - Applied Engineering Degree
 - Heavy concentration of hands-on learning, real-world applications & experience