Thwarting Emotet email conversation thread hijacking with clustering

Olivier Coutu & Pierre-Luc Vaudry

Olivier Coutu
Operations Manager

Pierre-Luc Vaudry
R&D Director

PART 1

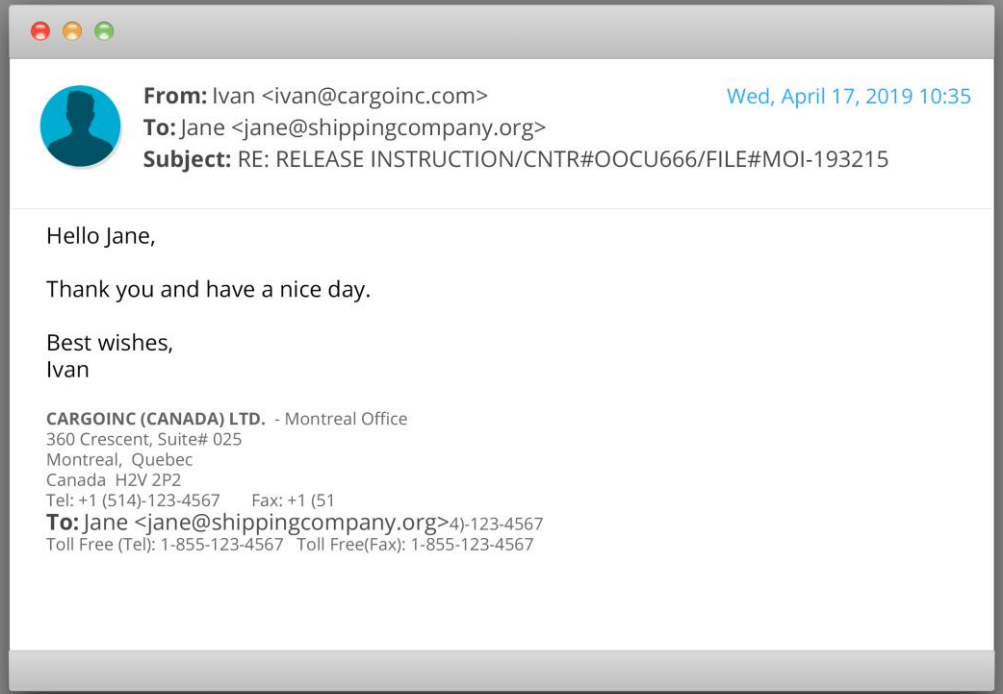
A War Story: Email conversation thread hijacking

