

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

Exchange Forensics : El caso del correo fantasma

BASADO EN HECHOS REALES_



Antonio Sanz
S2 Grupo
asanz@s2grupo.es
@antoniosanzalc



1. Identificación
2. Contención
3. Erradicación
4. Recuperación
5. Lecciones aprendidas

106

1. Identificación

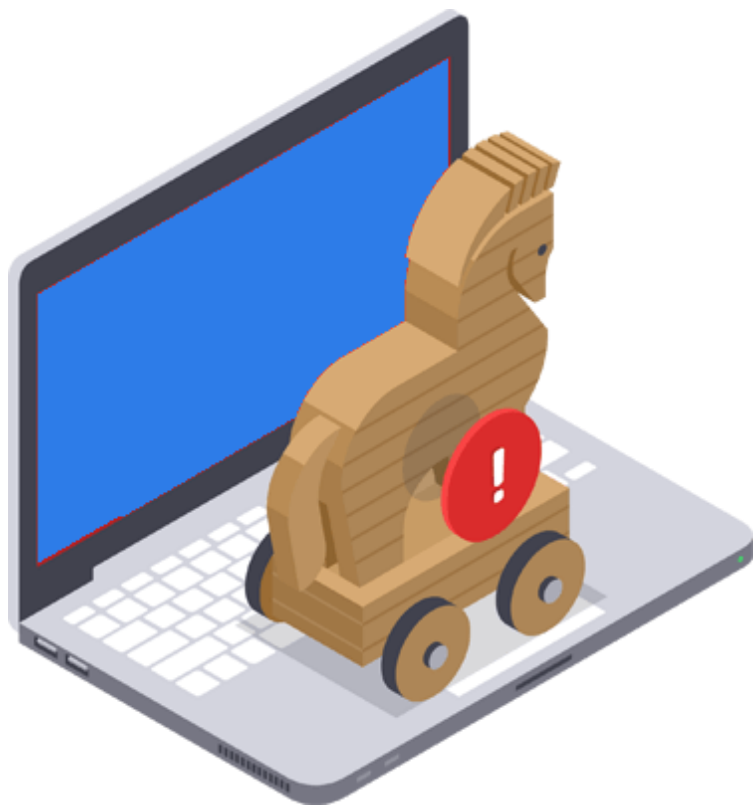


- Alerta de regla **YARA**
- Regla **especial** → Grupo de interés
- Activación del **Grupo de Respuesta**



- Correo con adjunto **malicioso**
- Info. de un **evento** próximo
- Enviado a un **directivo**

2. Contención



- **Confirmamos** grupo de interés
- Extraemos **IOC** (C2 + Patrones)
- **Compartimos** IOC



- No hay correo en **logs** de pasarela
- Señuelo contiene info. **interna**
- Conclusión: ! **Correo interno** !

→ → 1. Identificación

Message Tracking Results

Selected row will populate parameters for next message tracking search.

	Timestamp	EventId	Source	SourceConte	MessageId	MessageSubj	Sender
►	2008/10/02	RECEIVE	STOREDRIV		<5CD27AF76	Hierarchy	PublicFolc
	2008/10/03 1	RECEIVE	STOREDRIV		<5CD27AF76	Status	PublicFolc
	2008/10/17 1	RECEIVE	STOREDRIV		<5CD27AF76	Hierarchy	PublicFolc
	2008/10/20 1	RECEIVE	STOREDRIV		<5CD27AF76	Hierarchy	PublicFolc
	2008/10/21 1	RECEIVE	STOREDRIV		<5CD27AF76	Status	PublicFolc
	2008/10/24 1	RECEIVE	SMTP	08CB011EC3	<C1E4969F2	Hierarchy	E2K3-IS@
	2008/10/25 1	RECEIVE	SMTP	08CB011EC3	<C1E4969F2	Status	E2K3-IS@
	2008/10/28 1	RECEIVE	STOREDRIV		<5CD27AF76	Hierarchy	PublicFolc
	2008/10/29 1	RECEIVE	STOREDRIV		<5CD27AF76	Status	PublicFolc
	2008/10/31 1	RECEIVE	SMTP	08CB0765B2	<C1E4969F2	Hierarchy	E2K3-IS@



