Beta Presentation
Command & Control Simulator

The Capstone Experience

Team Vectra
Trevor Davis
Ben Hayes
Nixon Holley
Ben Tuckey
Andrew Vandercar

Department of Computer Science and Engineering
Michigan State University
Fall 2023
Project Overview

• C2 channels are used by attackers to control compromised devices
• Lack of public C2 data available to analysts
• Application simulates C2 channels
• Configurable parameters which replicate real-world attack behavior
• Log network traffic for data display/analysis
• Web UI controls the application and visualizes logs
System Architecture

TCP, HTTP, HTTPS

Client.py

python

AWS

EC2 Instance: Server.py Flask App WebUI

MySQL

RDS Instance: MySQL Database
Simulation Overview

<table>
<thead>
<tr>
<th>Simulation Name</th>
<th>Status</th>
<th>Start Date</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>demo</td>
<td>ended</td>
<td>2023-11-13 17:04:48</td>
<td>View / Edit, Delete</td>
</tr>
<tr>
<td>trp_demo</td>
<td>running</td>
<td>2023-11-13 17:07:43</td>
<td>View / Edit, Delete</td>
</tr>
</tbody>
</table>
New Simulation
Simulation Details

Command and Control Simulator

Simulation: demo

<table>
<thead>
<tr>
<th>Start Time</th>
<th>Protocol</th>
<th>Number of Tunnels</th>
<th>Connection Type</th>
<th>Beacon Time</th>
<th>Jitter Amount</th>
<th>Padding Type</th>
<th>Padding Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>2023-11-13 17:04:48</td>
<td>http</td>
<td>2</td>
<td>long</td>
<td>8.0</td>
<td>2.0</td>
<td>Random</td>
<td>0</td>
</tr>
</tbody>
</table>

Pcap Data

Playbook

<table>
<thead>
<tr>
<th>Job Type</th>
<th>Start Time</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>InterCommand Delay</td>
<td>5</td>
<td>complete</td>
</tr>
<tr>
<td>Encrypt File System</td>
<td>3</td>
<td>complete</td>
</tr>
<tr>
<td>InterCommand Delay</td>
<td>10</td>
<td>complete</td>
</tr>
<tr>
<td>E frustrate Data</td>
<td>5</td>
<td>complete</td>
</tr>
</tbody>
</table>
What’s left to do?

• Stretch Goals
  ▪ HTTP versions 2 & 3
  ▪ Remote shell mode
  ▪ Clone simulation parameters
  ▪ Automate running multiple simulations

• Other Tasks
  ▪ Create software documentation
  ▪ Refactor & Clean up code
  ▪ Brainstorm additional features
Questions?