Melting the Snow: Detecting Snowshoe Spam Domains Using Active DNS Measurements

Olivier van der Toorn <o.i.vandertoorn@utwente.nl>
November 13, 2018

University of Twente, Design and Analysis of Communication Systems

NOMS 2018
Introduction
Re: Your Abandoned Package For Delivery

Mr. Joseph Scott <Scott@world.sps.ne.jp>

Why is this message in Spam? It’s similar to messages that were detected by our spam filters. Learn more

To:

April 5 (1 day ago)

Re: Your Abandoned Package For Delivery

I have very vital information to give you, but first I must have your trust before I review it to you because it may cause me my job, so I need somebody that I can trust for me to be able to review the secret to you.

I am Mr. Joseph Scott, head of luggage/baggage storage facilities here at the McCarran International Airport, Nevada USA. During my recent withheld package routine check at the Airport Storage Vault, I discovered an abandoned shipment from a Diplomat from London and when scanned it revealed an undisclosed sum of money in a metal trunk box. The consignment was abandoned because the Contents of the consignment was not properly declared by the consignee as “MONEY” rather it was declared as personal effect to avoid interrogation and also the inability of the diplomat to pay for the United States Non Inspection Charges which is $3,700USD. On my assumption the consignment is still left in our Storage House here at the International Airport Nevada till date. The details of the consignment including your name, your email address and the official documents from the United Nations office in Geneva are tagged on the Trunk Box.

However, to enable me confirm if you are the actual recipient of this consignment as the assistant director of the Inspection Unit, I will advise you provide your current Phone Number and Fall Address, to enable me cross check if it corresponds with the address on the official documents including the name of nearest Airport around your city. Please note that this consignment is supposed to have been returned to the United States Treasury Department as unclaimed delivery due to the delays in concluding the clearance processes so as a result of this, I will not be able to receive your details on my official email account. So in order words to enable me cross check your details, I will advise you send the required details to my private email address for quick processing and response. Once I confirm you as the actual recipient of the trunk Box, it can get everything concluded within 48 hours upon your acceptance and proceed to your address for delivery.

KINDLY FILL IN THE FOLLOWING INFORMATION:

Your Full Name:
Your Country:
Your Direct Telephone Numbers:
Your Direct Office Phone Numbers:
Mobile Phone Number:
Your Current Home Address:
Your Office Address:
Your age:

Lastly, be informed that the reason I have taken it upon myself to contact you personally about this abandoned consignment is because I want us to transact this business and share the money 80% for you and 20% for me since the consignment has not yet been returned to the United States Treasury Department after being abandoned by the diplomat so immediately the confirmation is made, I will go ahead and pay for the United States Non Inspection Fee of $3,700 dollars and arrange for the box to be delivered to your doorstep. Or I can bring it by myself to avoid any more trouble but you have to assure me of my 20% share.

I wait to hear from you urgently if you are still alive and I will appreciate if we can keep this deal confidential. For further directives Email: josephscott870@gmail.com. You can call me on my telephone number: +1 762 763 7639 for verbal conversation. Please if am not available to accept your call, please and drop a message or send me a text.

