

# Detecting Malicious Activity in Cross-Boundary Communications

Joel Hypolite

(703) 983-1089 • [jhypolite@mitre.org](mailto:jhypolite@mitre.org)

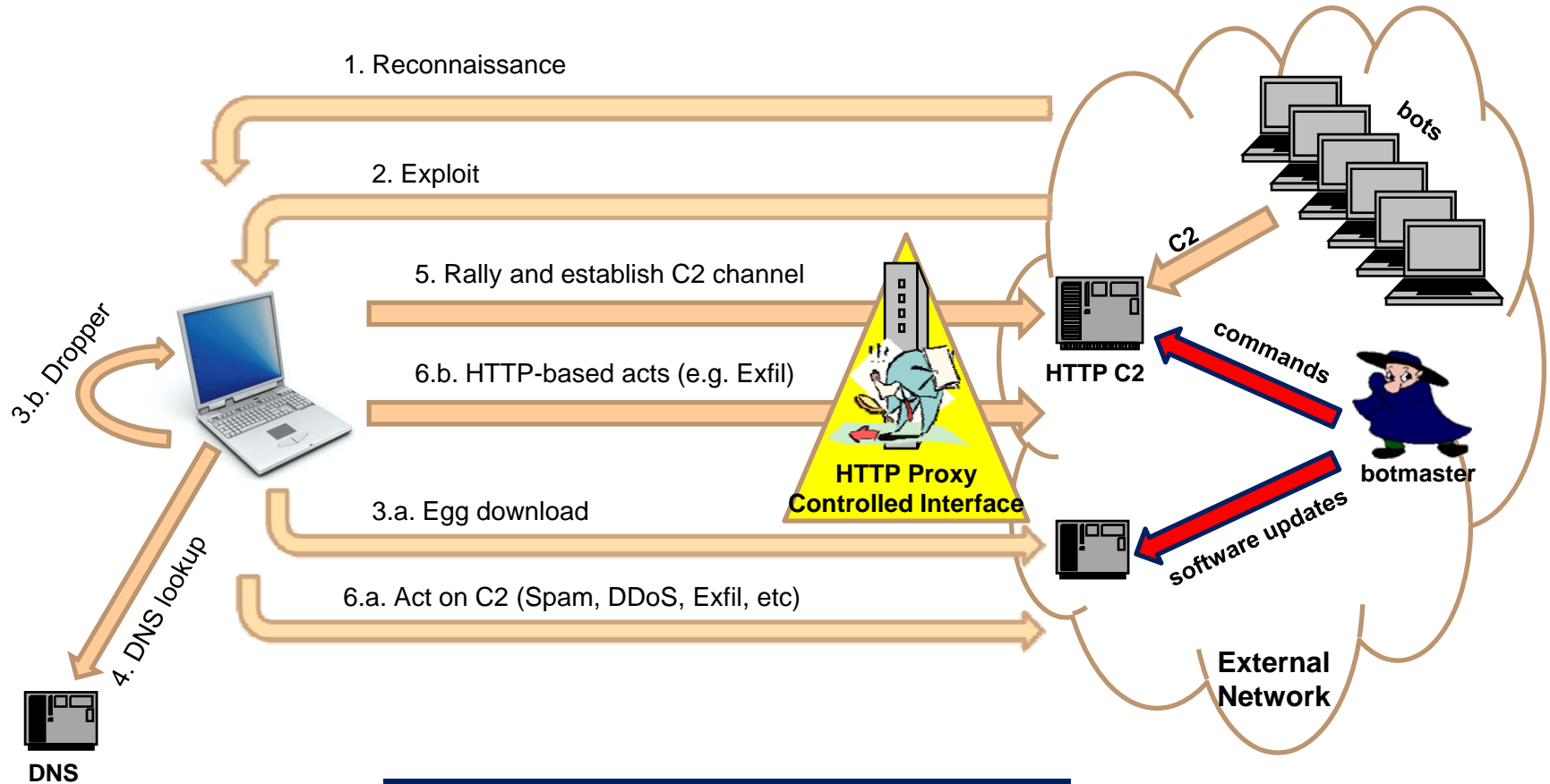
MSR



## Botnets are a key resource of the Advanced Cyber Threat

- **“This [botnet] attack went beyond simple mischief. It represented an actual threat to the national security and the ability of the Estonian government to govern its country.”**
  - **Michael Chertoff, DHS Secretary, remarks at RSA 2008**
- **Malicious adversary agents have a foothold inside the perimeter and attempt to communicate with the adversary**
  - **Command and Control (C2) and Data Exfiltration**
- **Existing network detection techniques lack analysis of data generated at the controlled interface**