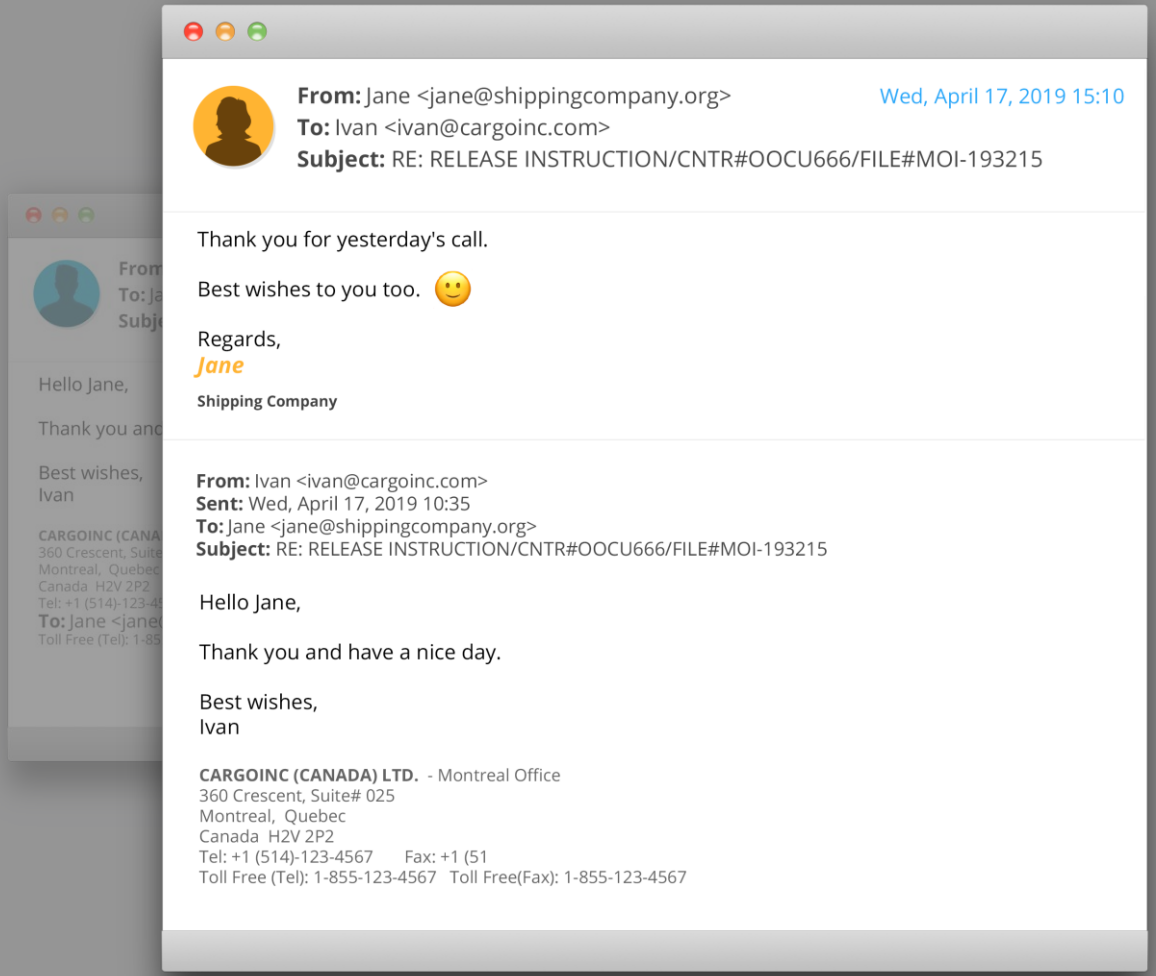
Ivan

Cargo Inc.

Jane

Shipping Company


From: Ivan <ivan@cargoinc.com>
Wed, April 17, 2019 10:35
To: Jane <jane@shippingcompany.org>
Subject: RE: RELEASE INSTRUCTION/CNTR#OOCU666/FILE#MOI-193215
Hello Jane,
Thank you and have a nice day.
Best wishes,
Ivan
CARGOINC (CANADA) LTD. - Montreal Office
360 Crescent, Suite# 025
Montreal, Quebec
Canada H2V 2P2
Tel: +1 (514)-123-4567 Fax: +1 (51
To: Jane <jane@shippingcompany.org>4)-123-4567
Toll Free (Tel): 1-855-123-4567 Toll Free(Fax): 1-855-123-4567



From: Jane <jane@shippingcompany.org>
To: Ivan <ivan@cargoinc.com>
Subject: RE: RELEASE INSTRUCTION/CNTR#OOCU666/FILE#MOI-193215
Wed, April 17, 2019 15:10

Thank you for yesterday's call.

Best wishes to you too.

Regards,
Jane
Shipping Company

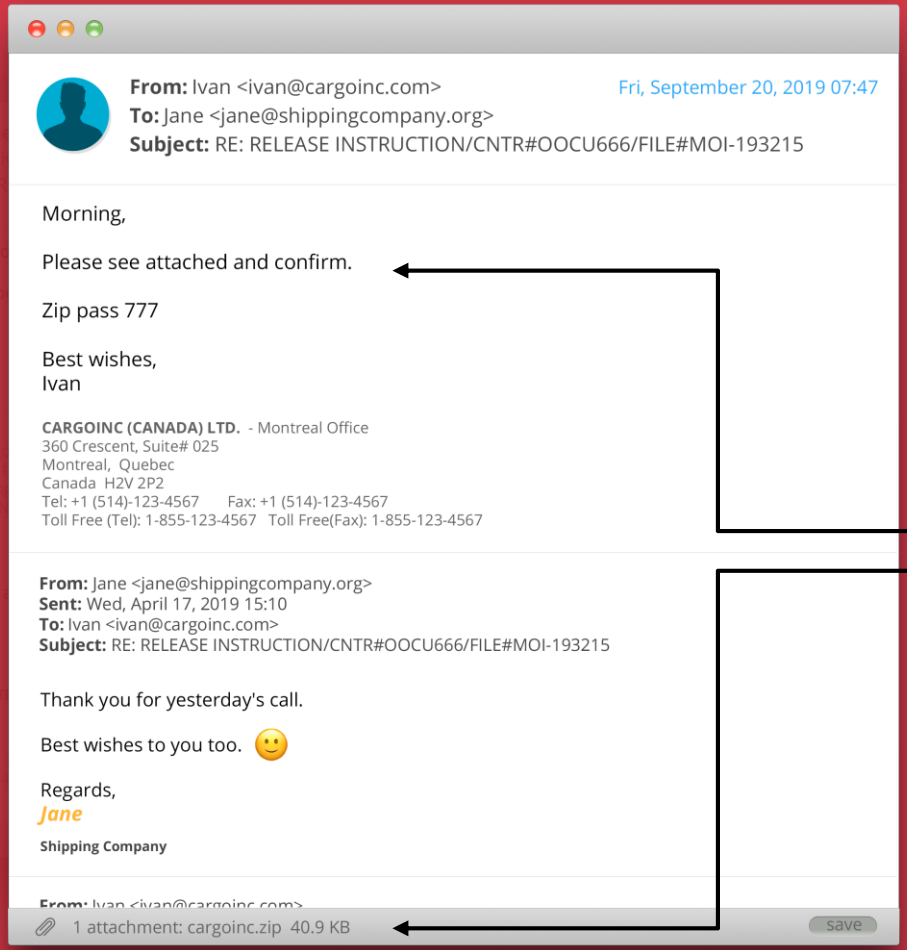
From: Ivan <ivan@cargoinc.com>
Sent: Wed, April 17, 2019 10:35
To: Jane <jane@shippingcompany.org>
Subject: RE: RELEASE INSTRUCTION/CNTR#OOCU666/FILE#MOI-193215

Hello Jane,

Thank you and have a nice day.