- Capturamos **RAM** y **disco** del equipo
- Nuestro correo malicioso **NO ESTÁ**
- Usuario no tiene privilegios de **Extranet (!OWA)**

Exchange: **EventHistoryDB**



- Recoge **eventos** del correo
- Extremadamente **minucioso**
- Accesible con **Powershell**
- Por defecto: **7 días**

```
Add-PSSnapin Microsoft.Exchange.Management.PowerShell.Support
$db = (get-mailbox <user alias>).database
$mb=(get-mailbox <user alias>).exchangeuid
Get-DatabaseEvent $db -MailboxGuid $mb -resultsizes unlimited | ? {$_.documentid -ne 0 -and
$_.CreateTime -ge "<mm/dd/yyyy>"} | fl > c:\temp\EventHistory.txt
```

```
Counter           : 15328155
CreateTime        : 1/28/2013 9:46:16 PM
ItemType          : MAPI_MESSAGE
EventName         : ObjectMoved
Flags             : None
MailboxGuid       : d05f83c1-255c-42ae-b74f-1ac3329b306a
ObjectClass       : IPM.Note
ItemEntryId       :
000000008CFDF3C2BA873648866A1C17D0E3F1AB0700BC9C9BA42124CD4F896E8915C86B2BD0000006027C20000BC9C9
2124CD4F896E8915C86B2BD0000041B6E6570000
ParentEntryId     :
000000008CFDF3C2BA873648866A1C17D0E3F1AB0100BC9C9BA42124CD4F896E8915C86B2BD0000006027C20000
OldItemEntryId    :
000000008CFDF3C2BA873648866A1C17D0E3F1AB0700BC9C9BA42124CD4F896E8915C86B2BD0000006027BF0000BC9C9
2124CD4F896E8915C86B2BD0000041B6D6260000
OldParentEntryId  :
000000008CFDF3C2BA873648866A1C17D0E3F1AB0100BC9C9BA42124CD4F896E8915C86B2BD0000006027BF0000
ItemCount         : 0
```

Exchange: **EventHistoryDB**



- MessageTracking nos da el **ItemID**
- No está en EventHistoryDB
- ¿Correo **borrado** del Exchange?
- Posible **Exchange COMPROMETIDO**

