Before TUTELAGE...

Intrusion by Adversary

Intrusion Event Logged

Victim Notification (Response?)

Manual Analysis of Reporting Logs

Reporting Process

BEFORE INTRUSION

TIME

MON TUE WED THU FRI

TOP SECRET//COMINT//REL TO USA,
Adversary Malware Design Process

Discovery of Adversary Tools & Tradecraft

Tailored Countermeasure Developed & Deployed

Countermeasure Development

Adversary Malware Decision Loop

Discovered of Adversary Intentions

SIGINT-Enabled Countermeasure Mitigates Adversary Intrusion

Plan

Deploy

Attack

TOP SECRET//COMINT//REL TO USA,
Application of Capabilities

Internet

DoD Gateways

NIPRNet

BACK TO CAPABILITIES
Operational Landscape

Threat Observability

Foreign Intel Service

Email Phishing

Script Kiddie

SIGINT
Discover & Warn

TUTELAGE
Understand & Mitigate

COMMERCIAL
Anti-Virus, Firewalls, Intrusion Detection, Intrusion Prevention

Zero Day Exploit

Threat Sophistication
TUTELAGE Capabilities

Alert/Tip
- Passive Sensor Generates Alert
- Storage
- "Activity Successful"

Redirect
- "What's My Destination?"
- Redirect to Safe Server
- Infected Host's Information

Intercept
- Malicious Activity
- "Activity Successful"

Block
- Blocks Entry/Exit Activity

Substitute
- "Attack"
- "Sleep"

Latency
- Speed Adjusted
Alert/Tip indicates the presence of malicious activity and communicates this information with the rest of the TUTELAGE enterprise and/or the SIGINT (passive/active) enterprise. Rule and Decision Logic determine whether data is stored.
Intercept is the means by which the TUTELAGE in-line packet processor can transparently intervene in adversarial activities, permitting the activity to appear to complete without disclosing that it did not reach/affect the intended target.

(S//REL TO USA, FVEY)

In-Line Packet Processor:
Re-routes traffic dynamically
Modify inbound & outbound packets
Insert and/or delete packets
Substitute is the TUTELAGE in-line packet processor’s ability to perform bidirectional content detection and replacement.
Redirect is the TUTELAGE in-line packet processor’s ability to change the course or direction of an adversarial (or adversarial induced) activity.
Block is the means by which the TUTELAGE in-line packet processor can deny entry/exit of network activity at the Internet Access Points (IAPs) based initially on source and/or destination Internet Protocol (IP) addresses and ports.
Latency is the means by which the TUTELAGE in-line packet processor can stealthily vary the in/outbound speed of an adversary's activities traversing the IAPs to provide a diminished quality of service. This creates more time for other TUTELAGE capabilities to be executed.
TUTELAGE currently operates against 28 major threat categories, using a total of 794 operational effects encompassed in seven capabilities (alerting/tipping, blocking, interception, sidelining, substitution, redirection and latency).

<table>
<thead>
<tr>
<th>Cyber Activity</th>
<th>Ops</th>
<th>Alert/Tip</th>
<th>Block</th>
<th>Intercept</th>
<th>Latency</th>
<th>Redirect</th>
<th>Substitute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adversarial Recon</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bishop Knight</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Black Energy Bot</td>
<td>24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blind Marksman</td>
<td>77</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Byzantine Foothold</td>
<td>96</td>
<td>1</td>
<td>12</td>
<td>83</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Byzantine Viking</td>
<td>36</td>
<td>1</td>
<td></td>
<td>4</td>
<td>31</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Carbon Peptide</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contioker</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cross-Domain Violations</td>
<td>77</td>
<td>77</td>
<td></td>
<td>77</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dancing Panda</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discovery</td>
<td>123</td>
<td>4</td>
<td></td>
<td>116</td>
<td>1</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Elomore Exploit Kit (TEC)</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GnomeFisher</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GnomeVision</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MakersMark</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maverick Church</td>
<td>12</td>
<td>4</td>
<td></td>
<td>8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Native Dancer</td>
<td>26</td>
<td></td>
<td></td>
<td></td>
<td>18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non Attributed Malware</td>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phoenix Exploit Kit</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td>8</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Weasel/Waggle/SubtleSnow</td>
<td>58</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>57</td>
</tr>
<tr>
<td>Widowkey</td>
<td>20</td>
<td>1</td>
<td></td>
<td></td>
<td>25</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zeus</td>
<td>17</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>18</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td>794</td>
<td>81</td>
<td>2</td>
<td>61</td>
<td>3</td>
<td>77</td>
<td>552</td>
</tr>
</tbody>
</table>