Thank you.
<table>
<thead>
<tr>
<th>Name</th>
<th>Subject</th>
<th>Email Address</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mr. Joseph Scott</td>
<td>Re: Your Abandoned Package For Delivery - Re: Your Abandoned Package For Delivery</td>
<td><a href="mailto:josephscott@gmail.com">josephscott@gmail.com</a></td>
<td>Apr 5</td>
</tr>
<tr>
<td>UN OFFICE FILE</td>
<td>Contact ORA Bank for your ATM Card - New Secretary-General Antonio Guterres (UNITED NATION COMPENSATION COMMITTEE PROGRAMME) UNITED STATES REGIONAL HEADQUARTER IN AFFILIATION WITH THE</td>
<td><a href="mailto:unofficefile@un.org">unofficefile@un.org</a></td>
<td>Apr 4</td>
</tr>
<tr>
<td>Evelyn Lai</td>
<td>Business proposal - Hello, I have a business proposal of great benefit for both of us. Contact me for details. Email: <a href="mailto:evelynlai1978@gmail.com">evelynlai1978@gmail.com</a> With Kind Regards. Ms. Evelyn Lai</td>
<td><a href="mailto:evelynlai1978@gmail.com">evelynlai1978@gmail.com</a></td>
<td>Apr 2</td>
</tr>
<tr>
<td>Pedro SANCHEZ (2)</td>
<td>BATCH NUMBER:LT0/17/2017-5RDEU - INTERNATIONAL LOTTO/EUROMILLION PROGRAMME INTERNATIONALE PROMOTION-GEWINNUTEILUNG REFERENZ NUMMER:RPCH0/1975D00145 ESP BATCH NUMBER:LT1</td>
<td><a href="mailto:pedro.sanchez@usa.com">pedro.sanchez@usa.com</a></td>
<td>Mar 31</td>
</tr>
<tr>
<td>Cpt. Stephen Laurence</td>
<td>God bless you and America!!! - Hello Dear, I apologize if the content of my email is contrary to your moral ethics but I find it pleasurable to offer you my partnership in business. I am Cpt. Stephen Laurence, an officer in the US</td>
<td><a href="mailto:cpt.stephen.laurence@usarmy.com">cpt.stephen.laurence@usarmy.com</a></td>
<td>Mar 31</td>
</tr>
<tr>
<td>Blood Sugar Blueprint</td>
<td>Urgent news about Metformin - I track that lets you eat sweets without spiking blood-sugar</td>
<td><a href="mailto:bloodsugarblueprint@gmail.com">bloodsugarblueprint@gmail.com</a></td>
<td>Mar 30</td>
</tr>
<tr>
<td>(unknown sender)</td>
<td>Attention: Beneficiary - Attention: Beneficiary. We received a payment instruction from the Debt Reconciliation Committee of African Union in conjunction with the International Monetary Fund (IMF) to credit your account with</td>
<td><a href="mailto:unknownsender@outlook.com">unknownsender@outlook.com</a></td>
<td>Mar 29</td>
</tr>
<tr>
<td><a href="mailto:dutch.guilty@yahoo.com">dutch.guilty@yahoo.com</a></td>
<td>crash with installing 18.04 on enabling format - crash with installing 18.04 on enabling format</td>
<td><a href="mailto:dutch.guilty@yahoo.com">dutch.guilty@yahoo.com</a></td>
<td>Mar 27</td>
</tr>
<tr>
<td>ROFL BANK</td>
<td>FUTON BANK - Attention Customer I am Dr. Mark McCool, I work with a reputable financial institution in United State of American Bank Address 111 Ballarat Ave,Pitman New Jersey 08072,FUTON BANK OF NEW</td>
<td><a href="mailto:roflbank@americantbank.com">roflbank@americantbank.com</a></td>
<td>Mar 26</td>
</tr>
<tr>
<td>Robin Walker</td>
<td>(no subject) - Ich bin Robin Walker, ein älterer Bürger von St. Alberts, Kanada. Ich habe einen Jackpot von 60 Million Dollar gewonnen, war der größte Gewinner der Lotterie in Alberta ist. In Namen von mir und</td>
<td><a href="mailto:robin.walker@canadianlottery.com">robin.walker@canadianlottery.com</a></td>
<td>Mar 26</td>
</tr>
<tr>
<td>QF-RA 2018</td>
<td>CFP - Qualitative Research and Integrating Academic Activities - Dear Oliver Van Der Toorn, We would like to invite you to contribute to the special three-track event on &quot;Qualitative Research and Integrating Academic Activity</td>
<td><a href="mailto:qf-ra2018@qualitative.com">qf-ra2018@qualitative.com</a></td>
<td>Mar 25</td>
</tr>
<tr>
<td>Keith B. Bolcar</td>
<td>OFFICE OF HOMELAND SECURITY - OFFICE OF HOMELAND SECURITY Immigration and Customs Enforcement US Department of Homeland Security, Street SW Suite 322,Atlanta Georgia 30303.2100 Park Drive North</td>
