Sinkhole all the things!

Using a (DNS) Sinkhole to Detect and Respond to Malicious Activity
About Me

Stefan Hazenbroek GNFA GCFA GCWN CISSP

Cyber Defence Analyst at Shell
Agenda

• Intro
• What is a Sinkhole?
• Implementing a Sinkhole
• DNS Response Policy Zones
• Q&A
How DNS Works
Paul Vixie (CEO, Farsight Security):

“Most new domain names are malicious. Every day lots of new names are added to the global DNS, and most of them belong to scammers, spammers, e-criminals and speculators.”

Source: 2010-07-28 http://www.circleid.com/posts/20100728_taking_back_the_dns/
FREE ccTLDs

.tk - Tokelau
.ml - Mali
.gz - Gabon
.cf - Central African Republic
.gq - Equatorial Guinea
## The Web's Top 10 TLDs with Shady Sites*

<table>
<thead>
<tr>
<th>Rank</th>
<th>Top Level Domain Name</th>
<th>Percentage of Shady Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>.zip</td>
<td>100.00%</td>
</tr>
<tr>
<td>2</td>
<td>.review</td>
<td>100.00%</td>
</tr>
<tr>
<td>3</td>
<td>.country</td>
<td>99.97%</td>
</tr>
<tr>
<td>4</td>
<td>.kim</td>
<td>99.74%</td>
</tr>
<tr>
<td>5</td>
<td>.cricket</td>
<td>99.57%</td>
</tr>
<tr>
<td>6</td>
<td>.science</td>
<td>99.35%</td>
</tr>
<tr>
<td>7</td>
<td>.work</td>
<td>98.20%</td>
</tr>
<tr>
<td>8</td>
<td>.party</td>
<td>98.07%</td>
</tr>
<tr>
<td>9</td>
<td>.gq (Equatorial Guinea)</td>
<td>97.68%</td>
</tr>
<tr>
<td>10</td>
<td>.link</td>
<td>96.98%</td>
</tr>
</tbody>
</table>

* As of August 15, 2015 - Percentages are based on categorizations of web sites actually visited by our 75 million users. A TLD having 100 percent shady sites correlates to sites categorized by Blue Coat.
So, what if you didn’t block these?
Challenge:
If you have multiple recursive/caching DNS servers, how do you know who the source of a DNS query is?
How does a Sinkhole change that?
“DNS sinkhole or black hole DNS is used to spoof DNS servers to prevent resolving host names of the specified URLs. This can be achieved by configuring the DNS forwarder to return a false IP address to a specific URL”
Snort:
11/10-14:21:18.698583 "http_inspect: NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE",TCP,x.x.x.x,80,x.x.x.x,49446,3,9521
11/10-14:22:06.307412 "ET INFO WinHttp AutoProxy Request wpad.dat Possible BadTunnel",TCP,x.x.x.x,57327,1.2.3.4,80,2022913,12942

Fakenet:
11/10/17 11:20:45 AM [HTTPListener80] src_ip="x.x.x.x" src_port="42798" http_version="HTTP/1.1" uri="/" user-agent="Wget" listener="httplistener" host="checkip.dyndns.org" response_type="text/html" method="GET"

Sinkhole:
INFO:store:webcam="Yes" os="" campaign="HacKed_EE28CCBF" uname="Pwnage" timestamp="2017-11-10 08:29:20.044563" av="" ipaddr="x.x.x.x" cleanup="un'|'|~[endof]" cname="NYORE" variant="njrat" id="0.7d"
INFO:store:timestamp="2017-11-10 09:53:53.062412" ipaddr="x.x.x.x" variant="unknown" cleanup=""
INFO:store:usb="true - 1/21/2015" campaign="plus" uname="TESTUSER" timestamp="2017-11-10 11:04:26.256251" av="nan-av" ipaddr="x.x.x.x" cleanup="uninstall" os="Microsoft® Windows Vista™ Business" cname="TESTUSER-PC" variant="h-worm User-Agent v2" id="5FA690E3"
What do you need?
▪ Control over the DNS servers your clients use
▪ A server (or virtual machine) to use as destination instead of the original IP

• Recommended:
▪ Configure Snort/Surikata/Bro on the traffic
▪ Setup netflow collection (for example using bro/sflow)
▪ Setup packet capture (tcpdump or any other tool)
BUT WAIT

THERE'S MORE
DNS Response Policy Zones

• Allow a nameserver to overlay custom information on top of the DNS estate to provide alternate responses to queries. Another generic name for the DNS RPZ functionality is “DNS Firewall”

• Benefits:
  ▪ Automatically redirect traffic based on threat intel feed
  ▪ Redirect based on source or destination subnets