Exchange: Audit log

```
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>Set-Mailbox kala -AuditEnabled $True
[PS] C:\Windows\system32>Set-Mailbox Mark -AuditEnabled $True
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>Get-Mailbox !fl name,AuditEnabled

Name           : Administrator
AuditEnabled    : False

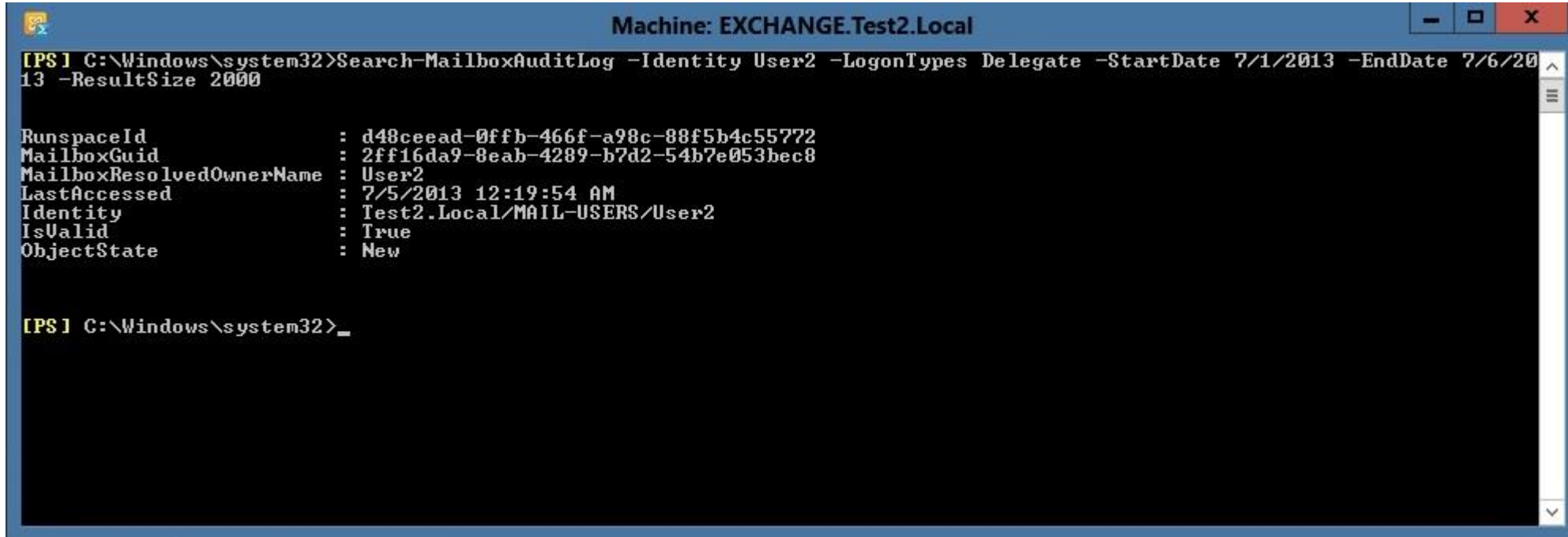
Name           : DiscoverySearchMailbox <D919BA05-46A6-415f-80AD-7E09334BB852>
AuditEnabled    : False

Name           : Jin
AuditEnabled    : False

Name           : Mark
AuditEnabled    : True
```

- Auditoria de Exchange
- Alta tasa de eventos → **Off** por defecto
- **Desactivada** para nuestro usuario

Exchange: Delegaciones



```
Machine: EXCHANGE.Test2.Local

[PS] C:\Windows\system32>Search-MailboxAuditLog -Identity User2 -LogonTypes Delegate -StartDate 7/1/2013 -EndDate 7/6/2013 -ResultSize 2000

RunspaceId           : d48ceead-0ffb-466f-a98c-88f5b4c55772
MailboxGuid           : 2ff16da9-8eab-4289-b7d2-54b7e053bec8
MailboxResolvedOwnerName : User2
LastAccessed          : 7/5/2013 12:19:54 AM
Identity              : Test2.Local/MAIL-USERS/User2
IsValid                : True
ObjectState            : New

[PS] C:\Windows\system32>
```

- User1 puede **acceder** al buzón de User2
- Necesita **auditoria** de Exchange
- **No existen** en nuestro caso

Exchange: Exportar buzón

```
[PS] C:\windows\system32>New-MailboxExportRequest -Mailbox two -FilePath \\EXCH2016\Root\two.pst
```

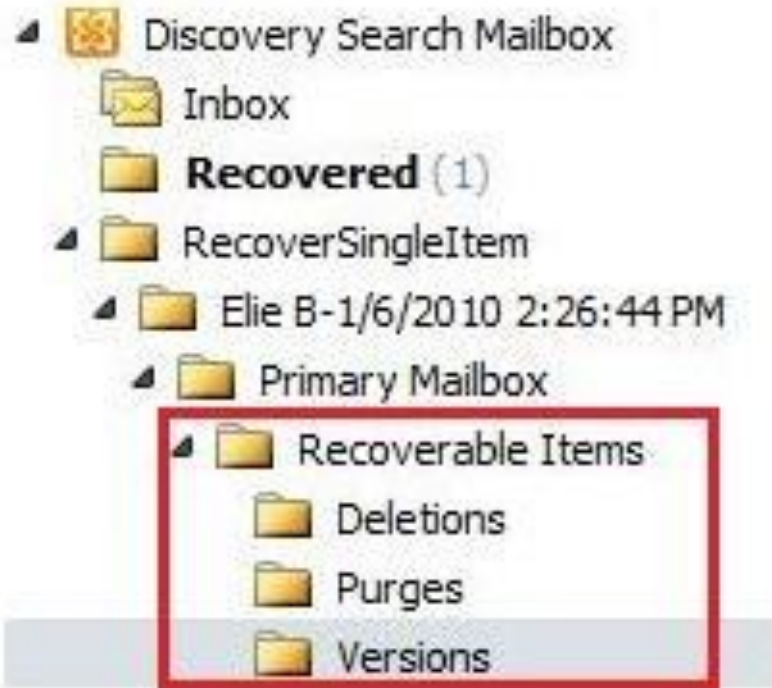
Name	Mailbox	Status
MailboxExport5	../Users/two	Queued

```
[PS] C:\windows\system32>Get-MailboxExportRequest | FT Identity,Mailbox,Status -AutoSize
```

