Measuring the Impact of a Successful DDoS Attack on the Customer Behavior of Managed DNS Service Providers

Abhishta
Roland van Rijswijk-Deij
Lambert J. M. Nieuwenhuis
A human DDoS?
Stakeholders of a DDoS attack

Attacker Attacks → Victim → Targeted Victim → Collateral Victims → Customers of Victim

DDoS protection companies

Pays

Protects

Provides Service
Damages

- Direct Damages
  - Loss due to infrastructure downtime.
  - Paid ransom.
  - Customer compensation etc.

- Indirect Damages
  - Reputational damage
  - Impact on stock price etc.
Questions

- Is there an impact of a successful DDoS attack on the customer behavior of a MDNS service provider? If yes-
  - How can we measure it?
  - Is the impact statistically significant?
  - What choices do the customers of the attacked MDNS providers make after the attack?
Is there an impact of a successful DDoS attack on the customer behavior of a MDNS service provider?
Value of a MDNS

Service availability is subject to DDoS risk

Service availability, albeit DDoS

ANS: Authoritative Name Server
MANS: Managed Authoritative Name Server
How can we measure it?
Modelling Customer Behaviour
Active DNS Measurements

OpenINTEL Dataset[#]

Trend and Event Window

Trend Period: $[-200, -1]$  
Event Period: $[1, 20]$
Large attacks on MDNS service providers

Attack on NS1 on 16\textsuperscript{th} May 2016.
- Had ~3150 domains (.com/.org/.net) one day before the attack.
- ~98% domains were exclusive.

Attack on Dyn on 21\textsuperscript{st} October 2016.
- Had ~167,000 domains (.com/.org/.net) one day before the attack.
- ~84% domains were exclusive.
Impact on total number of customers

NS1

Dyn
Change in behaviour!

Exclusive Customers

Non-Exclusive Customers
Being Non-exclusive...

**NS1**

**Dyn**
Domains that stopped using the services of the MDNS provider.
Is the impact statistically significant?
Statistical significance of the change in behavior variables.

- $H_{a1}$: There is no change in the behavior of domains that use an MDNS provider after a DDoS attack.
- $H_{a2}$: There is no change in the mean of behavior variables in the trend and the event period.

Table: Results of T-test on behavioral variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Trend Period Mean</th>
<th>Event Period Mean</th>
<th>t-statistic</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dyn</td>
<td>NS1</td>
<td>Dyn</td>
</tr>
<tr>
<td>△ Domains</td>
<td>127.05</td>
<td>6.87</td>
<td>-9.545</td>
</tr>
<tr>
<td>△ Exclusive Domains</td>
<td>126.985</td>
<td>6.80</td>
<td>-127.82</td>
</tr>
<tr>
<td>△ Nonexclusive Domains</td>
<td>0.065</td>
<td>0.07</td>
<td>118.27</td>
</tr>
<tr>
<td>ExExclusive</td>
<td>66.63</td>
<td>2.85</td>
<td>212.59</td>
</tr>
<tr>
<td>ExNonexclusive</td>
<td>10.68</td>
<td>0.24</td>
<td>7.682</td>
</tr>
<tr>
<td>NewExclusive</td>
<td>194.29</td>
<td>9.68</td>
<td>195.4</td>
</tr>
<tr>
<td>NewNonexclusive</td>
<td>10.07</td>
<td>0.29</td>
<td>15.32</td>
</tr>
<tr>
<td>ToNonexclusive</td>
<td>3.8</td>
<td>0.3</td>
<td>114</td>
</tr>
<tr>
<td>ToExclusive</td>
<td>3.1</td>
<td>0.27</td>
<td>3.36</td>
</tr>
</tbody>
</table>

*p-value ≤ 0.05
Choice of Secondary DNS provider
Top Secondary DNS choices before the attack.

**NS1**

<table>
<thead>
<tr>
<th>Service</th>
<th>Managed</th>
<th>Unprotected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon</td>
<td>80</td>
<td>20</td>
</tr>
<tr>
<td>Dyn</td>
<td>20</td>
<td>80</td>
</tr>
<tr>
<td>BuddyDNS</td>
<td>10</td>
<td>100</td>
</tr>
<tr>
<td>Pulsepoint</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>Verisign</td>
<td>50</td>
<td>50</td>
</tr>
</tbody>
</table>

**Dyn**

<table>
<thead>
<tr>
<th>Service</th>
<th>Managed</th>
<th>Unprotected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ultradns</td>
<td>12000</td>
<td>1000</td>
</tr>
<tr>
<td>IBM</td>
<td>800</td>
<td>8000</td>
</tr>
<tr>
<td>Verisign</td>
<td>1000</td>
<td>100</td>
</tr>
<tr>
<td>DNSmadeeasy</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>NS1</td>
<td>50</td>
<td>50</td>
</tr>
</tbody>
</table>
Top Secondary DNS choices after the attack.

**NS1**

- Dyn (Managed: 35, Unprotected: 0)
- Amazon (Managed: 15, Unprotected: 0)
- ClouDNS (Managed: 5, Unprotected: 0)
- DNSmadeeasy (Managed: 0, Unprotected: 0)
- LinkedIn (Managed: 0, Unprotected: 0)

**Dyn**

- DNSmadeeasy (Managed: 1200, Unprotected: 0)
- Ultradns (Managed: 600, Unprotected: 0)
- Amazon (Managed: 400, Unprotected: 0)
- NS1 (Managed: 200, Unprotected: 0)
- Akamai (Managed: 100, Unprotected: 0)
Applications
Loss of Customers for Dyn

By the most conservative of estimates, Dyn lost ~2000 domains due to single successful attack event!
Take Away

If we then focus on the aftermath of the attack, we observe a number of statistically significant changes:

- A significant number of MDNS customers that were using Dyn’s or NS1’s service exclusively switch to non-exclusive use in the aftermath of the attack. (Lasting change)
- No significant changes in the behaviour of Dyn customers that were already non-exclusive users.
- In terms of risk management, using multiple providers is a good strategy.
- Most of the customers that became non-exclusive after the attack on NS1 and Dyn chose an MDNS service provider as a secondary DNS to further reduce the risk of downtime.
Thank You

Contact: s.abhishta@utwente.nl
Website: www.abhishta.org