Best wishes,
Ivan

CARGOINC (CANADA) LTD. - Montreal Office
360 Crescent, Suite# 025
Montreal, Quebec
Canada H2V 2P2
Tel: +1 (514)-123-4567 Fax: +1 (51
Toll Free (Tel): 1-855-123-4567 Toll Free(Fax): 1-855-123-4567


From: Ivan <ivan@cargoinc.com>
Fri, September 20, 2019 07:47
To: Jane <jane@shippingcompany.org>
Subject: RE: RELEASE INSTRUCTION/CNTR#OOCU666/FILE#MOI-193215
Morning,
Please see attached and confirm.
Zip pass 777
Best wishes,
Ivan
CARGOINC (CANADA) LTD. - Montreal Office
360 Crescent, Suite# 025
Montreal, Quebec
Canada H2V 2P2
Tel: +1 (514)-123-4567 Fax: +1 (514)-123-4567
Toll Free (Tel): 1-855-123-4567 Toll Free(Fax): 1-855-123-4567
From: Jane <jane@shippingcompany.org>
Sent: Wed, April 17, 2019 15:10
To: Ivan <ivan@cargoinc.com>
Subject: RE: RELEASE INSTRUCTION/CNTR#OOCU666/FILE#MOI-193215
Thank you for yesterday's call.
Best wishes to you too.
Regards,
Jane
Shipping Company
1 attachment: cargoinc.zip 40.9 KB
save

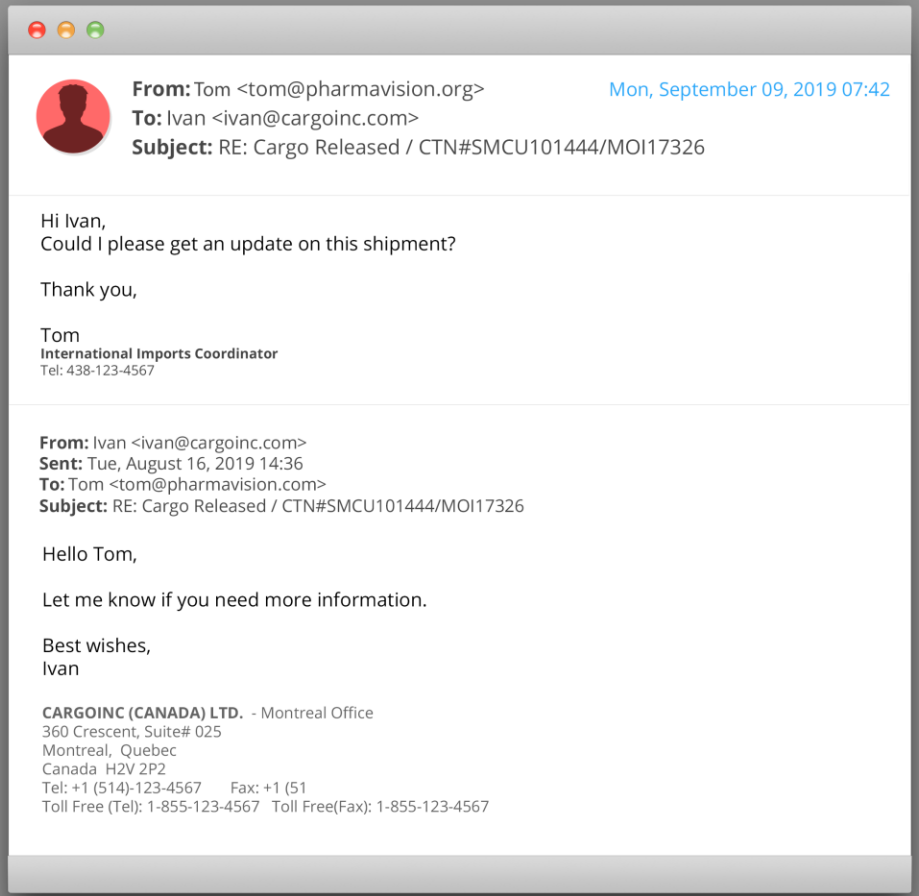
SUSPICIOUS

Ivan

Cargo Inc.

Tom

Pharma Vision



From: Tom <tom@pharmavision.org> Mon, September 09, 2019 07:42
To: Ivan <ivan@cargoinc.com>
Subject: RE: Cargo Released / CTN#SMCU101444/MOI17326

Hi Ivan,
Could I please get an update on this shipment?

