Data Exfiltration through DNS lookups and Botnet Control Structures

Nolan Berry
Cory Schwartz
Why is DNS a problem?

- Must be allowed through firewall
- Cannot block port 53 (DNS)
- Most environments don’t monitor DNS requests
How does DNS data exfiltration work?

• Source sends data encoded within DNS query
• DNS query sent to authoritative server (external host)
• Destination decodes and retrieves data
DETECTION/MITIGATION

1. Block connection based on IP-reputation or Geo-location

2. Block known malicious domain names on internal DNS server

3. Traffic analysis with big-data analytics
Our Exfiltration Tools

How does our tool works

• Base 64 encoding
• 200 Bytes at a time
• DNS lookup to authoritative server
• External server reassembles packets and constructs original file
Mitigation Elasticsearch + Packetbeat