UNIVERSITY OF TWENTE.

Open INTEL

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

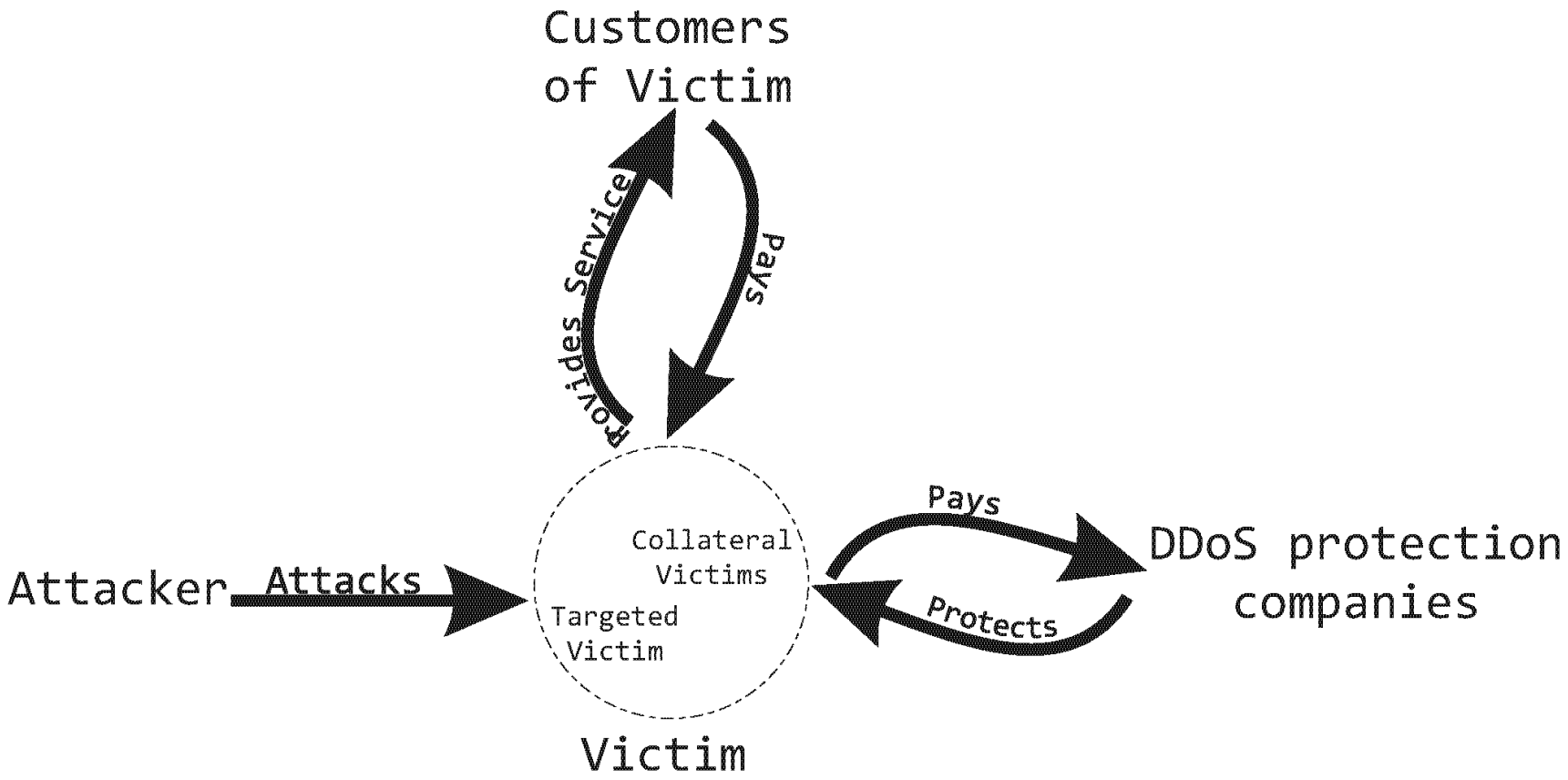
Abhishta

Roland van Rijswijk-Deij

Lambert J. M. Nieuwenhuis

A human DDoS?