Thank you,

Tom
International Imports Coordinator
Tel: 438-123-4567

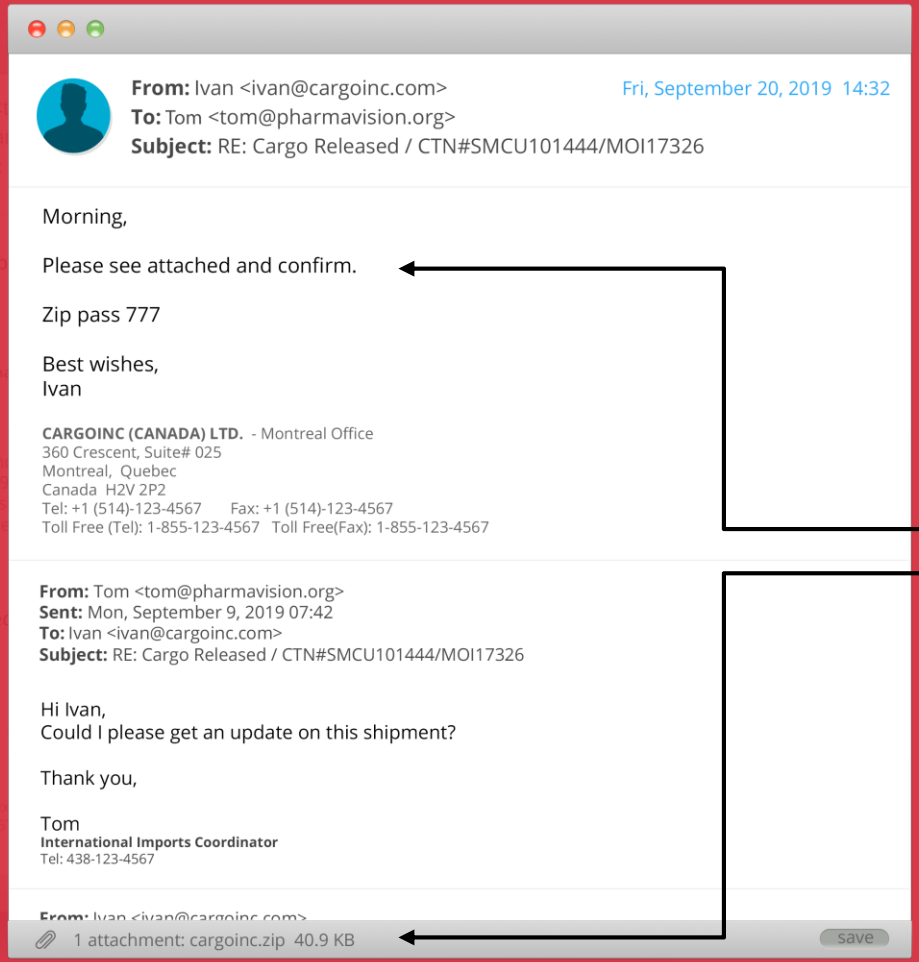
From: Ivan <ivan@cargoinc.com>
Sent: Tue, August 16, 2019 14:36
To: Tom <tom@pharmavision.com>
Subject: RE: Cargo Released / CTN#SMCU101444/MOI17326

Hello Tom,

Let me know if you need more information.

Best wishes,
Ivan

CARGOINC (CANADA) LTD. - Montreal Office
360 Crescent, Suite# 025
Montreal, Quebec
Canada H2V 2P2
Tel: +1 (514)-123-4567 Fax: +1 (51
Toll Free (Tel): 1-855-123-4567 Toll Free(Fax): 1-855-123-4567

