Getting Close to the Adversary

Forward-based Defense with QFIRE

June 3, 2011

QFIRE Pilot Lead

NSA/Technology Directorate

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20360401
Abstract

(TS//SI//REL) The goal of forward-based defense is to detect and mitigate malicious threats in real-time, *as close to the source as possible*. It is part of a layered defense strategy with four concentric zones: endpoint-, perimeter-, aggregation-, and forward-based defenses. The QUANTUMTHEORY mission leverages NSA’s vast system of distributed passive sensors to detect target traffic and tip a centralized command/control node. This node assesses the tip and injects a response towards the target using active TAO assets.

(TS//SI//REL) Extremely powerful CNE/CND/CNA network effects are enabled by integrating our passive and active systems:
- resetting connections
- redirecting targets for exploitation
- taking control of IRC bots
- corrupting file uploads/downloads
- More!

(TS//SI//REL) The success rate of these effects is largely determined by the latency from tip-to-target. **QFIRE** is a consolidated QUANTUMTHEORY platform under development that reduces latencies by co-locating (1) existing passive sensors with (2) local decision resolution, and (3) the ability to locally inject traffic to achieve the desired network effect.
Topics

- Layered Defense Model
- NSA TURBULENCE Architecture
  - TURMOIL passive SIGINT sensors
  - TURBINE active SIGINT command/control
- QUANTUM THEORY
  - Integrating passive/active systems for CNE/CND/CNA
- QFIRE
  - Consolidated low-latency QUANTUM THEORY capability under development for forward-based defense
Forward-based Defense
NSA TURBULENCE Architecture
Distributed Sensors: Passive Collection

(S//SI//REL) High-speed passive collection systems intercept foreign target satellite, microwave, and cable communications as they transit the globe.
TURBINE: Active Mission Management

(TS//SI//REL) TURBINE provides centralized automated command/control of a large network of active implants.

Accesses:
- TURMOIL
- TUTELAGE
- Implants (TAO)
QUANTUMTHEORY

(TS//SI//REL) Extremely powerful CNE/CND/CNA network effects are enabled by integrating our passive and active systems:

- Resetting connections (QUANTUMSKY)
- Redirecting targets for exploitation (QUANTUMINSERT)
- Taking control of IRC bots (QUANTUMBOT)
- Corrupting file uploads/downloads (QUANTUMCOPPER)

(TS//SI//REL) QUANTUMTHEORY dynamically injects packets into a target’s network session to achieve CNE/CND/CNA network effects.

- **Detect:** TURMOIL passive sensors detect target traffic & tip TURBINE command/control.
- **Decide:** TURBINE mission logic constructs response & forwards to TAO node.
- **Inject:** TAO node injects response onto Internet towards target.

(TS//SI//REL) The propagation delay from tip-to-target determines the success rate of the network effect. **Less Latency = More Success!**
QFIRE: Consolidate for Low Latency

- (TS//SI//REL) Eliminate trans-Atlantic/Pacific latency
  - QUANTUMTHEORY Path: site → NSAW-TURBINE → target

- (TS//SI//REL) QFIRE collocates at site: sensor, decision logic, and local/regional injection capability to achieve low latency.
  - Use existing SIGINT sensors for alerting
  - Local decision resolution (local TURBINE)
  - Local/regional injection capability
  - QFIRE Path: site → target

- (TS//SI//REL) A low latency capability substantially increases the variety of achievable CNE/CND/CNA network effects and improves their overall effectiveness.
QFIRE/Forward-Based Defense: Development/Dependencies

QFIRE
- Develop/deploy QFIRE prototype for SCS site(s)
- Conduct time trials & evaluate operational effectiveness
- Develop/deploy QFIRE for high-speed SSO cable site(s)

Dependencies
- Grow regional shooter infrastructure (more Points-of-Presence)
- Develop local/regional insertion capability at SSO cable accesses
- Enhance cloud analytics and QUANTUM missions
- Botnet mitigation pilot effort
QFIRE Components @ SCS

Internet Option A
- SCS Site RMS
- Cooperative
- RF-Tx
- RF-Rx

Internet Option B
- SCS Site RMS
- Non-cooperative
- Wireless Access Point
- WAP
- NAT-GW
- Internet
- Wireless Clients
- Wired Clients

Regional Inject node is on Internet.
Local Inject node is collocated with RelayNode in Diode RelayNode.

Wired Clients
Wired Clients

Low-Speed Packet
High-side

Packet(s)
InjectPacket

Target
Serve

Inject

Low-Side

Even

TURBINE

TURMOIL

WC2

injectCommand XML

injectCommand RPC

A or B

A or B
QFIRE @ SCS: Physical/Virtual Network Architecture
iz in ur space-time continuum, upsetting all your gravity and quantum and stuffs.

@nsa.ic.gov
HTTP Web Client/Server

- Client initiates request, then server replies
- TCP socket:
  - Client: TCP SYN
  - Server: TCP SYN/ACK
- HTTP 1.1 Persistent Connection
  - Client: HTTP GET1
  - Server: HTTP Response1
  - Client: HTTP GET2
  - Server: HTTP Response2
QUANTUM INSERT: racing the server

The Game:
- **Wait** for client to initiate new connection
- Observe server-to-client TCP SYN/ACK
- **Shoot!** (HTTP Payload)
- **Hope** to beat server-to-client HTTP Response

The Challenge:
- Can only win the race on some links/targets
- For many links/targets: too slow to win the race!
QUANTUM INSERT: racing the server

QI detects/shoots on server-to-client TCP SYN/ACK

TCP SYN  HTTP GET  win!  lose

HTTP RESPONSE

QI

HTTP Payload
## QUANTUMTHEORY Latency*

<table>
<thead>
<tr>
<th>Node</th>
<th>QUANTUMTHEORY Function</th>
<th>Minimum Latency to Reach Next Node (ms)</th>
<th>Total Latency (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAS</td>
<td>Site Access System: Front end &amp; Layer 0/1</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>Stage0</td>
<td>TUMULT: Demux &amp; Layer 2</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>Sensor</td>
<td>TURMOIL: Layer 3+Passive Sensor/Event Detection</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>ITx</td>
<td>ISLANDTRANSPORT: Enterprise Message Service</td>
<td>120</td>
<td>130</td>
</tr>
<tr>
<td>C&amp;C</td>
<td>TURBINE: Command/Control Decision Logic</td>
<td>20</td>
<td>150</td>
</tr>
<tr>
<td>Diode</td>
<td>SURPLUSHANGAR: High-to-Low Diode</td>
<td>20</td>
<td>170</td>
</tr>
<tr>
<td>CovNet</td>
<td>TAO Covert Network (MIDDLEMAN)</td>
<td>70</td>
<td>240</td>
</tr>
<tr>
<td>Inject</td>
<td>TAO injection implant</td>
<td>75</td>
<td>315</td>
</tr>
<tr>
<td>Target</td>
<td>Destination for CNE/CND/CNA network effect</td>
<td>--</td>
<td>686</td>
</tr>
</tbody>
</table>

*Timing Measurements, QUANTUMTHEORY Workshop, October 2010*