Implementation of DNS Sinkholes in Next-Generation Firewalls

Christian Tsirlis, Brad Wilson
Advisor: Jorge Crichigno

Department of Integrated Information Technology
University of South Carolina

December 2nd, 2021
Agenda

• Purpose
• Introduction
• Problem description
• Proposed solution and implementation
  • Anti-spyware profile
  • External dynamic list
• DNS Sinkhole Validation
  • Use of nslookup command
• Analyzing traffic logs
• Conclusion
Purpose

- Understand DNS Sinkholes
- Implement DNS Sinkholes in Security Policies
- Protect network from malicious attackers inside and outside of the network
- Analyze DNS and web browser traffic traversing the network
- Build stronger policies to minimize attacks
Introduction

- A DNS sinkhole is a technique used to protect hosts from malicious domains.
Problem Description

• Suspected malicious activity from internal network attempting to access malicious domains.

• Effectiveness of security policies using DNS sinkholes to protect internal network.
Proposed Solution and Implementation

• Sinkhole anti-spyware profile created.
  • Alerts network administrations and logs traffic.
  • Used in security policy to perform sinkhole action.

• Sinkhole external dynamic list created.
  • Unique list to test sinkhole effectiveness.
  • Used in anti-spyware profile to filter DNS request.
Proposed Solution and Implementation

• Security policy with anti-spyware profile attached.

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>any-zone-to-any-zone</td>
<td>any</td>
<td>any</td>
</tr>
<tr>
<td>2</td>
<td>intrazone-default</td>
<td>any</td>
<td>(intrazone)</td>
</tr>
<tr>
<td>3</td>
<td>interzone-default</td>
<td>any</td>
<td>any</td>
</tr>
</tbody>
</table>

• Closer look at the security policy rule.
  • Focusing on the Actions tab.
  • Anti-spyware was added as a profile setting.
DNS Sinkhole Validation

• How to verify?
  • nslookup returns the ip address of the requested domain.
  • We used the nslookup command to confirm if the sinkhole was working.

• Results
  • DNS Sinkhole works with nslookup.
  • Web browser can evade DNS sinkhole using encrypted web browser traffic.
Analyzing Traffic Logs

- Search traffic logs by “sinkhole” action.
- Ability to know the source address of DNS request.
- Provides the URL requested by client.
Conclusion

• Why is this work important?

  • Our test highlights, that there are some weaknesses in DNS sinkholes and how web browsers can encrypt data, which makes the domain request impossible to see.

• Future work includes deeper packet analysis

• Use of URL filtering with DNS sinkhole is effective

• Questions?

• Thank you for listening and watching