Identity	Mailbox	Status
/Users/two\MailboxExport2	/Users/two	Completed
/Users/two\MailboxExport5	/Users/two	Completed
/Users/two\MailboxExport4	/Users/two	Completed
/Users/two\MailboxExport	/Users/two	Completed
/Users/two\MailboxExport3	/Users/two	Completed
/Users/two\MailboxExport1	/Users/two	Completed

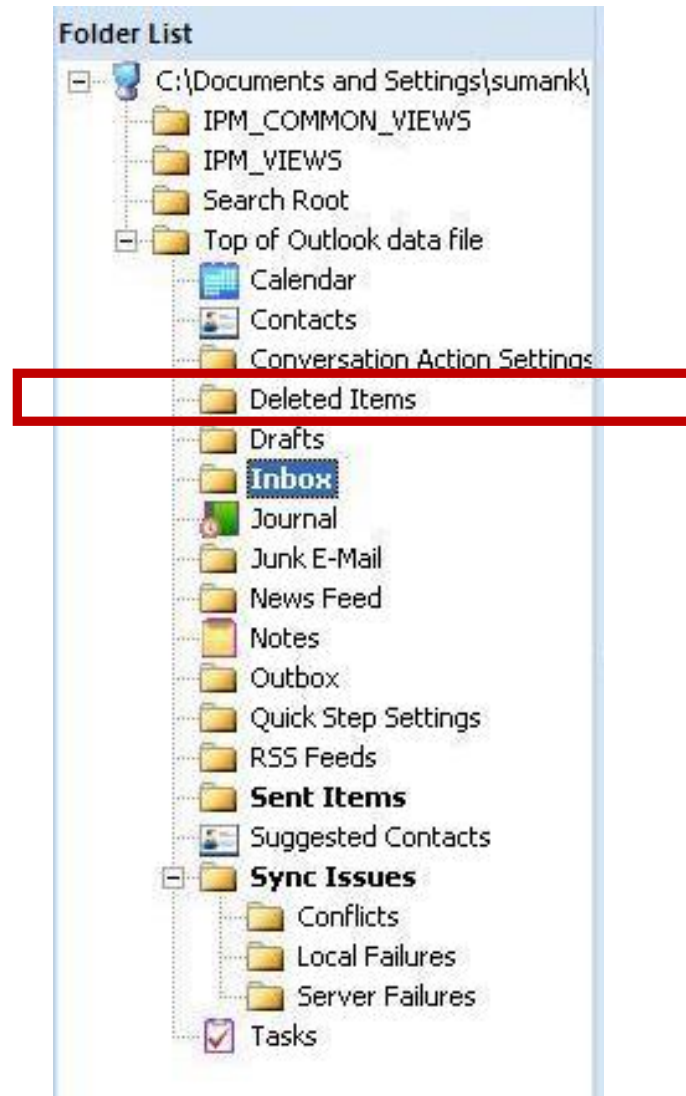
- Exporta el buzón **completo**
- Se realiza con **consentimiento** del usuario
- Objetivo: **Elementos recuperables**

Exchange: Elementos recuperables



- “**Papelera**” de Exchange
- **Invisibles** al usuario
- No solo correos (contactos, citas)
- Valor por defecto: **14 días / 30Gb**