TUTELAGE posture against major threats as of 11 February 2011.
Upgrades & What They Mean

Upgrade to 10G Sensor provides additional capabilities and enables future upgrades:

• Immediate Benefits:
  – Increased speed and capacity
  – TS/!SI signatures
  – Full Snort (Current sensors use packet-based Snort. 10G sensors use session-based Snort.)
  – Multi-event Snort

• Future Upgrades:
  – POPQUIZ: Real-time behavioral analytics
  – GNOMEVISION: De-obfuscation of malicious packages
  – Cryptanalytic Capabilities
  – Netflow: Traffic analysis with GHOSTMACHINE
TCP Reset prevents malicious activity by breaking the connection.
Sideline is an intentional redirection of an activity to a secondary level of intervention where an intermediate host(s) (e.g. Listening Post, Quarantine, etc.) is staged to provide additional processing/manipulation to better engage and/or thwart adversarial activity.
Sideline for Listening Posts

Sidelining is an intentional redirection of an activity to a secondary level of intervention where an intermediate host(s) (e.g. Listening Post, Quarantine, etc.) is staged to provide additional processing/manipulation to better engage and/or thwart adversarial activity.
Integrating with the DOD’s Host-Based Security System allows malicious activity detected through classified signatures in TUTELAGE to be dealt with at the host level. Using HBSS, TUTELAGE can trigger less sensitive alerts to local network administrators.
TUTELAGE can tip QUANTUM to enable offensive action in adversary space.
TUTELAGE can tip QUANTUM to enable offensive action in adversary space.
Real-time cryptanalytics allows Quantum operations to take place at net-speed.
OPS SUCCESS STORIES
• Based on information from SIGINT collection, a TUTELAGE countermeasure was developed and deployed in 2009 for a particular BYZANTINE HADES attack.

• On October 21st and 22nd 2010, the spear-phishing attack was launched. The attack targeted four users, including the Chairman of the Joint Chiefs of Staff and the Chief of Naval Operations, with a carefully disguised malicious PDF.

• NTOC operated the countermeasure and the attack was thwarted.
WAG Attempts to Deliver Holiday Present to DoD

23 December
• NTOC-TX calls ops center advising of phishing campaign with “Merry Christmas” subject associated with WAG actors
• WAG actors attempted to use ZEUS malware to exfiltrate documents
• NTOC-TX did malware analysis and identified 2 new callback domains
• In < 3 hours, received CyberCommand approval and placed domains on DNS interdiction

30 December
• NTOC-TX notices new spike in WAG mail signature
• NTOC-TX discovers new callback domain
• In < 20 minutes, received approval and placed domain on DNS interdiction
• NTOC-W confirmed same malware from Xmas themed event
AMULETSTELLAR Spearphishing... Trying to Make New Friends

- In SIGINT, NTOC observed AMULETSTELLAR use of @yahoo.com email account
- On Christmas Day, account was used to generated LinkedIn requests to 10 general and flag grade officers
- NTOC leveraged TUTELAGE and SIGINT for further discovery of activity
- In coordination with CyberCommand,
  - Published 10 advisories
  - Identified 2 additional LinkedIn accounts
  - Deployed 4 countermeasures
  - Intercepted over 2000 emails from AMULETSTELLAR actors
Combating the Low Orbit Ion Cannon (LOIC)

- The open-source LOIC tool has been used by “Anonymous” and others in several DDoS attacks.

- NTOC developed signatures to detect specific content strings generated by this tool.

- For example, for packets containing the string “Sweet_dreams_from_AnonOPs” TUTELAGE will perform an ACL Block against the offending IP once a threshold is met.

- Observed here is traffic from an ongoing DDoS against several DoD IPs. TUTELAGE is blocking the malicious IP from communicating with any DoD machines.
QUESTIONS?