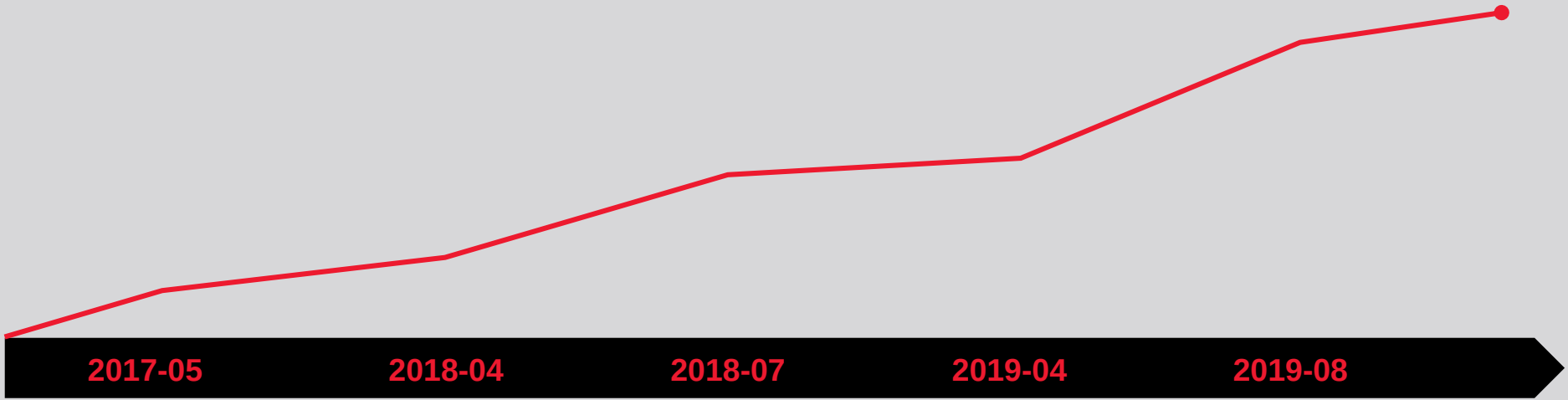

From: Ivan <ivan@cargoinc.com>
Fri, September 20, 2019 14:32
To: Tom <tom@pharmavision.org>
Subject: RE: Cargo Released / CTN#SMCU101444/MOI17326
Morning,
Please see attached and confirm.
Zip pass 777
Best wishes,
Ivan
CARGOINC (CANADA) LTD. - Montreal Office
360 Crescent, Suite# 025
Montreal, Quebec
Canada H2V 2P2
Tel: +1 (514)-123-4567 Fax: +1 (514)-123-4567
Toll Free (Tel): 1-855-123-4567 Toll Free(Fax): 1-855-123-4567
From: Tom <tom@pharmavision.org>
Sent: Mon, September 9, 2019 07:42
To: Ivan <ivan@cargoinc.com>
Subject: RE: Cargo Released / CTN#SMCU101444/MOI17326
Hi Ivan,
Could I please get an update on this shipment?
Thank you,
Tom
International Imports Coordinator
Tel: 438-123-4567
1 attachment: cargoinc.zip 40.9 KB
save

SUSPICIOUS

Email conversation thread hijacking: how it works

- Compromised user, emails siphoned out
- Content of emails replayed
- Attachment name

Email thread hijacking: A History



2017-05

North Korean hackers

2018-04

First time MO is observed by ZEROSPAM

2018-07

Emotet makes the news

2019-04

Emotet is reported to be using this MO

2019-08

We detect our first sizeable wave using clustering

Erratum regarding Emotet on 2019-08-02

The email conversation thread hijacking campaign samples we had from the beginning of August turned out, after verification, not to be carrying Emotet. Over time, we observed various other malware to be using email conversation thread hijacking, such as Ursnif, QBot, and PredatorTheThief.

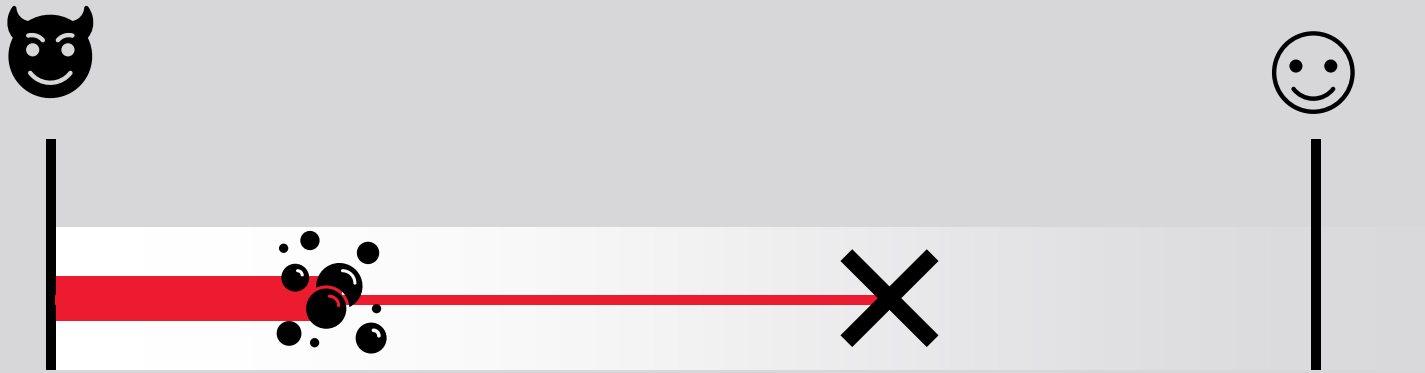
Suspicious cluster alert!

