# Presentation Outline

- 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

Communications Security Establishment | Centre de la sécurité des télécommunications

Olympia version 0.5.0

File Tools Window Help

Olympia | Gimme all you got

Gimme all you got | Gimme all you got by Country

Search

Continent: africa

Country: kenya

Date Range: Last 30 days

Start Date:

End Date:

Comments

- Show VPNs
- Show Toygrippe Range Events
- Show CNO Event Summaries
- Show User Online Events on IP
- Show router configuration information (TIDAL SURGE)
- Show IP Communications
- Show Geolocation Information
- Show Network Information
- Show SIGINT Observable Feature Information
- Show Survey Information
- Show Geolocation Map
- Reverse DNS Lookup
- Show Port Scans on IP

Select All | Deselect All

Run

Athena View (JPA) (10000)

Showing page 1

| Source | System | First Seen | Last Seen | Hostname | IP | Port | Protocol | Status | TTL | Product | Version | Banner Information |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| GCHQ | Hacienda | Tue May 19 08:11:03 GMT 2009 | Tue May 19 08:11:03 GMT 2009 | | [redacted] | 80 | tcp | filtered | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 08:11:03 GMT 2009 | Tue May 19 08:11:03 GMT 2009 | | | 110 | tcp | filtered | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 08:11:03 GMT 2009 | Tue May 19 08:11:03 GMT 2009 | | | 111 | tcp | filtered | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 08:11:03 GMT 2009 | Tue May 19 08:11:03 GMT 2009 | | | 161 | tcp | filtered | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 08:11:03 GMT 2009 | Tue May 19 08:11:03 GMT 2009 | | | 162 | tcp | filtered | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 08:11:03 GMT 2009 | Tue May 19 08:11:03 GMT 2009 | | | 443 | tcp | filtered | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 08:11:03 GMT 2009 | Tue May 19 08:11:03 GMT 2009 | | | 500 | tcp | filtered | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 08:07:29 GMT 2009 | Tue May 19 08:07:29 GMT 2009 | | | 0 | unknown | unreachable | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:15:01 GMT 2009 | Tue May 19 04:15:01 GMT 2009 | | | 110 | tcp | open | 0 | Kerio MailServer POP3 Server | 6.1.2 | 4152.1242730171@kv_svr |
| GCHQ | Hacienda | Tue May 19 04:15:01 GMT 2009 | Tue May 19 04:15:01 GMT 2009 | | | 443 | tcp | open | 0 | Kerio MailServer Webmail | 6.1.2 | unknown |
| GCHQ | Hacienda | Tue May 19 04:15:01 GMT 2009 | Tue May 19 04:15:01 GMT 2009 | | | 25 | tcp | open | 0 | Microsoft ESMTP | 6.0.3790.3959 | unknown |
| GCHQ | Hacienda | Tue May 19 04:15:01 GMT 2009 | Tue May 19 04:15:01 GMT 2009 | | | 80 | tcp | open | 0 | Microsoft IIS webserver | 6.0 | unknown |
| GCHQ | Hacienda | Tue May 19 04:15:01 GMT 2009 | Tue May 19 04:15:01 GMT 2009 | | | 21 | tcp | open | 0 | Microsoft ftpd | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:15:01 GMT 2009 | Tue May 19 04:15:01 GMT 2009 | | | 22 | tcp | closed | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:15:01 GMT 2009 | Tue May 19 04:15:01 GMT 2009 | | | 23 | tcp | closed | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:15:01 GMT 2009 | Tue May 19 04:15:01 GMT 2009 | | | 111 | tcp | closed | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:15:01 GMT 2009 | Tue May 19 04:15:01 GMT 2009 | | | 161 | tcp | closed | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:15:01 GMT 2009 | Tue May 19 04:15:01 GMT 2009 | | | 162 | tcp | closed | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:17:28 GMT 2009 | Tue May 19 04:17:28 GMT 2009 | | | 21 | tcp | closed | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:17:28 GMT 2009 | Tue May 19 04:17:28 GMT 2009 | | | 22 | tcp | closed | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:17:28 GMT 2009 | Tue May 19 04:17:28 GMT 2009 | | | 23 | tcp | closed | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:17:28 GMT 2009 | Tue May 19 04:17:28 GMT 2009 | | | 25 | tcp | closed | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:17:28 GMT 2009 | Tue May 19 04:17:28 GMT 2009 | | | 80 | tcp | open | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:17:28 GMT 2009 | Tue May 19 04:17:28 GMT 2009 | | | 110 | tcp | closed | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:17:28 GMT 2009 | Tue May 19 04:17:28 GMT 2009 | | | 111 | tcp | closed | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:17:28 GMT 2009 | Tue May 19 04:17:28 GMT 2009 | | | 161 | tcp | closed | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:17:28 GMT 2009 | Tue May 19 04:17:28 GMT 2009 | | | 162 | tcp | closed | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:17:28 