<td>keith.bolcar@ homelandsec.gov</td>
<td>Mar 23</td>
</tr>
<tr>
<td>Mr. Abdullah Ibrahim</td>
<td>get back to me as soon as you got my message - Attn: Sir, We were mandated by the Federal Government of Nigeria last week so affect the release of sum of N5,000,000.00 to each affected (SCAM) victim around the globe</td>
<td><a href="mailto:abdullah.ibrahim@federal.gov">abdullah.ibrahim@federal.gov</a></td>
<td>Mar 23</td>
</tr>
<tr>
<td>United Nations Office</td>
<td>Quickly contact diplomat George Porter here at Bradley International Airport Connections... - We hereby inform you that the Scotland Yard Police, Interpol, Federal Bureau of Investigation, (FBI) United States of America, the I</td>
<td><a href="mailto:unitednations@connections.com">unitednations@connections.com</a></td>
<td>Mar 23</td>
</tr>
<tr>
<td>Mr. Ivan Ronald</td>
<td>Re: Investment Proposal/For Your Consideration - Hello Good morning Do you have any project or an on going project which requires funding? I got your contact from a Business Directory in my search for a trustworthy and</td>
<td><a href="mailto:ivanronald@investment.com">ivanronald@investment.com</a></td>
<td>Mar 22</td>
</tr>
<tr>
<td>Patrick Ozougo Enq.</td>
<td>Contact Him... - Dear, I want to inform you about the success in transferring the funds. I left 30.6 Million compensation for your efforts. Do contact my secretary Mr.Benjamin Mark via his email address (samnai07)</td>
<td><a href="mailto:patrickozougoenq@compensation.com">patrickozougoenq@compensation.com</a></td>
<td>Mar 21</td>
</tr>
<tr>
<td>Mr. Adebayo Adealu</td>
<td>Kindly get back to Me... - Dear Secretory, My name is Mr.Adebayo Adealu,the deputy governor CBN. This is to bring the good news to you that I have been mandated by the President Federal Republic in conjunction with the Fe</td>
<td><a href="mailto:adebayo.adelau@cbn.gov">adebayo.adelau@cbn.gov</a></td>
<td>Mar 19</td>
</tr>
<tr>
<td>Obot Nicolas</td>
<td>funding - Are you looking for a business loan, personal loans, mortgages, car loans, student loans, debt consolidation loans, unsecured loans, risk capital, at a low interest rate and affordable interest rate of</td>
<td><a href="mailto:obotnicolas@funding.com">obotnicolas@funding.com</a></td>
<td>Mar 17</td>
</tr>
<tr>
<td>Amo Risile</td>
<td>Malien sie mir, wenn Sie das bekommen - Meine Namen sind Amo Risile, der Sieger der Nationalen Lotterie von vierundzwanzig Millionen, fünfhunderttausend zweiundsiebenhundertachtundachtzig Pfund. (€ 4, 501,823.) Am 27. Dezember</td>
<td><a href="mailto:amo.risile@malien.com">amo.risile@malien.com</a></td>
<td>Mar 17</td>
</tr>
<tr>
<td>MONEYGARU FOUNDATION</td>
<td>ATM - - CLAIM YOUR MONEYGARU PREPAID VISA CARD CREDITED WITH $850000.00 USD - Reply To Claim It (mail)</td>
<td><a href="mailto:moneygaru@foundation.com">moneygaru@foundation.com</a></td>
<td>Mar 16</td>
</tr>
<tr>
<td>Delivery</td>
<td>Contact diplomat John Malvin now at John.F.Kennedy international airport New York USA, ... - Attention, I'm Diplomat John Malvin, I have been trying to reach you on your telephone about an hour now just to inform you about</td>
<td><a href="mailto:delivery@diplomat.com">delivery@diplomat.com</a></td>
<td>Mar 14</td>
</tr>
<tr>
<td>Kamernet</td>
<td>Vind je nieuwe huurder of huiseigenaar eenvoudig bij Kamernet - Piaats gratis de advertentie en onmiddellijk aanmelden! Kamernet Piaats gratis advertentie Piaats gratis je advertentie De beschikbare kamer van won</td>
<td><a href="mailto:kamernet@eenvoudig.com">kamernet@eenvoudig.com</a></td>
<td>Mar 13</td>
</tr>
<tr>
<td>CRYPTO_Currency_Institute</td>
<td>Easy_L00PHE-87-Turn~$10~$10~$10~$000~? Renegade_Russian-Analyzer-Relays-How-To<del>Turn</del>$10 To $100</td>
<td><a href="mailto:cryptocurrency@easy.com">cryptocurrency@easy.com</a></td>
<td>Mar 8</td>
</tr>
</tbody>
</table>
Snowshoe Spam