	Blocked	Subnetworks	org.	Subject	Sender
⌄	32/45	1	34	Re: New Car Catalog	ivan@infecteddealer.org (Ivan)

Subject	Sender
Re: New Car Catalog	ivan@infecteddealer.org (Ivan)
Re: RE: BTZ-3 Rear view mirrors	stacy@infecteddealer.org (Stacy)
Re: Fw: Updated price list	ivan@infecteddealer.org (Ivan)
Re: Re: RE: Fuel consumption sheet update	ivan@infecteddealer.org (Ivan)
Re: Problème de miroir sur modèle cv17	stacy@infecteddealer.org (Stacy)

Time To Block

Reducing the Time To Block



NEW CAMPAIGN LAUNCH

CLUSTERING

REACTION BY ADJUSTING FILTERING IN LESS THAN **20 MINUTES**

CLIENT UNAWARE & SECURE

Defending against email thread hijacking

Don’t whitelist your contacts

Quarantine suspicious files

Enable DMARC verification

PART 2

Under the hood: Clustering-based campaign detection

ZERO SPAM

Why clustering for email filtering?

Clustering is the task of **grouping** objects that are **similar (in some sense)** together into groups (called *clusters*).

An ***email campaign*** is a **coordinated set** of individual email messages that are deployed across a **specific period of time** with **one specific purpose**.

A ***spam campaign*** is a particular case of an email campaign where the means and/or purpose are **not legitimate**.

Our email clustering implementation

	Blocked	Subnetworks	org.	Subject	Sender
>	32/45	1	34	Re: New Catalog	ivan@infecteddealer.org (Ivan)
>	0/19	1	17	Deal of the Week! APC Back-UPS only $59.99 + Free Shipping!	noreply@p.tigerdirect.com (TigerDirectB2B)
>	352/352	279	119	Power up your manlyness and you ll become her #1.	RogerBrooksmii@epm.net.co (Camila)
>	271/271	77	17	Ich habe die verdammte Nachricht verpasst	AntjeAdelhardtfatya@access kenya.com
>	21/21	1	16	Implement Project Management Culture	delivery@email.grceducators.com (Ashley Moras)

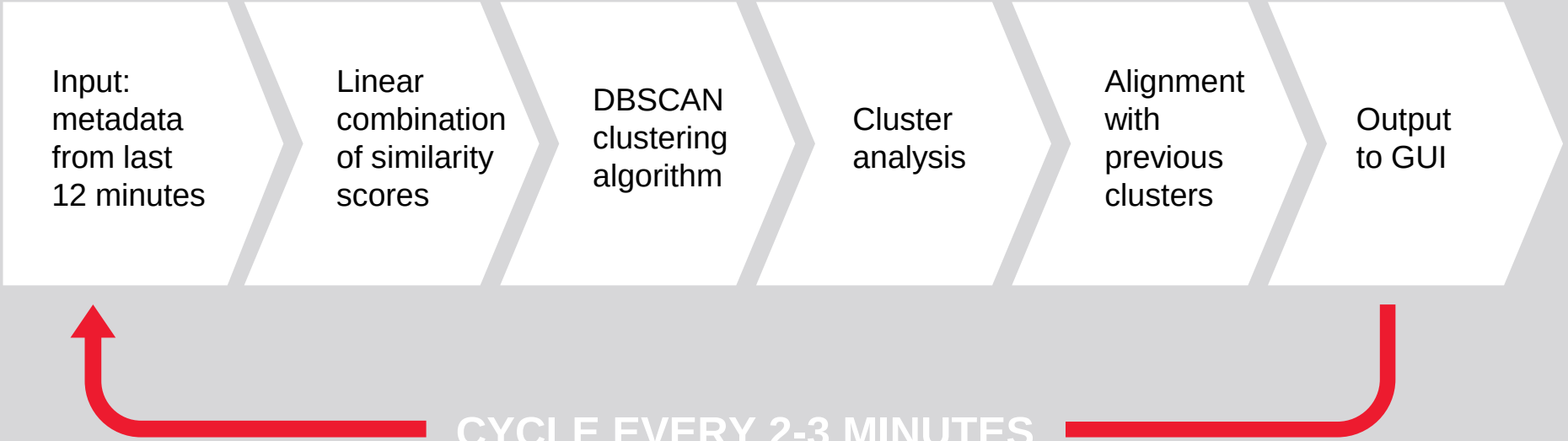
Spam cluster: filtering view

Subject	Sender	Blocked ?	Extensions	Host
"Unstoppable love force" will be all about you.	GeorgeBryantyzewe@livingarts.it (Lula)	Yes	None	80.191.237.169
Stunning success among women guaranteed!	KyleRogerstikj@lovetoeat.it (Zoe)	Yes	None	95.71.124.31
Using this doping will give your couple the night of your dreams.	DonaldClarklayo@litmat.it (Laurel)	Yes	None	103.60.214.18
Demonstrate her your love evidence tonight!	JackGarciatyqxm@luxuryevents.it (Jami)	Yes	None	14.102.69.226
100% Safe To Take, With NO Side.	MarkScottvuxip@lostrillonenews.it (Mayra)	Yes	None	92.50.38.98
A man must get a stiffy!	FrankJacksonsy@provedorsmart.com.br (Rigoberto)	Yes	None	168.90.65.30
To be like iron, your loving device needs this total hardening!	AndrewJacksonsezli@sinalbr.com.br (Veronica)	Yes	None	186.225.135.54
Thinking desire left you forever?	LarryWilsonvofvi@lusettitours.it (Greta)	Yes	None	87.229.143.10
Incredible solution for all-night stud action!	MikeGreenuqiba@ttnet.com.tr (Princess)	Yes	None	78.188.222.90
Demonstrate her your love evidence tonight!	BruceClarkfetx@logoplus.it (Elliana)	Yes	None	196.15.168.146

