

Using Honeyclients for Detection and Response Against New Attacks

Kathy Wang

703-983-6976 • knwang@mitre.org

Army-Contract MOIE

The logo for the MITRE Technology Program, featuring a stylized graphic of stacked blocks in yellow, orange, and blue to the left of the text.

MITRE
Technology
Program

Problem

- **We lack a proactive detection technology for client-side attacks**
- **We need to be able to proactively detect and characterize client-side attacks before we get hit**

Background

We know that client-side attacks are increasing in numbers and in sophistication:

The screenshot shows the InformationWeek website interface. At the top left is the CMP logo (United Business Media). To its right is the text "Part of the TechWeb Business Technology Network". The main header features the "InformationWeek" logo in red and black, with the tagline "BUSINESS INNOVATION POWERED BY TECHNOLOGY" below it. On the top right, there are navigation links for "HOME" and "EVENTS", and a search box. Below the header is a blue navigation bar with tabs for "WINDOWS", "SOFTWARE", "HARDWARE", "SECURITY", and "O". Underneath this is a grey bar with links for "Storage | PCs | Servers | Mobile | Networking | Desktops | RFID". The main content area is titled "SECURITY | VIRUSES AND PATCHES". The featured article is "From Russia With Malware" dated May 30, 2005. The article text reads: "An online site in Russia is using an affiliate model to spread malicious code, including back doors, other Trojans, spyware, and adware". The author is Gregg Keizer from TechWeb. To the right of the article are links for "E-Mail This Article", "Print This Article", "Discuss This Article", "Write To An Editor", and "Subscribe To InformationWeek". A short excerpt of the article is shown at the bottom: "An online business based in Russia is paying Web sites 6 cents for each machine they infect with adware and spyware, according to security researchers who call the practice 'awful.'"

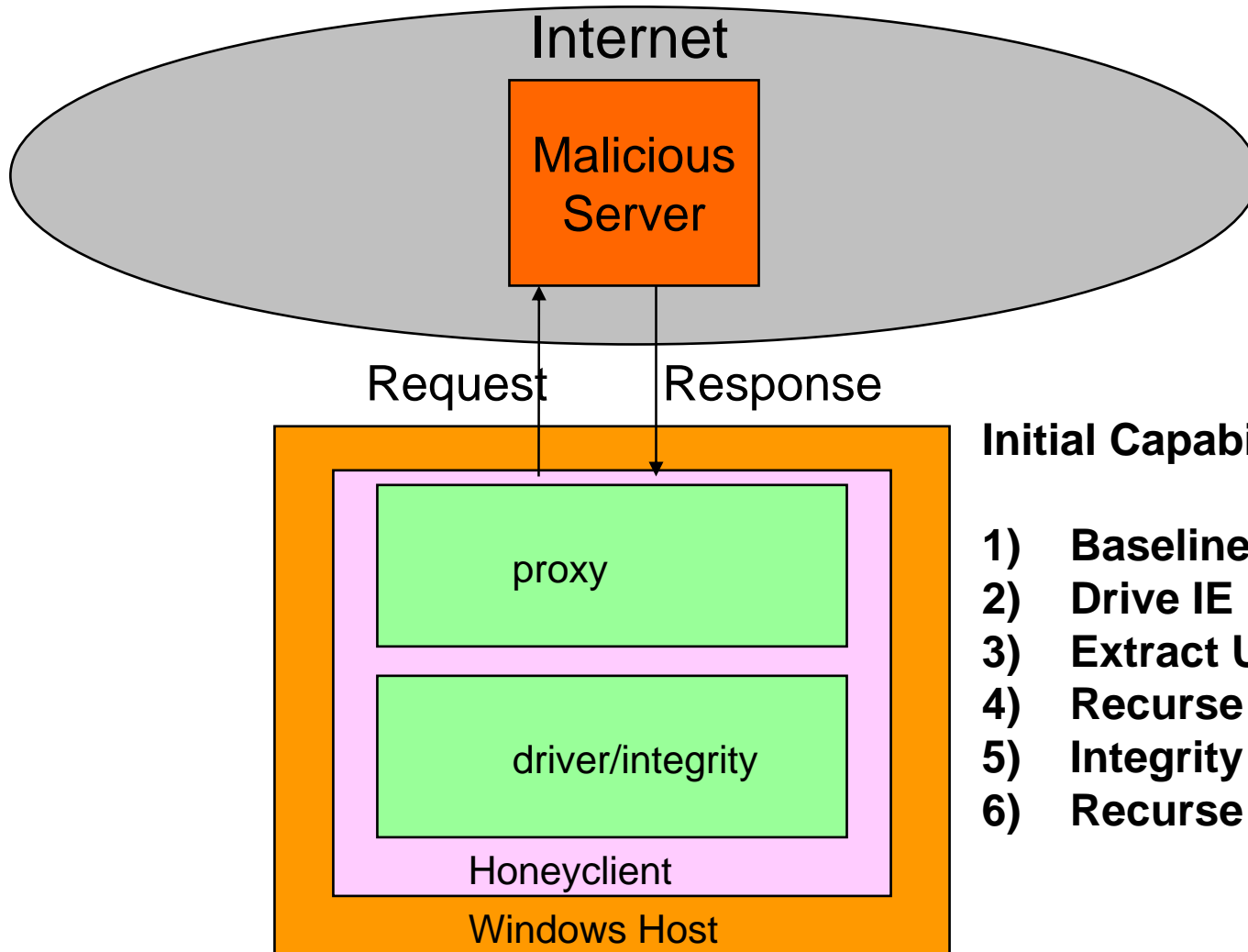
Objective

- **Develop attack detection and client-side exploit categorization tool**
 - **Initial prototype (written by PI) available**
 - **Want to add centralized logging, virtual machine re-imaging, exploit characterization and categorization**
- **Use honeyclients to achieve this objective**
 - **A honeyclient is a system that appears open to attacks**
 - **A honeyclient monitors host activity to proactively detect client-side exploits**