Stakeholders of a DDoS attack



Damages

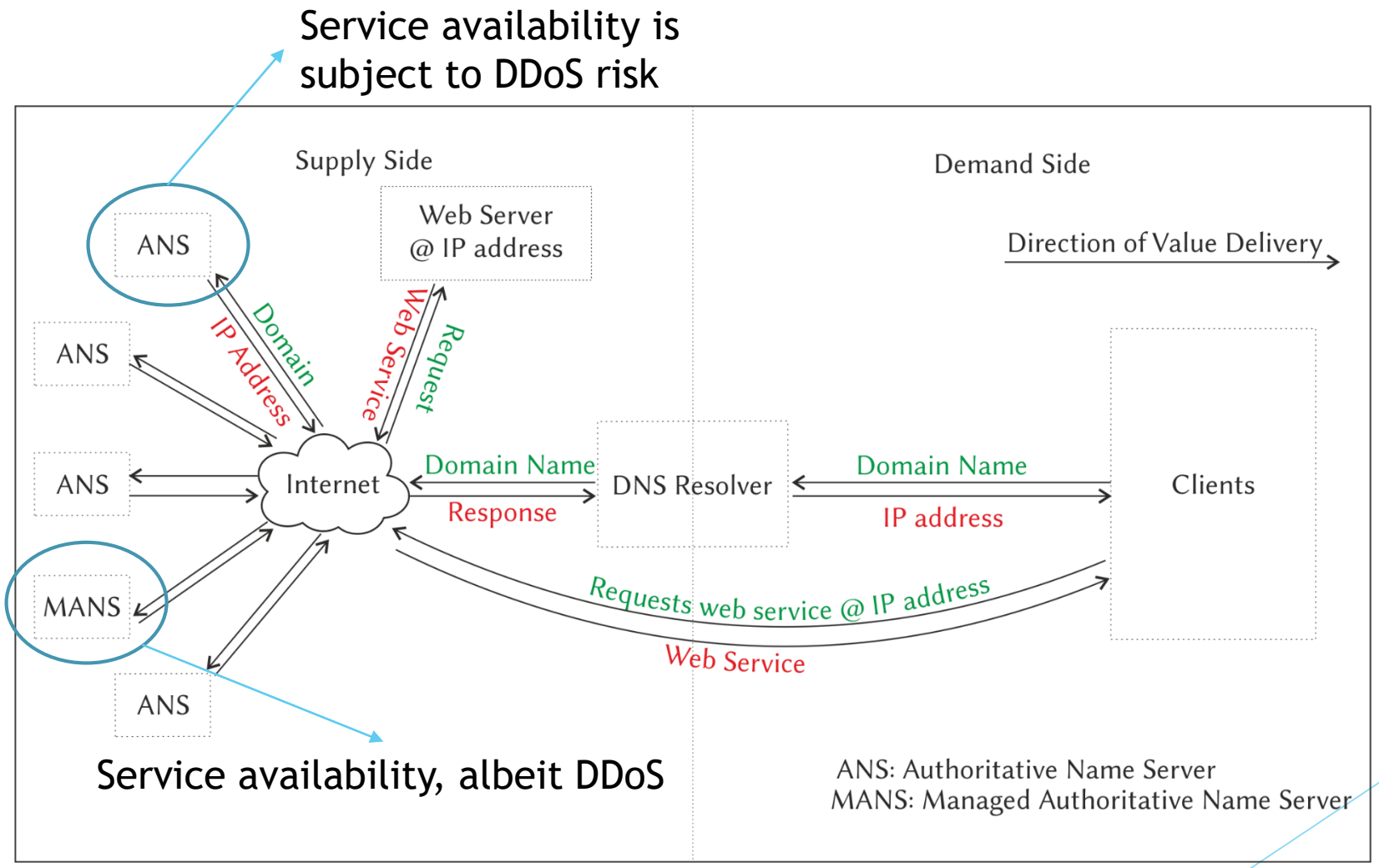
- Direct Damages
  - Loss due to infrastructure downtime.
  - Paid ransom.
  - Customer compensation etc.
- Indirect Damages
  - Reputational damage
  - Impact on stock price etc.

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?

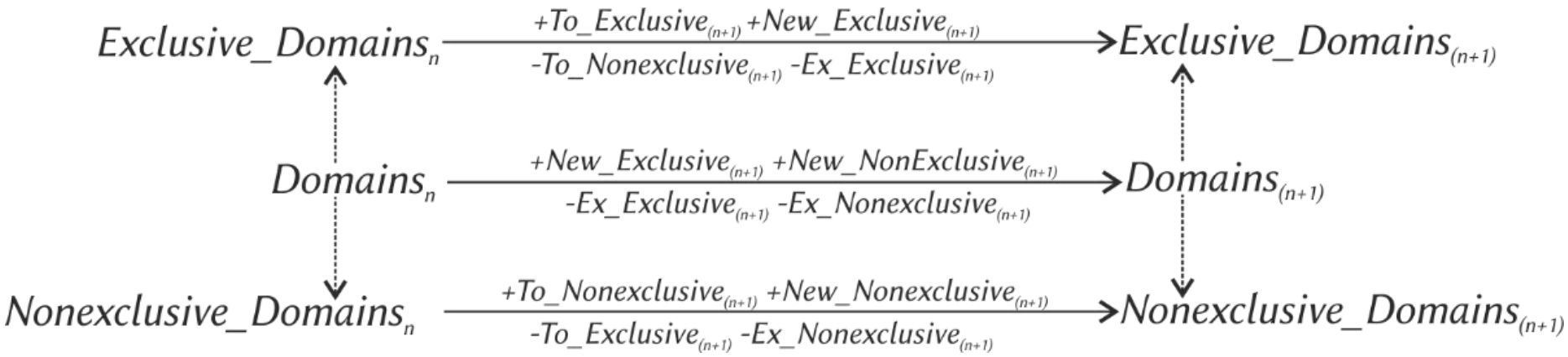
Is there an impact of a successful DDoS attack on the customer behavior of a MDNS service provider?

