What is HACIENDA?

• Data reconnaissance tool developed by the CITD team in JTRIG
• Port Scans entire countries
  – Uses nmap as port scanning tool
  – Uses GEOFUSION for IP Geolocation
  – Randomly scans every IP identified for that country
Countries

- Completed full scans of 27 countries including
- Completed partial scans of 5 additional countries
Tasking & Access

- To task HACIENDA with a Country or Subnet
  - [Redacted]
  - CITD alias ([Redacted])

- Access to the Data
  - At GCHQ, request a GLOBAL SURGE account from [Redacted]
  - At CSEC, contact
  - At NSA, contact
  - At DSD, contact
Ports

- Pulls back hostname, banners, application names and port status
- Gathers additional information for...
  - 21 (ftp): directory listing
  - 80 (http): content of main page
  - 443 (https): content of main page
  - 111 (rpc): results of rpcinfo
Host 1 \hspace{1cm} Host 2

\begin{align*}
\text{SYN (SEQ} &= x) \\
\text{RST (SEQ} &= y, \text{ ACK} = x + 1)
\end{align*}
The Results...

- All stored in JTRIG’s internal database
- Available in GLOBAL SURGE
  - NAC’s Network Knowledge Base Prototype
- Transferred by MAILORDER to
  - CSEC
  - DSD
  - NSA NTOC
How is it used?

- **CNE**
  - ORB Detection
  - Vulnerability Assessments
- **SD**
  - Network Analysis
  - Target Discovery
The Hacking Process

1. \((R)\)econnaissance
2. \((I)nfection
3. \((C)o\)mmand And Control
4. \((E)xfiltration
Reconnaissance

Publicly Available Information
(Email Address, Location, Network Info, Passwords, etc.)

Research

Hacker

Enumerate (Network)
Scan (Services)
Operating Systems
Versions
Domain Names

Victim

Reconnaissance  Infection  Command and Control  Exfiltration
Infection

Email with Attachment or Link

Special Packets to Exploit Services

Use Login Credentials

Reconnaissance  Infection  Command and Control  Exfiltration

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
Command and Control

Push Tools and Send Commands
(Tasking, Survey, etc.)

Hacker → Victim

Beacons and Responses

Reconnaissance  Infection  Command and Control  Exfiltration
Exfiltration

Exfil using known and custom protocols
(Known: HTTP, SMTP, ICMP, FTP, etc)
Reconnaissance

This system is audited for USSID 18 and Human Rights Act compliance
CLASSIFICATION: TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL

X-KEYSCORE C2C Session Viewer

<table>
<thead>
<tr>
<th>Session</th>
<th>Case Notation</th>
<th>From IP</th>
<th>To IP</th>
<th>From Port</th>
<th>To Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Internet Protocol, Src: 192.168.0.8 (192.168.0.8), Dst: 192.168.0.8 (192.168.0.8)
Version: 4
Header Length: 20 bytes
Differentiated Services Field: 0x00 (DS0: 0x00; Default; ECN: 0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
..... 0 = ECN-Capable Transport (ECT): 0
..... 0 = ECN-CE: 0
Total Length: 60
Identification: 0x2d3e (11966)
Flags: 0x00
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 64
Protocol: ICMP (0x01)
Header checksum: 0x897a [correct]
[Good: True]
[Bad: False]
Source: 192.168.0.8 (192.168.0.8)
Destination: 192.168.0.8 (192.168.0.8)
Internet Control Message Protocol
Type: 0 [Echo [ping] reply]
Code: 0 [0]
Checksum: 0x52ee [correct]
Identifier: 0x0001
Sequence number: 623 (0x026b)
Data [32 bytes]
0600 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79
0610 7a 7b 7c 7d 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0620 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0630 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0640 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Reconnaissance  Infection  Command and Control  Exfiltration
Password Guessing

<table>
<thead>
<tr>
<th>USER</th>
<th>PASS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>#mafiafute197532@%!?*</td>
</tr>
<tr>
<td>Administrator</td>
<td>sh315l1k3p4rty3v3r</td>
</tr>
<tr>
<td>Administrator</td>
<td>Sh3I5Lik3P4rtY@v3r</td>
</tr>
<tr>
<td>Administrator</td>
<td>Sh5l8lK6P8rtY6v5r</td>
</tr>
<tr>
<td>Administrator</td>
<td>kalimero4cappy</td>
</tr>
<tr>
<td>Administrator</td>
<td>P@ssword</td>
</tr>
<tr>
<td>Administrator</td>
<td>P@ssword</td>
</tr>
<tr>
<td>Administrator</td>
<td>P@ssword</td>
</tr>
<tr>
<td>Administrator</td>
<td>P@ssword</td>
</tr>
</tbody>
</table>

Iraqi Ministry of Finance

Reconnaissance  Infection  Command and Control  Exfiltration
Windows cmd.exe
LANDMARK – automated tradecraft to further expand CNE covert infrastructure
LANDMARK

☆ CSEC’s Operational Relay Box (ORB) covert infrastructure used to provide an additional level of non-attribution; subsequently used for exploits and exfiltration

☆ 2-3 times/year, 1 day focused effort to acquire as many new ORBs as possible in as many non 5-Eyes countries as possible
LANDMARK – the recent past....

- February 2010
- Operation encompassing the whole of LONGRUN solely using OLYMPIA (CSEC’s network knowledge engine with automated tradecraft)
- 8 teams of 3 network exploitation analysts busy for 5-8 hours
- A list of 3000+ potential ORBs
BUT, network analysis still manual!
LANDMARK today...

Network analysis tradecraft to determine vulnerable devices has been encoded within OLYMPIA.
GSM provider

NSA TAO requested assistance gaining access to the network

Network analysis using OLYMPIA:
- DNS query to determine IP address
- IP address to network range
- Network range to port scan
- Are there any vulnerable devices in that range?

Duration: < 5 minutes
Use Case 1: Finding Orbs

MUGSHOT CORE - Q/A Framework

Vulnerability Profile

GCHQ
© Crown Copyright. All rights reserved.
Benefits

- Automated Vulnerability Assessment
  - Using Vulnerability Profiles for Remote and Content Delivery vectors
- Automated Target Development and Monitoring
  - Identify and characterise target machines
- Profiles machines, including:
  - Browser, OS, PSP, Patch History
  - Activity
  - Download
- Automated Target Technology Tracking (Stats & Trends)
  - Browsers, OS, PSP etc
- ORB Identification
  - Initial ten fold increase in Orb Identification rate over manual process
UK TOP SECRET STRAP 1

Defining Attributes

- Attribute Definition
  - Name
  - Description
  - Type
  - Data sources

Machine Communication Attributes

- FTP login
- DNS Request
- HTTPS connection

Machine Attributes

- Open port (25, 80, 443)
- Server banner (Server: Apache)
- PSP fingerprint (Kaspersky v7.01)
- XFF (192.168.2.1)
- Web Request (test.exe, file.pdf)
- SNMP sysname

DNS Name (webhost.com)
MUGSHOT GOALS

- Automated Target Characterisation and Monitoring
  - Automatically understand everything important about CNE target networks from passive and active sources.

- Automated Un-Targeted Characterisation
  - Automatically understand everything important about all machines on the Internet from passive and active sources.