Malware-Focused Network Signatures
Network Countermeasures

- IP connectivity
  - Restrict network access using routers and firewalls

- DNS
  - Reroute known malicious domains to an internal host (sinkhole) – config proxy servers to defend

- Content-filters
  - Proxies, intrusion detection systems, intrusion prevention systems for intercepting web requests in order to detect or prevent access
Network Countermeasures

- Mine logs, alerts, and packet captures for forensic information (already generated)
  - No risk of infection when performing passive analysis versus actively attempting to run malware
  - Malware can be programmed to detect active analysis (detect lab environment)

- Indications of malicious activity
  - Beacons to malicious sites (example of malicious activity)

<table>
<thead>
<tr>
<th>Information type</th>
<th>Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain (with resolved IP address)</td>
<td><a href="http://www.badsite.com">www.badsite.com</a> (123.123.123.10)</td>
</tr>
<tr>
<td>IP address</td>
<td>123.64.64.64</td>
</tr>
<tr>
<td>GET request</td>
<td>GET /index.htm HTTP 1.1 Accept: <em>/</em></td>
</tr>
<tr>
<td></td>
<td>User-Agent: Wefa7e</td>
</tr>
<tr>
<td></td>
<td>Cache-Control: no</td>
</tr>
</tbody>
</table>

The **User-Agent** request header contains a characteristic string that allows the network protocol peers to identify the application type, operating system, software vendor or software version of the requesting software user agent.
Operation Security

- Game between Investigators and Attackers – attackers can identify investigation activities
  - Send a phishing link to specific individual and watch for access from an unexpected geo area
  - Embed unused domain and watch for attempts to resolve the domain
- Attackers could change their tactics if they found they are being investigated.
Safely Investigation Online

- **Indirection**
  - Use network anonymizers such as Tor/proxy to hide yourself
  - Use a virtual machine and virtual networks running through remote infrastructure (cellular, Amazon EC2, etc)
  - Cellular connection/VPN

- **IP address and DNS information**
  - See Regional Internet Registries to find out organizational assignment of IP blocks (registered name)
  - Query whois records of DNS names to find contact information online - anonymous (domaintools.com)
Content-based Network Countermeasures

- Intrusion Detection with Snort
  - Rules that link together elements that must be true to fire
  - Attributes to look at: Size of payload, flag fields, specific settings of TCP/IP headers, HTTP headers, content in payload
  - Create snort rules

At the start of 2019, 87 percent of Web traffic was encrypted, compared to just 53 percent in 2016, Meeker said, citing Fortinet’s Quarterly Threat Landscape Report.

Header: rule action, protocol, src, dest IP, ports

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"TROJAN Malicious User-Agent"; content:"|od oa|User-Agent": We фа; classtype:trojan-activity; sid:2000001; rev:1;)
```

Option: conditions the rule should fire
Content-based Network Countermeasures

- Potential Snort rule to detect Web7e – (We[a-z0-9]{4}). False positive – Webmin software (matches the rule)
- New rule generated (p305) and tested across real traffic; done manually
- Non-live Traffic: each time we may see Web95 each time we run the malware
- Next host run the malware: We9753 – different on every trial run – random seed
- Attacker can intentionally generate false positives
Combining Dynamic and Static Analysis

- Attackers mimicking typical web requests
- IRC (Internet Relay Chat) was popular in the 1990s – e.g. communicate with botnet – IDS watch IRC traffic
- Blend in with HTTP/HTTPS (encrypt content)
- Encoding commands in URLs and HTTP headers (p311)
- Perform encoded request through DNS
- Tunneling malicious comm. By misusing fields (User-agent field, disguise as web requests)
- Malware circumventing intrusion detection filters similar to Tor circumventing censorship filters
Finding the Networking Code

- Finding networking code to develop signature
  - WinSock API (WSAStartup, getaddrinfo, socket, connect, send, recv, WSAGetLastError) – Malware typically use these functions
  - WinInet API (InternetOpen, InternetConnect, InternetOpenURL, InternetReadFile, InternetWriteFile, HTTPOpenRequest, HTTPQueryInfo, HTTPSendRequest) – higher-level APIs (more effectively blend into normal traffic)
  - COM interface (URLDownloadToFile, CoInitialize, CoCreateInstance, Navigate) – High-level API
- Finding hard-coded patterns or stable content to create rules
Project

- Go over the project
Spreading of Wannacry

- SMB – Server Message Block – file sharing, network browsing, printing services, interprocess communication over network – NetBIOS
- MS17-010 – Targeting Port 445, 137, 138, 139.
  - `srv!SrvOs2FeaListSizeToNt` calculate FEA list size, wrong WORD cast
  - FEA List converted to NTFEA LIST -> overflow in non-page pool because size is miscalculated.

```c
v1 = 0;
length = *(DWORD *)pOs2Fea;
pBody = pOs2Fea + 4;
v9 = 0;
v4 = pOs2Fea + Length;
while ( pBody < v4 ) { if ( pBody + 4 >= v4
|| (v5 = *_BYTE *>(pBody + 1) + *(WORD *)(pBody + 2),
v8 = *_BYTE *>(pBody + 1) + *(WORD *)(pBody + 2),
v5 + pBody + 5 > v4 ) )
```
Hard-coded Data - Interesting Example

- Manual content means more hard-coded data – malware authors may make mistakes (typos)

Mozilla – Mozilla/MoZilla

Difference between Google Translate and WannaCry
Linguistic Analysis - WannaCry

- A number of unique characteristics in the note indicate it was written by a fluent Chinese speaker.
- A typo in the note, “帮组” (bang zu) instead of “帮助” (bang zhu) meaning “help,”
- One term, “礼拜” for “week,” is more common in South China, Hong Kong, Taiwan, and Singapore; although it is occasionally used in other regions of the country.
- Indication: attackers know English, use Google Translate for other languages, but write own Chinese versions (traces showing that they might be from south China region.
- North Korea – Lazarus Group (NSA)