Spam cluster: clustering view

Subject	Size	Message ID	Sender	Extensions	Attachments
"Unstoppable love force" will be all about you.	18410	<33F491BE.1CF8EFE7@livingarts.it>	Lula	(None)	(None)
Stunning success among women guaranteed!	18836	<F2F2E9B1.7FDC8FF2@lovetoeat.it>	Zoe	(None)	(None)
Using this doping will give your couple the night of your dreams.	17713	<3BDD20B8.F040AC36@litmat.it>	Laurel	(None)	(None)
Demonstrate her your love evidence tonight!	18343	<1B186A66.70E0ADFC@luxuryevents.it>	Jami	(None)	(None)
100% Safe To Take, With NO Side.	18106	<4EB8EDFA.5380186A@lostrillonenews.it>	Mayra	(None)	(None)
A man must get a stiffy!	18931	<1D6E06F5.93344F8A@provedorsmart.com.br>	Rigoberto	(None)	(None)
To be like iron, your loving device needs this total hardening!	18670	<10DF37E3.21CC2315@sinalbr.com.br>	Veronica	(None)	(None)
Thinking desire left you forever?	18057	<20B88DA2.C5E8CFE7@lusettitours.it>	Greta	(None)	(None)
Incredible solution for all-night stud action!	18805	<77A1B80B.0F317866@ttnet.com.tr>	Princess	(None)	(None)
Demonstrate her your love evidence tonight!	18052	<7EDA9771.2279F2B2@logoplus.it>	Elliana	(None)	(None)

Inside the clustering pipeline

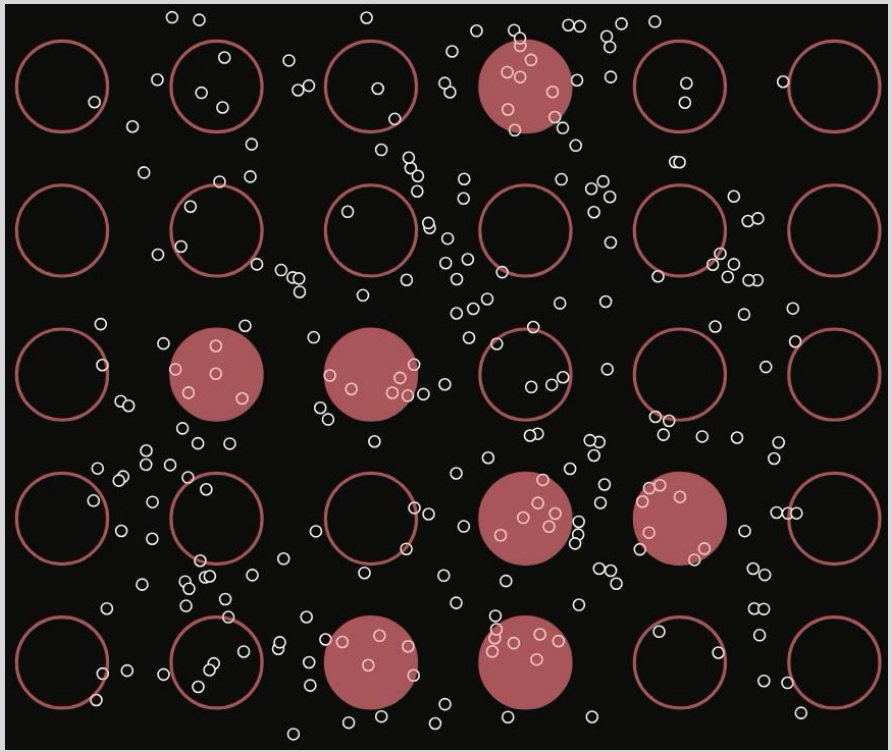


Why DBSCAN over other algorithms?