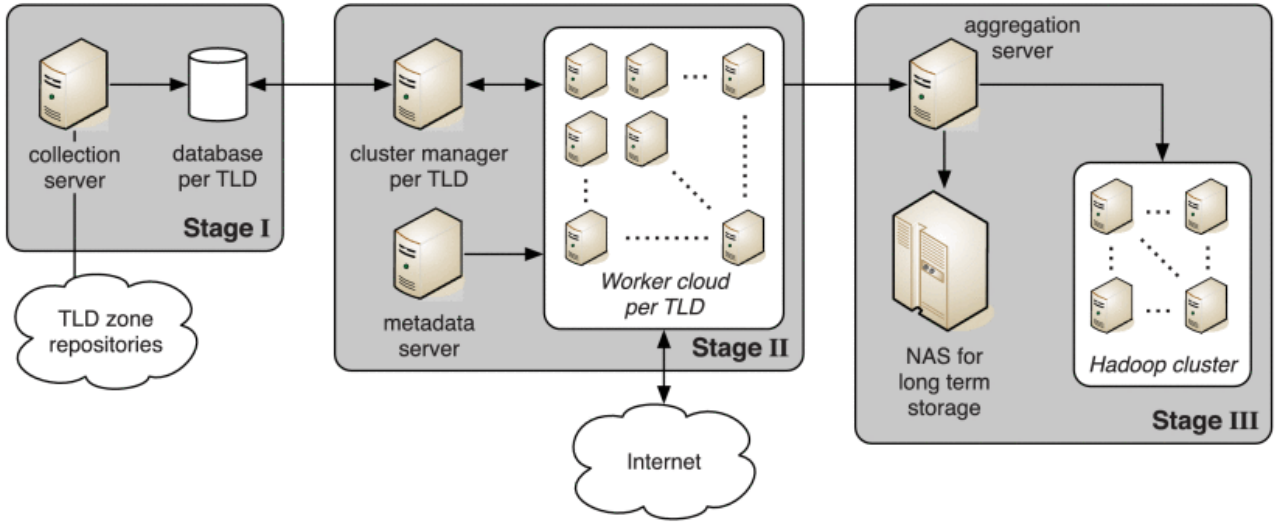
Value of a MDNS



How can we measure it?

Modelling Customer Behaviour



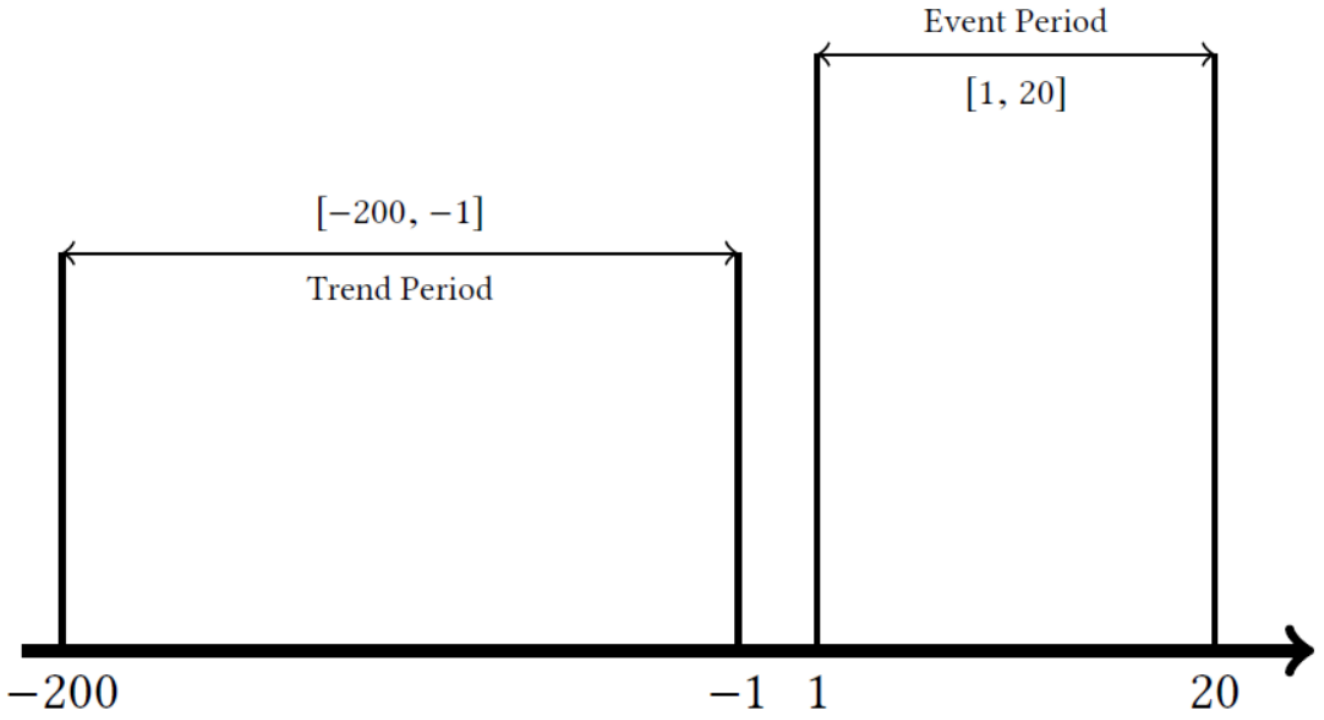


Active DNS Measurements

OpenINTEL Dataset[#]

[#] R. van Rijswijk-Deij, M. Jonker, A. Sperotto and A. Pras, "A High-Performance, Scalable Infrastructure for Large-Scale Active DNS Measurements," in *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 6, pp. 1877-1888, June 2016.