- few hosts

Spam

Internet
Snowshoe Spam

Spam

- few hosts
- many messages per host
Snowshoe Spam

- few hosts
- many messages per host

Spam

Internet

Snowshoe Spam

- many hosts
Snowshoe Spam

- **Spam**
  - few hosts
  - many messages per host

- **Snowshoe Spam**
  - many hosts
  - few messages per host
### Original Message

<table>
<thead>
<tr>
<th>Message ID</th>
<th><a href="mailto:820093659.47491888.1520538809384.JavaMail.root@basil.ocn.ne.jp">820093659.47491888.1520538809384.JavaMail.root@basil.ocn.ne.jp</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Created at:</td>
<td>Thu. Mar 8, 2018 at 8:53 PM (Delivered after 402 seconds)</td>
</tr>
<tr>
<td>From:</td>
<td>MARX MARC <a href="mailto:ktaguchi@basil.ocn.ne.jp">ktaguchi@basil.ocn.ne.jp</a></td>
</tr>
<tr>
<td>To:</td>
<td></td>
</tr>
<tr>
<td>Subject:</td>
<td>loan offer listings</td>
</tr>
<tr>
<td>SPF:</td>
<td>PASS with IP 153.149.236.10 [Learn more]</td>
</tr>
</tbody>
</table>
### Original Message

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message ID</td>
<td><a href="mailto:820093659.47491888.1520638809384.JavaMail.root@basil.ocn.ne.jp">820093659.47491888.1520638809384.JavaMail.root@basil.ocn.ne.jp</a></td>
</tr>
<tr>
<td>Created at</td>
<td>Thu, Mar 8, 2018 at 8:53 PM (Delivered after 402 seconds)</td>
</tr>
<tr>
<td>From</td>
<td>MARX MARC <a href="mailto:ktaguchi@basil.ocn.ne.jp">ktaguchi@basil.ocn.ne.jp</a></td>
</tr>
<tr>
<td>To</td>
<td></td>
</tr>
<tr>
<td>Subject</td>
<td>loan offer listings</td>
</tr>
<tr>
<td>SPF</td>
<td>PASS with IP 153.149.236.10. [Learn more](Learn more)</td>
</tr>
</tbody>
</table>
Assumption: Background

SPF record from ‘consultant.com’

v=spf1
<table>
<thead>
<tr>
<th>SPF record from ‘consultant.com’</th>
</tr>
</thead>
<tbody>
<tr>
<td>v=spf1 ip4:213.165.64.0/23 ip4:74.208.5.64/26 ip4:74.208.122.0/26 ip4:212.227.126.128/25 ip4:212.227.15.0/24 ip4:212.227.17.0/27 ip4:74.208.4.192/26 ip4:82.165.159.0/24 ip4:217.72.207.0/27</td>
</tr>
</tbody>
</table>
Assumption: Background