- Input: precomputed distance matrix

$$pseudo\text{-}distance = \frac{1}{similarity + \epsilon}$$

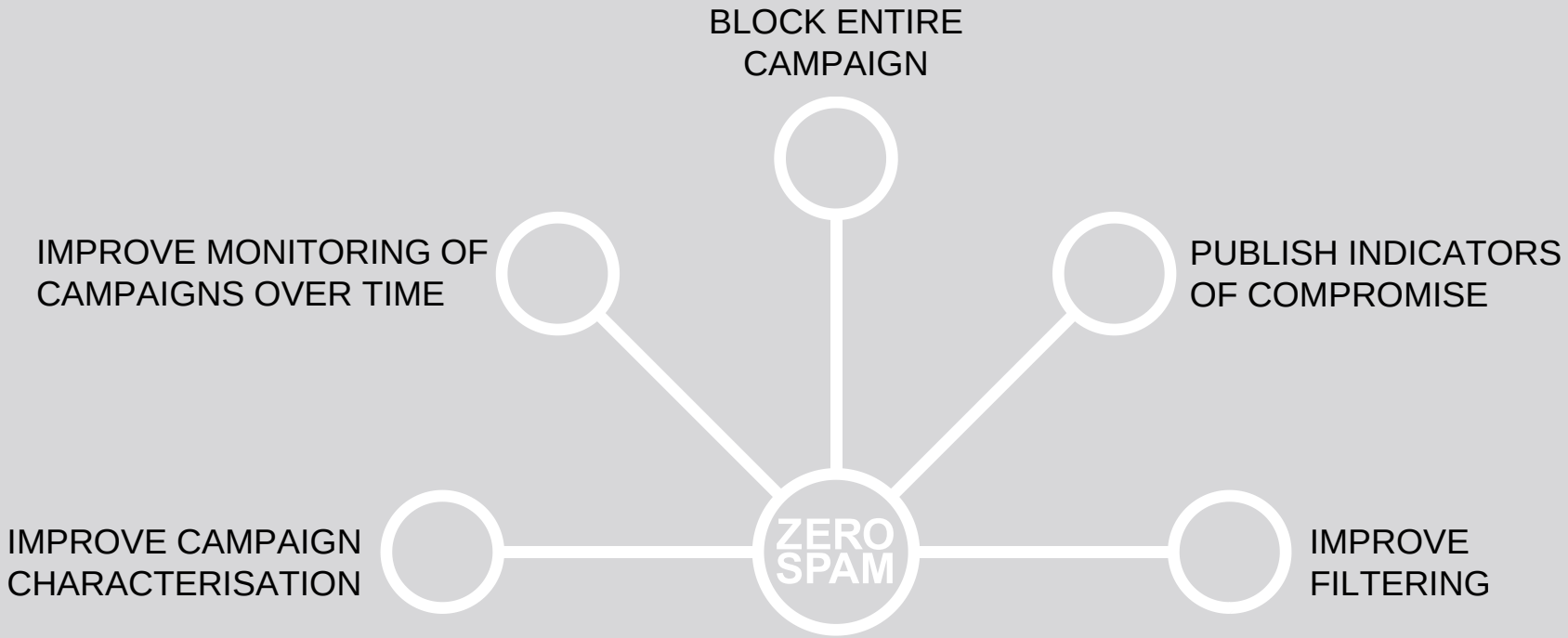
- Outliers: emails not part of a campaign
- Chains of similarity inside a cluster



DBSCAN visualisation © Naftali Harris, 2012-2019

How to evaluate and optimize

What's coming?



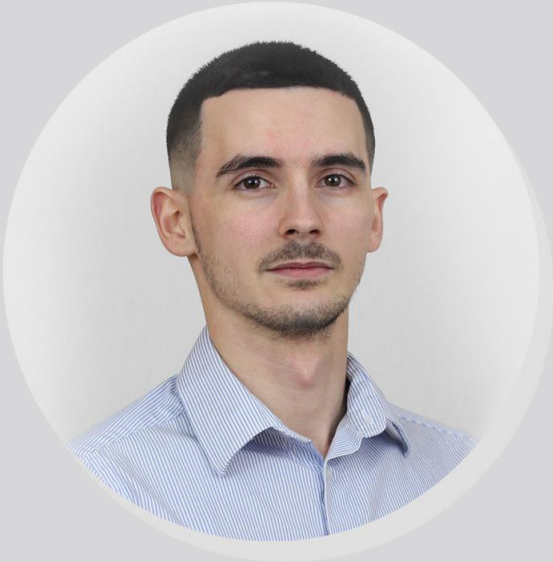
Clustering: a generic option in your toolset

Detect diverse emerging threats

Applicable to many data streams

Quickly implemented

Acknowledgements



ZERO SPAM

Vlad Stamate
Security Analyst

SOPHOS labs

Luca Nagy
Threat Researcher

References

DBSCAN

- https://www.naftaliharris.com/blog/visualizing-dbscan-clustering/
- Scikit-learn Python machine learning library

Clustering emails

- Qian et al. (2010). A Case for Unsupervised-learning-based Spam Filtering
- Chen et al. (2014). Clustering Spam Campaigns with Fuzzy Hashing
- Sarantopoulos, C. (2015). Identification and on-line incremental clustering of spam campaigns
- Patidar et al. (2016). Activity Detection from Email Meta-Data Clustering
- Smirnov (2018). Clustering and classification methods for spam analysis

Emotet timeline

- https://unit42.paloaltonetworks.com/unit42-freemilk-highly-targeted-spear-phishing-campaign/
- https://www.zdnet.com/article/emotet-hijacks-email-conversation-threads-to-insert-links-to-malware/

Questions?

www.zerospam.ca