Trend and Event Window



Large attacks on MDNS service providers

Attack on NS1 on 16th May 2016.

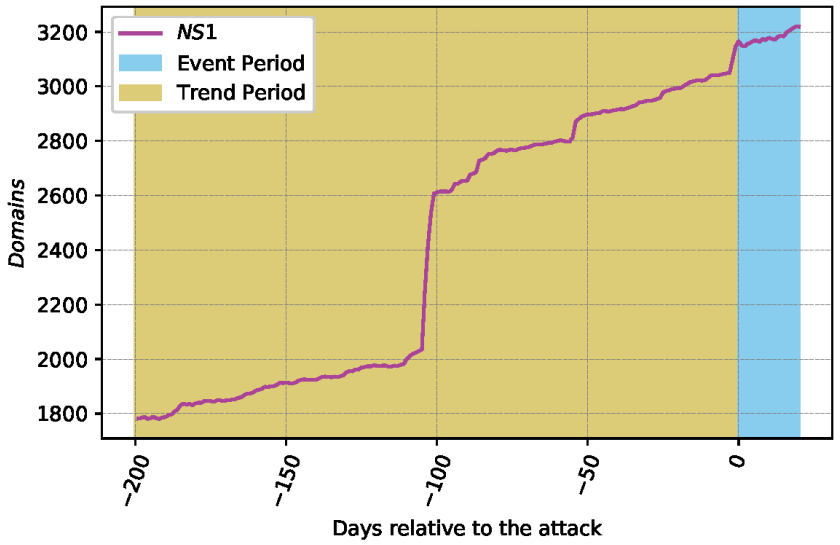
- Had ~3150 domains (.com/.org/.net) one day before the attack.
- ~98% domains were exclusive.

Attack on Dyn on 21st October 2016.

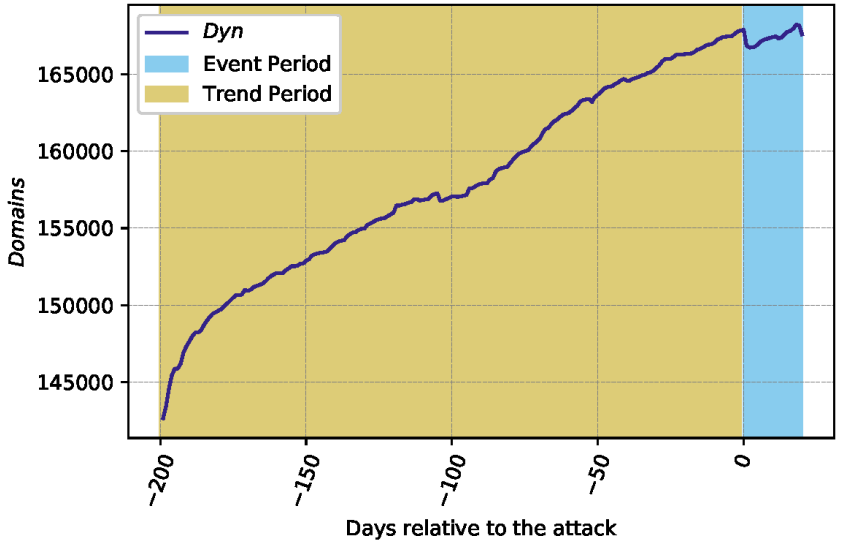
- Had ~167,000 domains (.com/.org/.net) one day before the attack.
- ~84% domains were exclusive.