SPF record from ‘consultant.com’

v=spf1 ip4:213.165.64.0/23 ip4:74.208.5.64/26 ip4:74.208.122.0/26 ip4:212.227.126.128/25
ip4:212.227.15.0/24 ip4:212.227.17.0/27 ip4:74.208.4.192/26 ip4:82.165.159.0/24
ip4:217.72.207.0/27 -all
SPF record from ‘consultant.com’

\v=spf1 \text{ip4:} 213.165.64.0/23 \text{ip4:} 74.208.5.64/26 \text{ip4:} 74.208.122.0/26 \text{ip4:} 212.227.126.128/25 \text{ip4:} 212.227.15.0/24 \text{ip4:} 212.227.17.0/27 \text{ip4:} 74.208.4.192/26 \text{ip4:} 82.165.159.0/24 \text{ip4:} 217.72.207.0/27 -all

Email from ‘paypoint_sanchez@consultant.com’

Received-SPF: fail (google.com: domain of paypoint_sanchez@consultant.com does not designate 103.10.4.139 as permitted sender) client-ip=103.10.4.139;
Assumption: Background

SPF record from 'consultant.com'

v=spf1 ip4:213.165.64.0/23 ip4:74.208.5.64/26 ip4:74.208.122.0/26 ip4:212.227.126.128/25 ip4:212.227.15.0/24 ip4:212.227.17.0/27 ip4:74.208.4.192/26 ip4:82.165.159.0/24 ip4:217.72.207.0/27 -all

Email from ‘paypoint_sanchez@consultant.com’

Received-SPF: fail (google.com: domain of paypoint_sanchez@consultant.com does not designate 103.10.4.139 as permitted sender) client-ip=103.10.4.139;

Typical usage of SPF

v=spf1 a mx ip4:167.160.22.0/24 -all
Hypothesis

While snowshoe spammers are hard to detect, but still leave a trace in the DNS.
While snowshoe spammers are hard to detect, but still leave a trace in the DNS.

Snowshoe spam + SPF
While snowshoe spammers are hard to detect, but still leave a trace in the DNS.

Snowshoe spam + SPF
Many hosts + a DNS record for each host or a long SPF record
While snowshoe spammers are hard to detect, but still leave a trace in the DNS.

Snowshoe spam + SPF

Many hosts + a DNS record for each host or a long SPF record

Domain with many records or long SPF records
While snowshoe spammers are hard to detect, but still leave a trace in the DNS.

**Snowshoe spam + SPF**

Many hosts + a DNS record for each host or a long SPF record

Domain with many records or long SPF records

**Active DNS measurements** are a good way to detect snowshoe spam domains.
Methodology
Overview

OpenINTEL
(DNS data source)
Overview

OpenINTEL (DNS data source) → Machine Learning (processing)
Overview

OpenINTEL (DNS data source) → Machine Learning (processing) → Realtime Blackhole List (storage)
Overview

OpenINTEL
(DNS data source)

Machine Learning
(processing)

Realtime Blackhole List
(storage)

SURFnet
(validation)
OpenINTEL: Background

- Active DNS measurement platform
OpenINTEL: Background

- Active DNS measurement platform
- Queries more than 60% of registered domain names (in total more than 206 million)
OpenINTEL: Background

- Active DNS measurement platform
- Queries more than 60% of registered domain names (in total more than 206 million)
  - A
  - AAAA
  - MX
  - NS
  - ...

Every 24 hours a measurement is started
OpenINTEL: Background

• Active DNS measurement platform
• Queries more than 60% of registered domain names (in total more than 206 million)
  • A
  • AAAA
  • MX
  • NS
  • ...
• Every 24 hours a measurement is started
37 features
37 features

- Simple: number of MX addresses
37 features

- Simple: number of MX addresses
- Complex: number of IP addresses inside an SPF record
37 features

- Simple: number of MX addresses
- Complex: number of IP addresses inside an SPF record

These features are not computed for every domain in OpenINTEL.
OpenINTEL: Long Tail Analysis
OpenINTEL (DNS data source) → Machine Learning (processing) → Realtime Blackhole List (storage) → SURFnet (validation)
We have trained and evaluated 12 Machine Learning algorithms.