Activities

- Proactively detect new exploits – critical system files changed
- Capture exploit payload and effects
- Secure the honeyclient
- Start with IE client and build modular architecture to support other protocol clients (e.g. DNS, IM, chat clients)
- Perform controlled validation and then deploy live
- Disguise honeyclients to avoid detection

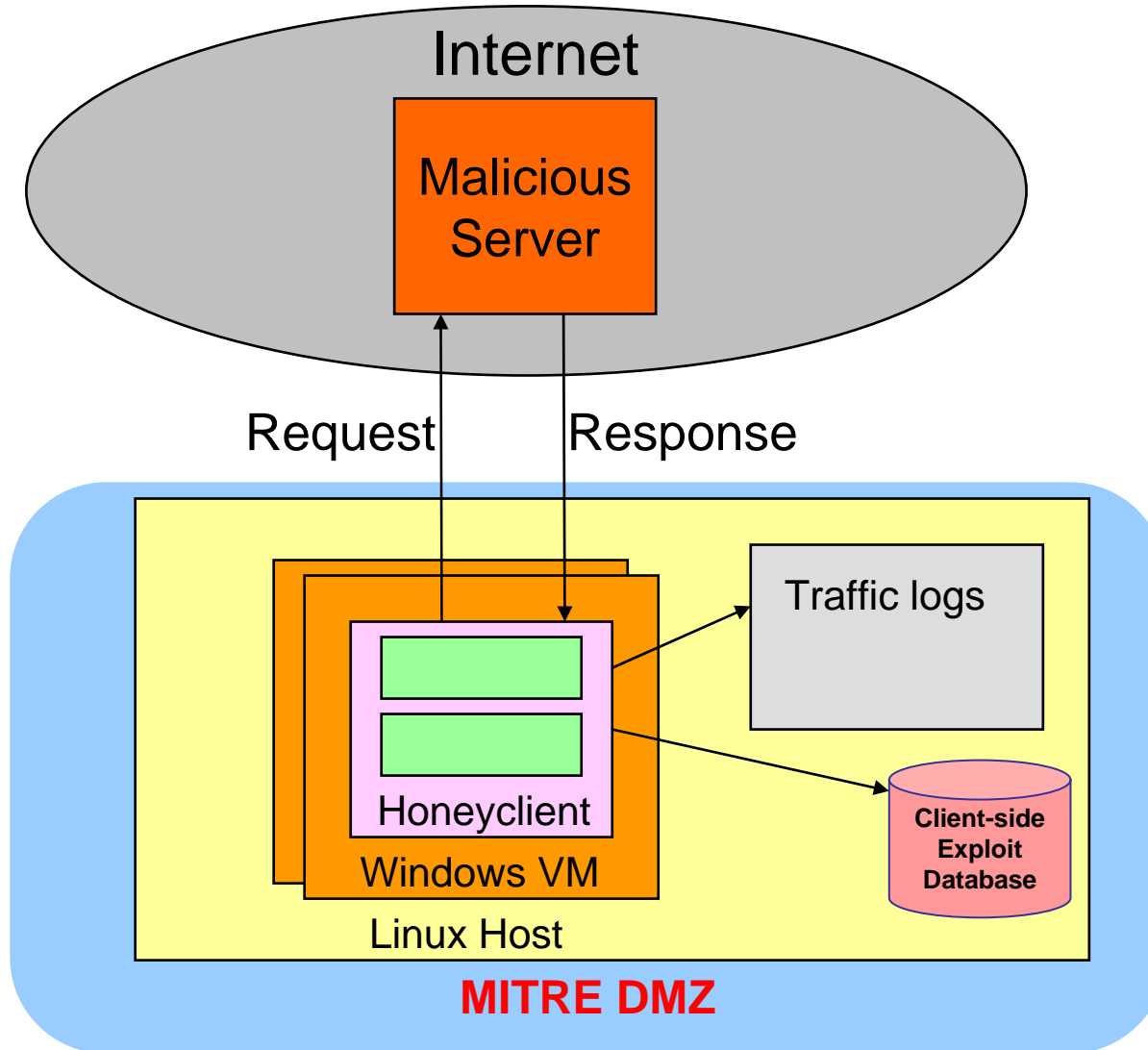
Initial Prototype



Initial Capabilities

- 1) **Baseline integrity**
- 2) **Drive IE**
- 3) **Extract URLs**
- 4) **Recurse (internal)**
- 5) **Integrity checks**
- 6) **Recurse (external)**

Completed Prototype



Additional Capabilities

- 7) Virtual host
- 8) Image rotation
- 9) Traffic history
- 10) Protective FW
- 11) Exploit DB
- 12) Modular clients
- 13) Secure logging
- 14) Memory checks

Extensive Testing

Impacts

- **Sponsors with network security management and defense missions will benefit directly from honeyclient technology**
- **Honeyclient technology will benefit MITRE initiatives as well**
 - **MITRE Corporate Security**
 - **MITRE Information Security Projects**
- **Products and standards**
 - **Contact vendors about new vulnerabilities in client applications**

Future – Distributed Honeyclients