Impact on total number of customers

NS1

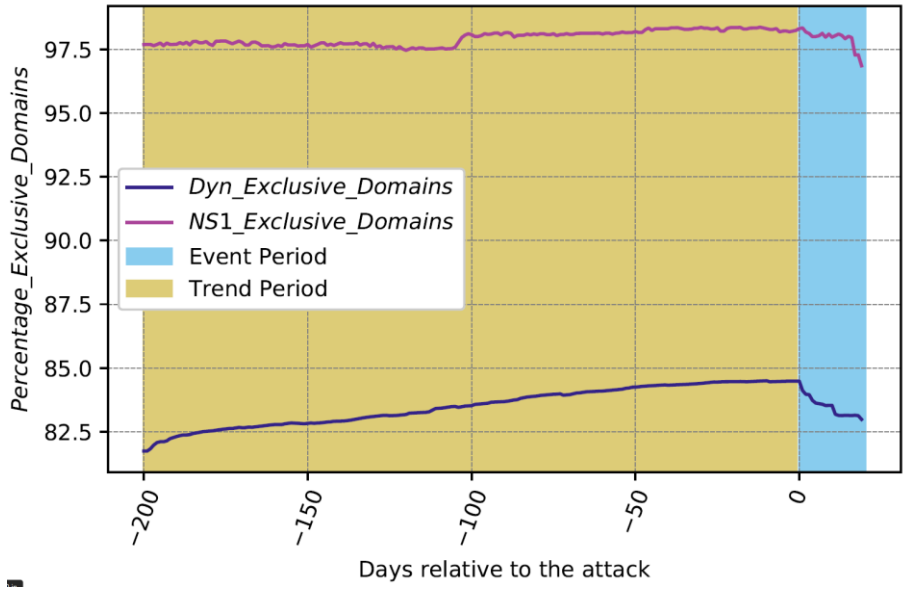


Dyn

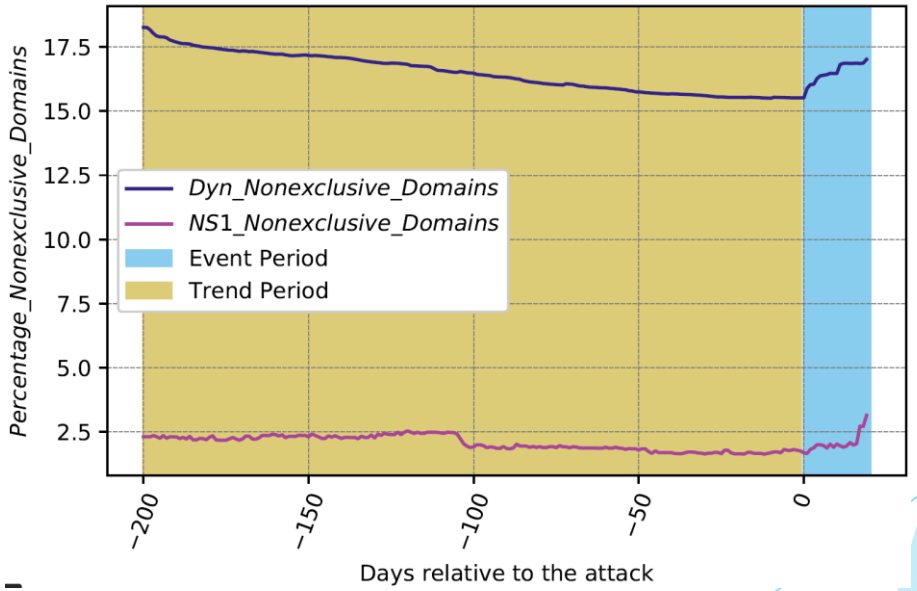


Change in behaviour!