# Background



**Life-Cycle of a Typical Bot**

# Objective



- **Detect botnet activity at the controlled interface**
- **Reverse engineer bots and analyze their application level (HTTP) communications through the controlled interface**
  - **Identify bots, C2 sites, egg download sites, etc.**
- **Demonstrate that active and passive monitoring techniques are effective at detecting malicious botnet activity**

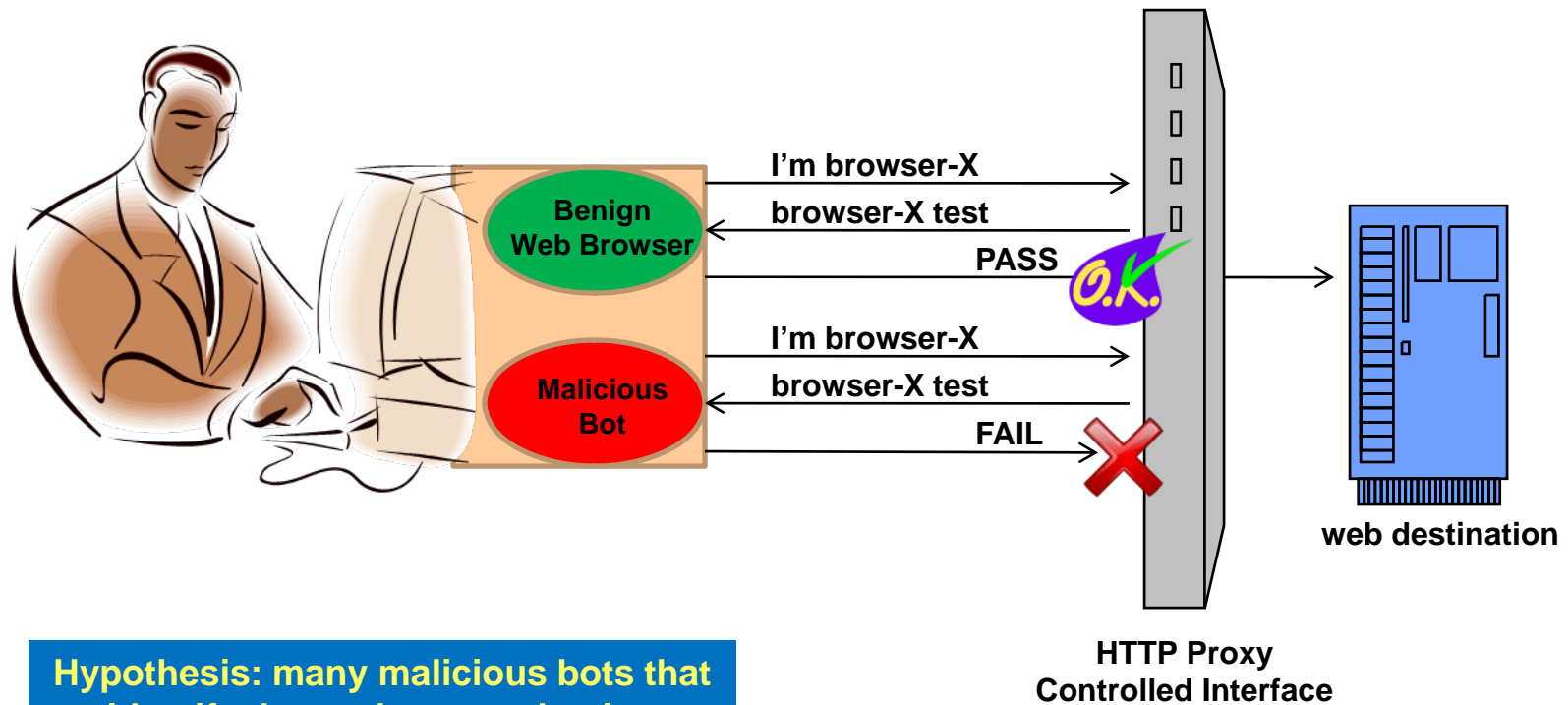
# Activities



- **Analyzed well-known bots**
  - **Identified and reverse engineered over a dozen malicious bots that use HTTP for the C2 channel**
  
- **Obtained large dataset**
  - **30 days of archived proxy logs from a large enterprise**
  
- **Developing bot detection techniques**
  - **active monitoring**
    - **e.g., injection of user agent challenges**
  - **passive monitoring**
    - **e.g., heuristics to look for destinations with low diversity**

