25 – Malware-Focused Network Signatures

Network Countermeasures
Approaches to Finding Countermeasures
Maintaining OpSec
Content-based Network Countermeasures (Snort)
Snort Actions
Content
Combining Dynamic and Static Analysis
Attack Methods – Blending In
Sources of Network Content
Creating a Signature
Network Countermeasures

● Simple ones:
  - Filter by IP-Address/Port
  - Restrict access by IP-Address/Port
  - Sinkhole bad machines (DNS reroute)
  - Provide proxy servers to disable selected access

● IPS content-based countermeasures using deep packet inspection.

● Basic network indicators should be focus of basic malware analysis
Approaches to Finding Countermeasures

- Mine logs, alerts, packet captures (if any), i.e., information already captured about the malware
- Inspect and record behavior of system in your malware analysis lab environment
- Maintain *operations security* (OpSec) when looking up information about the malware on the open internet. Malware may be recording your behavior (unused link ruse.)
Maintaining OpSec

- If connecting to internet to investigate servers used in the attack, use indirection
  - TOR, proxy, web-based anonymizer
- Get IP/Domain information from cached source if possible. (Links from pages in google cache will be live.) E.g.: BFK DNS logger (freely available)
Content-Based Network Countermeasures (Snort)

• Rule form:
  action proto src_ip src_port direction dst_ip dst_port (options)

• Example:
  alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTPS_PORTS
  (msg:"TROJAN Malicious User-Agent";content:"0od0oa|User-Agent:\ Wefa73";classtype:trojan-activity;sid:2000001;rev:1;)

• $HOME_NET, $EXTERNAL_NET, $HTTPS_PORTS: configured variable values.

• ->: direction specifier.

• Options: message to print, content pattern, rule category, unique rule identifier, rule revision.
Snort Actions

- alert (generate alert then log)
- log (log the packet)
- pass (ignore the packet)
- activate (alert then turn on another rule)
- dynamic (remain idle until activated, then log)
- reject (block the packet, log, TCP RST or ICMP unreachable)
- sdrop (drop but don't log)
Content

- content:”|0d 0a|User-Agent\: Wefa73”
- Vertical bar used to offset hex content.
- 0d0a represents crlf (header separator)
- This matches a specific user-agent string.
- Malware this was intended to catch generates the user-agent string on the fly.
- More appropriate options:
  
  ```
  flow:established,to_server; content:"|0d 0a|User-Agent\|3a| We"; isdataat:6,relative; content:"|od 0a|"; distance:0; content:"\|User-Agent\|3a\| Webmin\|0d 0a\"; pcre:"/User-Agent\: We[a-z0-9]{4}\|x0d\|x0a/";
  ```
Combining Dynamic and Static Analysis

• Objectives:
  - Full coverage of functionality (follow all paths)
  - Understand functionality (including input/output)

• Pitfalls:
  - Don't overanalyze. Use following hierarchy to decide how far to go:
    • Surface Analysis
    • Communication method coverage
    • Operational replication (server-based controller)
    • Code coverage (every block executed)
Attack Methods – Blending In

- Malware may mimic/use/abuse existing protocols: HTTP, HTTPS, DNS
- Information may be embedded in GET request URLs or other headers
- Novel User-Agents or parameters may be used, but using reasonable user-agents (esp. host specific) makes traffic blend better
- Information may be inserted into existing (useful) web infrastructure
- Client-initiated beaconing is often employed due to abundance of NATs.
Sources of Network Content

- Important to understand these sources in generating a network signature
  - Random data
  - Data from standard networking libraries
  - Hard-coded data from malware
  - Data about host and configuration
  - Data received from somewhere else (C&C server)
Creating a Signature

- Analyze the parsing routines
- Target multiple elements of the malware
- Focus on elements that are part of both endpoints
- Focus on elements that are part of a key
- Identify elements that are not immediately apparent in traffic
Next Time

- PMA Chapter 15