Exclusive Customers

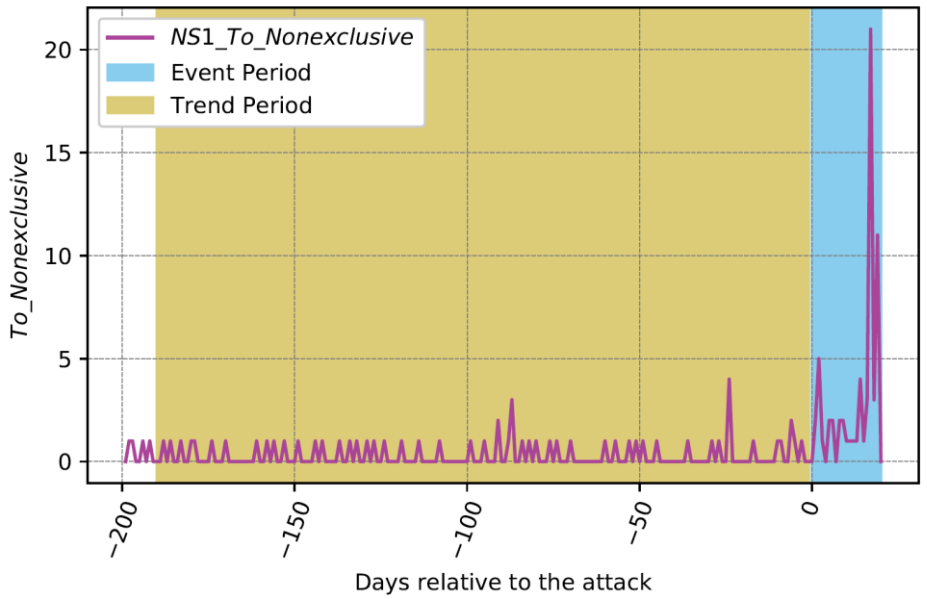


Non-Exclusive Customers

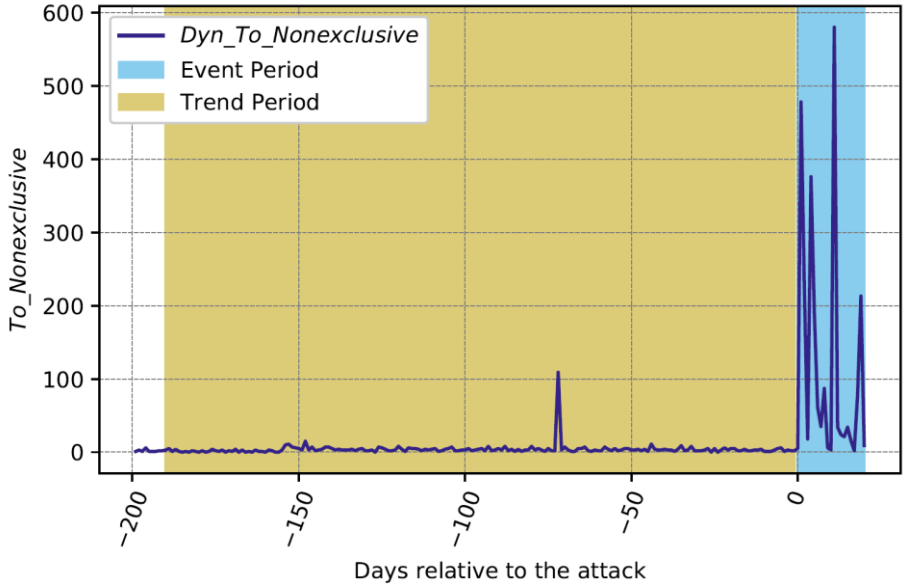


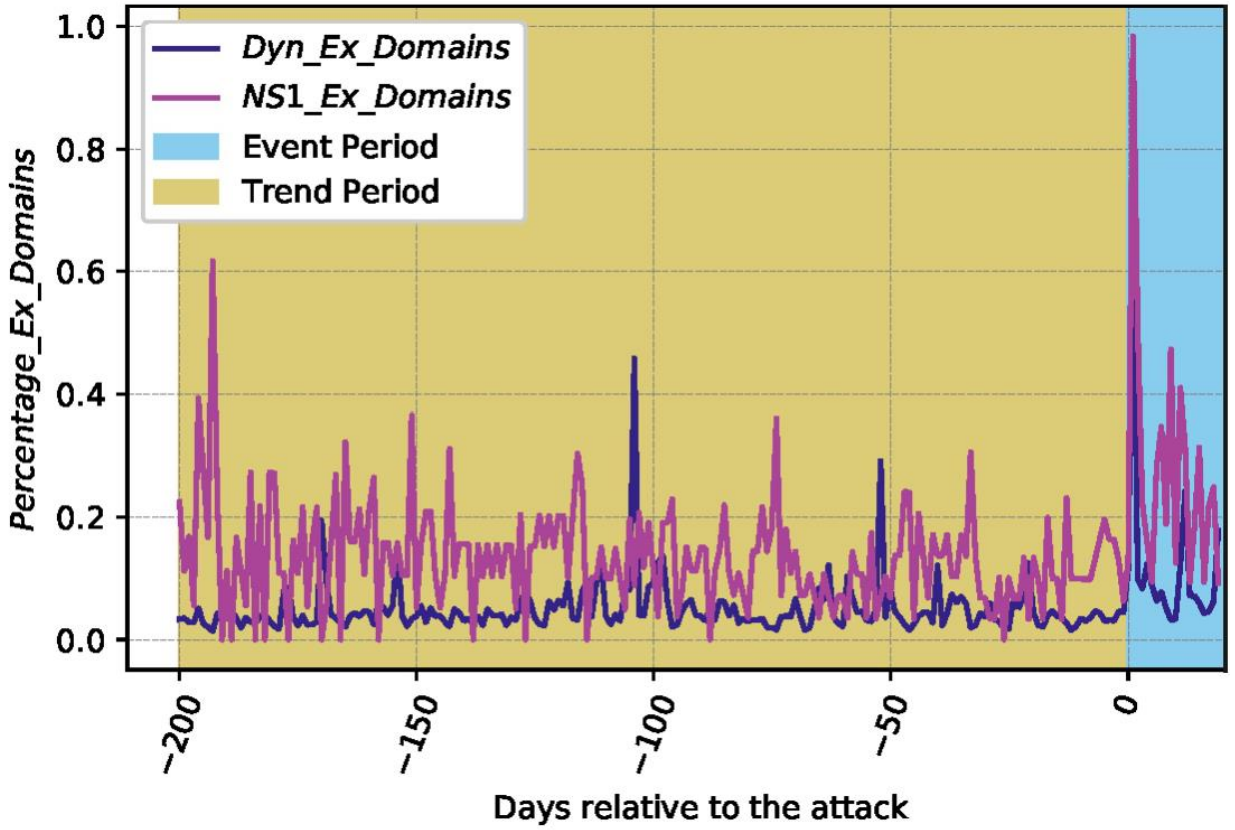
Being Non-exclusive…

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

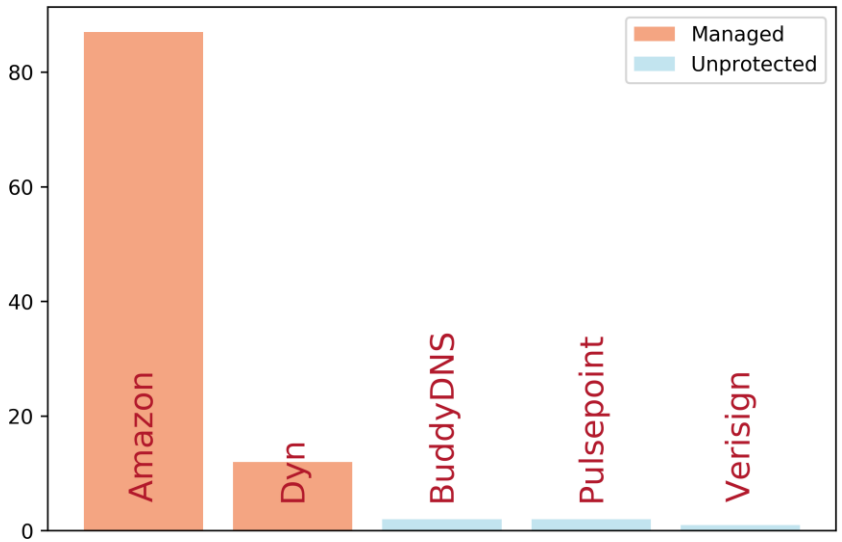
Variable	Trend Period Mean		Event Period Mean		t-statistic	
	Dyn	NS1	Dyn	NS1	Dyn	NS1
Δ *Domains*	127.05	6.87	-9.545	3.42	2.229*	1.45
Δ *Exclusive_Domains*	126.985	6.80	-127.82	1.42	3.16*	2.18*
Δ *Nonexclusive_Domains*	0.065	0.07	118.27	2	−3.341*	−1.42
Ex_Exclusive	66.63	2.85	212.59	5.47	−2.595*	−2.02*
Ex_Nonexclusive	10.68	0.24	7.682	3.19	1.93	−7.32*
New_Exclusive	194.29	9.68	195.4	8.90	-0.057	0.40
New_Nonexclusive	10.07	0.29	15.32	3.19	−2.49*	−8.1*
To_Nonexclusive	3.8	0.3	114	3	−3.12*	−2.57*
To_Exclusive	3.1	0.27	3.36	1	-0.44	-5.1