- Training dataset from domains on the long tail which appear in known blacklists.
We have trained and evaluated 12 Machine Learning algorithms.

- Training dataset from domains on the long tail which appear in known blacklists.

The performance of each classifier is compared based on the precision metric.

\[
\text{Precision} = \frac{\text{True Positives}}{\text{True Positives} + \text{False Positives}}
\]
We have trained and evaluated 12 Machine Learning algorithms.

- Training dataset from domains on the long tail which appear in known blacklists.

The performance of each classifier is compared based on the precision metric.

\[
\text{Precision} = \frac{\text{True Positives}}{\text{True Positives} + \text{False Positives}}
\]

Selected the ‘AdaBoost’ classifier as our classifier of choice, since it had the highest precision (98% with a FPR of 1%).
Realtime Blackhole List (RBL)

OpenINTEL (DNS data source) → Machine Learning (processing) → Realtime Blackhole List (storage) → SURFnet (validation)
SURFnet

OpenINTEL (DNS data source)

Machine Learning (processing)

Realtime Blackhole List (storage)

SURFnet (validation)
Active DNS measurements of more than 60% of registered domain names forms the source of our data. We filter out large domains via the Long Tail Analysis.
Active DNS measurements of more than 60% of registered domain names forms the source of our data. We filter out large domains via the Long Tail Analysis.

We have selected the AdaBoost classifier as our classifier of choice, since it had the highest precision metric.
Active DNS measurements of more than 60% of registered domain names forms the source of our data. We filter out large domains via the Long Tail Analysis.

We have selected the AdaBoost classifier as our classifier of choice, since it had the highest precision metric.

The results of our daily detections are stored in an RBL.
Active DNS measurements of more than 60% of registered domain names forms the source of our data. We filter out large domains via the Long Tail Analysis.

We have selected the AdaBoost classifier as our classifier of choice, since it had the highest precision metric.

The results of our daily detections are stored in an RBL.

We have evaluated the RBL in SURFmailfilter.
Results
Distinction between two types

Number of A records

Number of MX records

CDF

spam

ham

16.6

11.2

77.0
<table>
<thead>
<tr>
<th>Domain</th>
<th>A records</th>
<th>MX records</th>
</tr>
</thead>
<tbody>
<tr>
<td>(ham) google.com</td>
<td>1</td>
<td>5</td>
</tr>
</tbody>
</table>
## Example

<table>
<thead>
<tr>
<th>Domain</th>
<th>A records</th>
<th>MX records</th>
</tr>
</thead>
<tbody>
<tr>
<td>(ham) google.com</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>(spam) giftiedan.com</td>
<td>61</td>
<td>1</td>
</tr>
</tbody>
</table>
## Example

<table>
<thead>
<tr>
<th>Domain</th>
<th>A records</th>
<th>MX records</th>
</tr>
</thead>
<tbody>
<tr>
<td>(ham) google.com</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>(spam) giftiedan.com</td>
<td>61</td>
<td>1</td>
</tr>
<tr>
<td>(spam) twirlmore.com</td>
<td>1</td>
<td>253</td>
</tr>
</tbody>
</table>
RBL comparison (2 month period)
RBL comparison (2 month period)

Number of detected domains

Detection in advance (days)

30705
$\Delta t < 2$ days
RBL comparison (2 month period)

- 30705 domains detected in advance with Δt < 2 days
- 1972 domains detected in advance with Δt ≥ 2 days

Histogram showing the number of detected domains over detection in advance (days) from 0 to 80 days.
RBL comparison (2 month period)

![Graph showing number of detected domains vs. detection in advance (days)]

- Δt < 2 days: 30705 domains
- Δt ≥ 2 days: 1972 domains

Number of detected domains
Detection in advance (days)