# Highlight

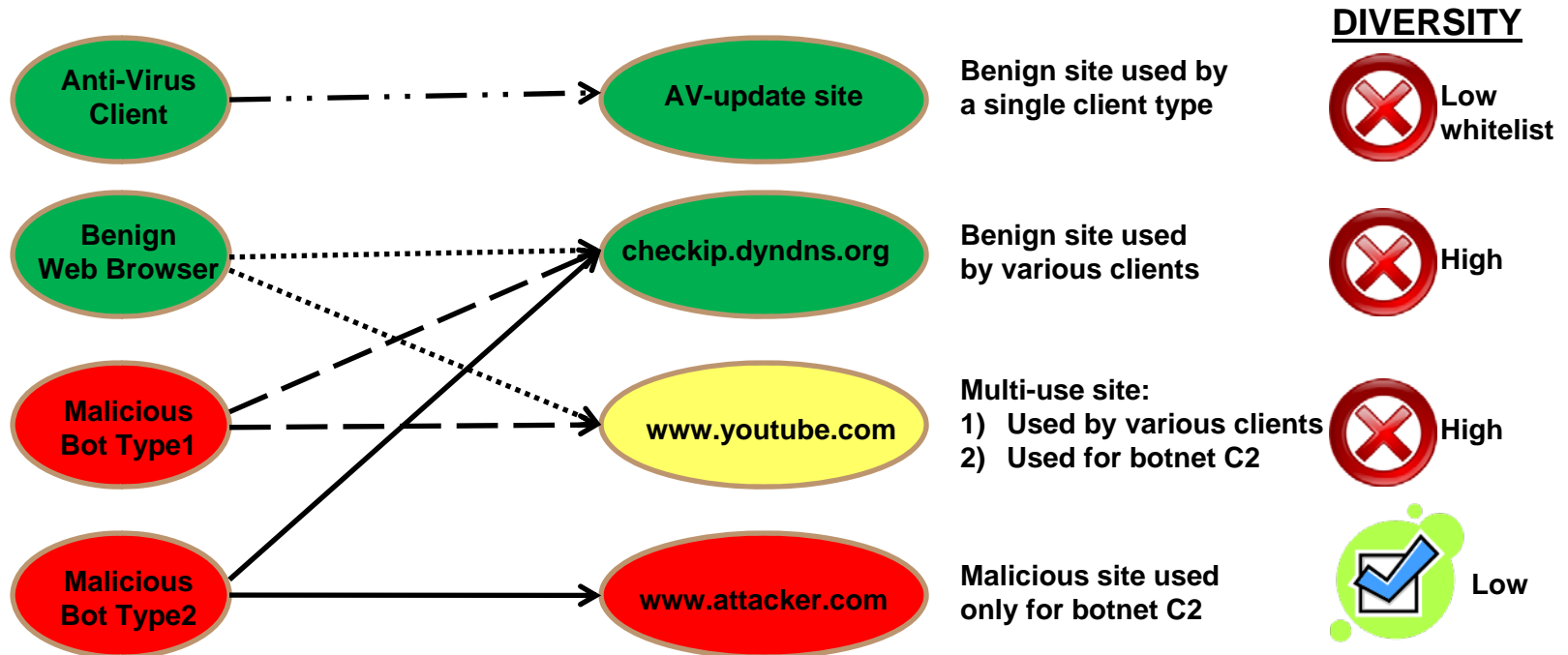
- Active Monitoring: User Agent Challenge



**Hypothesis: many malicious bots that identify themselves as a benign application do not implement the full capability of that application**

# Highlight

## ■ Passive Monitoring: Remote-Site Diversity Measurement



**Hypothesis: many malicious botnet HTTP C2 destinations only receive requests from bots, whereas many normal web destinations receive requests from a diverse set of user agents**

Bot Type 1 connects to youtube.com to read C2 posted as user comments. Such a C2 will work for similar sites, such as blogs, wikis, etc.

Bot Type 2 connects to a dedicated attacker site for botnet C2.

# Impacts



- **Advanced malware analysis environment with the capability to stage botnets, and to reverse engineer and monitor bots**
- **Botnet detection via active and passive monitoring**
  - **Exploring the limits of HTTP proxy log analysis to detect distributed multi-protocol threats such as bots/botnets**
  - **A capability to detect malicious activity circumventing a controlled interface raises the bar for botmasters**
  - **Will provide new detection capabilities for MITRE sponsors and Defense Industrial Base (DIB) partners**

# Future Plans

- Incorporate additional data sources and knowledge to improve detection strength