*p -value ≤ 0.05

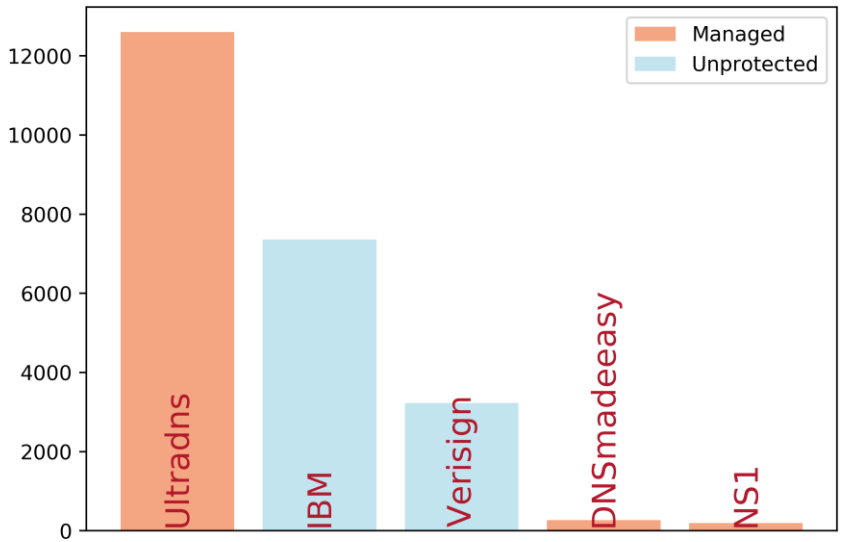
Choice of Secondary DNS provider

Top Secondary DNS choices before the attack.