- 0
- 10
- 100
- 1000
- 10000
- 100000

Δt < 2 days

Δt ≥ 2 days
RBL comparison (2 month period)

Number of detected domains

Detection in advance (days)

30705
Δt < 2 days

1972
Δt ≥ 2 days

1154
971
1105
RBL comparison (2 month period)

- Δt < 2 days: 30705 domains detected
- Δt ≥ 2 days: 1972 domains detected

Number of detected domains vs. Detection in advance (days)

- 949 domains detected at 60 days
- 971 domains detected at 70 days
- 1105 domains detected at 80 days
- 1154 domains detected at 90 days
- 30705 domains detected at 0 days
- 1972 domains detected at 100 days

Δt < 2 days
Δt ≥ 2 days
RBL comparison (9 month period)

![Detection in advance (days)](image)

- Number of detected domains:
  - $\Delta t < 2$ days: 57,724
  - $\Delta t \geq 2$ days: 6,710

- Detection in advance:
  - $\Delta t < 2$ days: 205 days
  - $\Delta t \geq 2$ days: 1,305 days
## SURFnet evaluation

<table>
<thead>
<tr>
<th>Domain names</th>
<th>Observation dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>daadzgam.com</td>
<td>2017-05-24</td>
</tr>
<tr>
<td>realdrippy.com</td>
<td>2017-06-23</td>
</tr>
<tr>
<td>coachspoke.com</td>
<td>2017-07-23</td>
</tr>
<tr>
<td>stillscratch.com</td>
<td></td>
</tr>
<tr>
<td>homerope.com</td>
<td></td>
</tr>
<tr>
<td>quittradition.com</td>
<td></td>
</tr>
</tbody>
</table>

*Observation dates*
SURFnet evaluation

Domain names
- daadzgam.com
- realdripply.com
- coachspoke.com
- stillscratch.com
- homerope.com
- quittradition.com

Observation dates
- 2017-05-24
- 2017-06-23
- 2017-07-23
SURFnet evaluation

- Δt < 2 days

- 45% of received emails fall in this category
- 18% of observed domains fall in this category
SURFnet evaluation

- 17% of received emails fall in this category
- 26% of observed domains fall in this category

![Graph showing domain names and observation dates with blacklisted and detected flags with Δt ≥ 2 days indication]
SURFnet evaluation

• 38% of received emails fall in this category
• 57% of observed domains fall in this category
SURFnet evaluation

- 41% of emails were received in the purple areas
  - 59% of these emails have not been marked as spam
SURFnet evaluation

Additional score of the RBL

Emails marked as spam

0% 3% 19% 50% 53%
SURFnet evaluation

Additional score of the RBL

Emails marked as spam

0% 3% 19% 50% 53% 55% 70% 79% 88% 99% 100%

0.0 0.5 1.0 1.5 2.0 2.5 3.0 3.5 4.0 4.5 5.0

Additional score of the RBL
Conclusion
Conclusion

Using active DNS and by applying machine learning we are able to detect snowshoe spam domains.
Using active DNS and by applying machine learning we are able to detect snowshoe spam domains.

We are able to detect domains from 2 to 180 days in advance when compared to other blacklists.
Conclusion

Using **active DNS** and by applying **machine learning** we are able to detect snowshoe spam domains.

We are able to detect domains from **2 to 180 days in advance** when compared to other blacklists.

This time advantage translates into additional email being marked as spam.

**Emails which would otherwise bypass the email filter.**
Conclusion

Using active DNS and by applying machine learning we are able to detect snowshoe spam domains.

We are able to detect domains from 2 to 180 days in advance when compared to other blacklists.

This time advantage translates into additional email being marked as spam.

Emails which would otherwise bypass the email filter.

After the evaluation period, SURFnet has deployed our RBL in production.
Thank you for listening¹.

Are there any questions?

¹Images are from Pixabay and Wikimedia