GMT 2009 | Tue May 19 04:17:28 GMT 2009 | | | 443 | tcp | open | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:17:40 GMT 2009 | Tue May 19 04:17:40 GMT 2009 | | | 21 | tcp | closed | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:17:40 GMT 2009 | Tue May 19 04:17:40 GMT 2009 | | | 22 | tcp | closed | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:17:40 GMT 2009 | Tue May 19 04:17:40 GMT 2009 | | | 23 | tcp | closed | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:17:40 GMT 2009 | Tue May 19 04:17:40 GMT 2009 | | | 25 | tcp | closed | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:17:40 GMT 2009 | Tue May 19 04:17:40 GMT 2009 | | | 80 | tcp | open | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:17:40 GMT 2009 | Tue May 19 04:17:40 GMT 2009 | | | 110 | tcp | closed | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:17:40 GMT 2009 | Tue May 19 04:17:40 GMT 2009 | | | 111 | tcp | closed | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:17:40 GMT 2009 | Tue May 19 04:17:40 GMT 2009 | | | 161 | tcp | closed | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:17:40 GMT 2009 | Tue May 19 04:17:40 GMT 2009 | | | 162 | tcp | closed | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:17:40 GMT 2009 | Tue May 19 04:17:40 GMT 2009 | | | 443 | tcp | open | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue May 19 04:16:24 GMT 2009 | Tue May 19 04:16:24 GMT 2009 | | | 0 | unknown | unreachable | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue Jun 17 00:13:13 GMT 2008 | Tue Jun 17 00:13:13 GMT 2008 | | | 0 | unknown | unreachable | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue Jun 17 00:13:39 GMT 2008 | Tue Jun 17 00:13:39 GMT 2008 | | | 0 | unknown | unreachable | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue Jun 17 00:12:49 GMT 2008 | Tue Jun 17 00:12:49 GMT 2008 | | | 0 | unknown | unreachable | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue Jun 17 00:13:56 GMT 2008 | Tue Jun 17 00:13:56 GMT 2008 | | | 0 | unknown | unreachable | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue Jun 17 00:13:59 GMT 2008 | Tue Jun 17 00:13:59 GMT 2008 | | | 0 | unknown | unreachable | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue Jun 17 07:00:29 GMT 2008 | Tue Jun 17 07:00:29 GMT 2008 | | | 0 | unknown | unreachable | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue Jun 17 07:03:13 GMT 2008 | Tue Jun 17 07:03:13 GMT 2008 | | | 0 | unknown | unreachable | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue Jun 17 07:01:12 GMT 2008 | Tue Jun 17 07:01:12 GMT 2008 | | | 0 | unknown | unreachable | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue Jul 07 07:30:40 GMT 2009 | Wed Feb 03 11:13:34 GMT 2010 | 80-247-147-40.reverse.nevaldes.net | | 0 | unknown | unreachable | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue Jul 07 07:32:20 GMT 2009 | Wed Feb 03 11:14:55 GMT 2010 | 80-247-147-41.reverse.nevaldes.net | | 0 | unknown | unreachable | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue Jul 07 07:31:23 GMT 2009 | Wed Feb 03 11:15:34 GMT 2010 | 80-247-147-42.reverse.nevaldes.net | | 0 | unknown | unreachable | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue Jul 07 07:32:13 GMT 2009 | Wed Feb 03 11:13:39 GMT 2010 | 80-247-147-43.reverse.nevaldes.net | | 0 | unknown | unreachable | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue Jul 07 07:30:17 GMT 2009 | Wed Feb 03 11:15:11 GMT 2010 | 80-247-147-44.reverse.nevaldes.net | | 0 | unknown | unreachable | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue Jul 07 07:32:54 GMT 2009 | Wed Feb 03 11:13:15 GMT 2010 | 80-247-147-45.reverse.nevaldes.net | | 0 | unknown | unreachable | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue Jul 07 06:49:57 GMT 2009 | Wed Feb 03 11:14:50 GMT 2010 | 80-247-147-46.reverse.nevaldes.net | | 0 | unknown | unreachable | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue Jul 07 06:47:17 GMT 2009 | Wed Feb 03 11:14:09 GMT 2010 | 80-247-147-47.reverse.nevaldes.net | | 0 | unknown | unreachable | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue Jul 07 06:18:02 GMT 2009 | Wed Feb 03 12:02:07 GMT 2010 | | | 0 | unknown | unreachable | 0 | unknown | unknown | unknown |
| GCHQ | Hacienda | Tue Jun 17 00:36:20 GMT 2008 | Tue Jun 17 00:36:20 GMT 2008 | gw02-gw.emperion.net | | 23 | tcp | open | 0 | Cisco router | unknown | unknown |

- BUT, network analysis still manual!

Canada

# LANDMARK today…

- Network analysis tradecraft to determine vulnerable devices has been encoded within OLYMPIA

[redacted]

- [redacted] 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