NS1

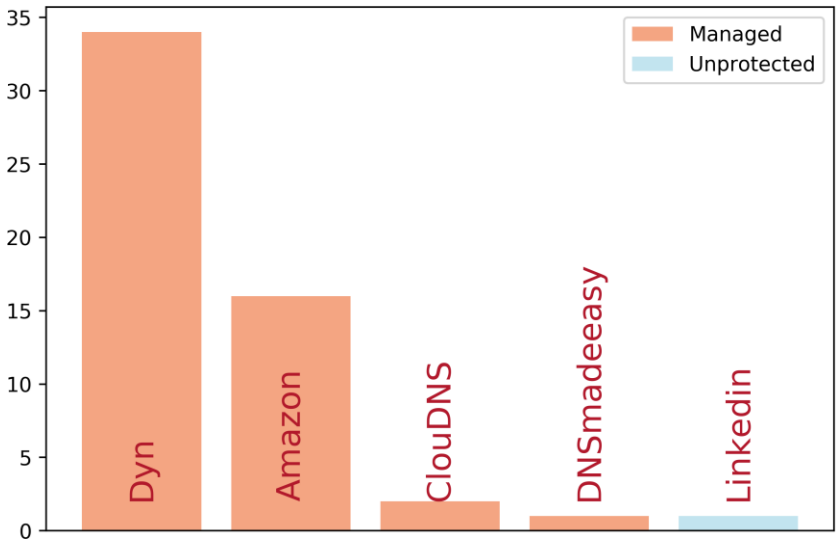


Dyn

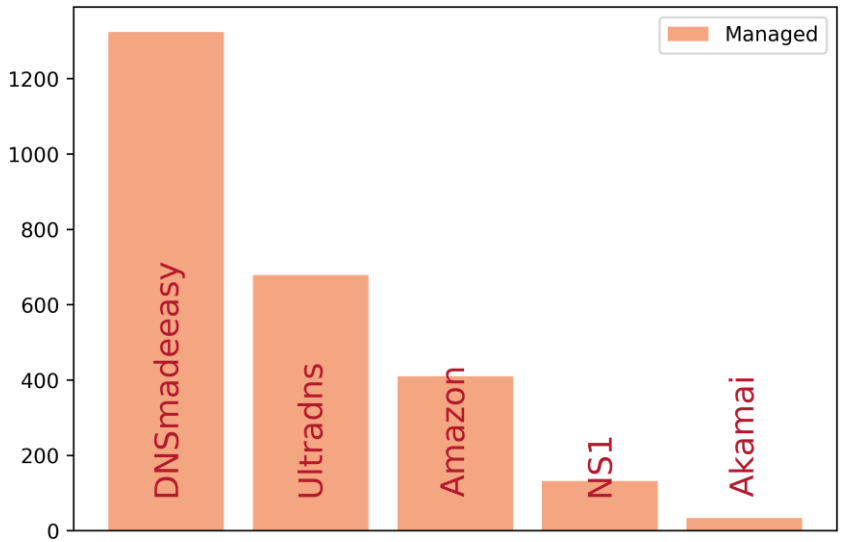


Top Secondary DNS choices after the attack.

NS1

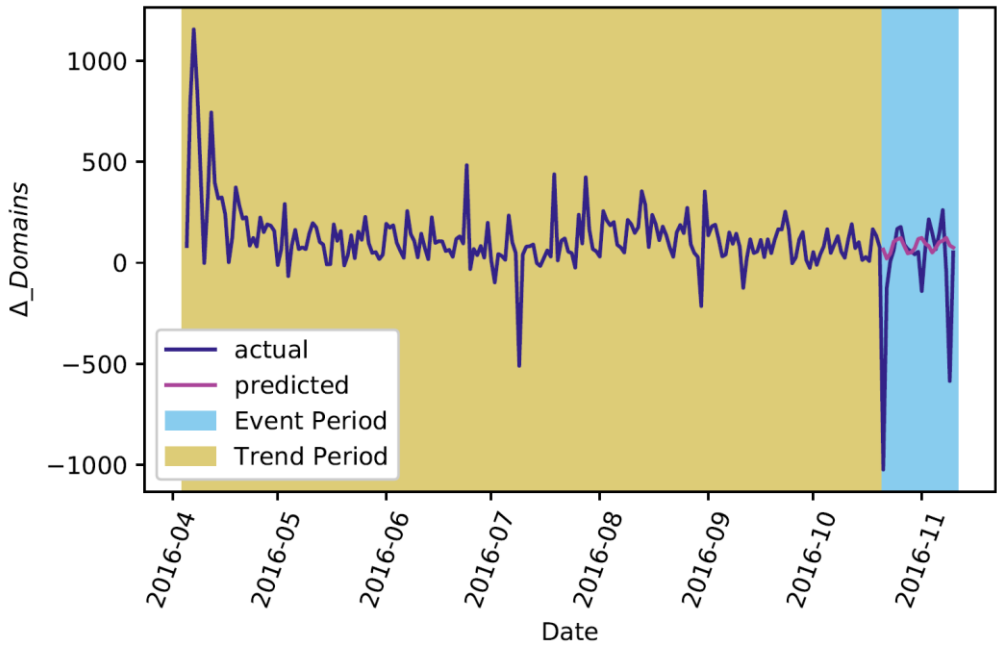


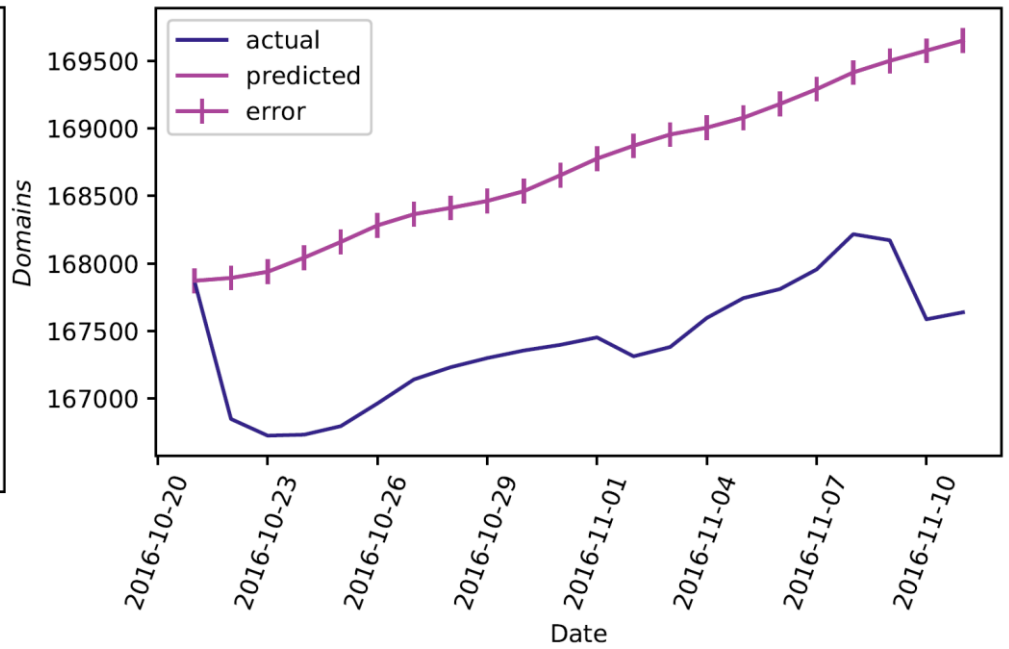
Dyn



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