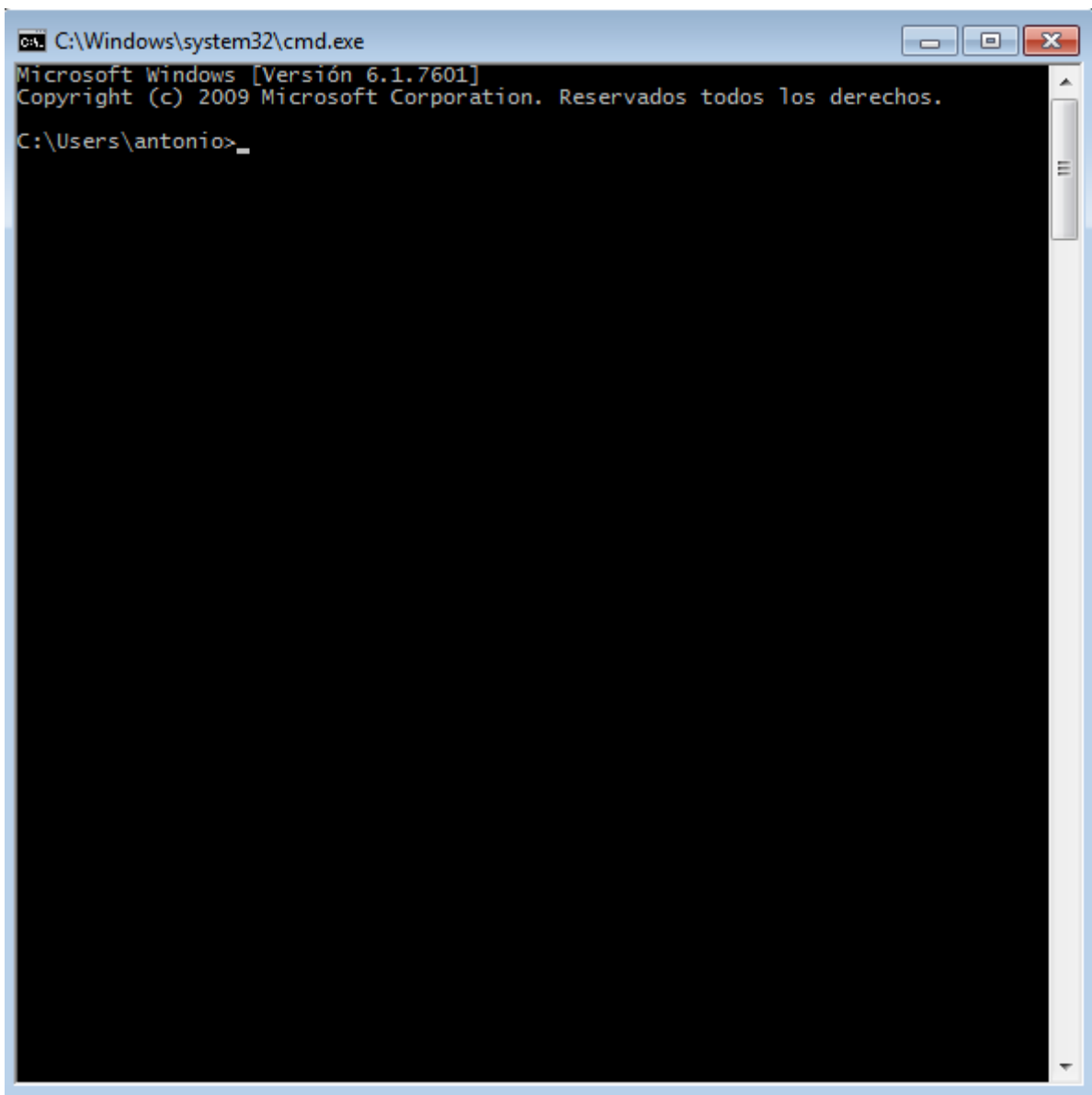
Email forensics: .pst analysis



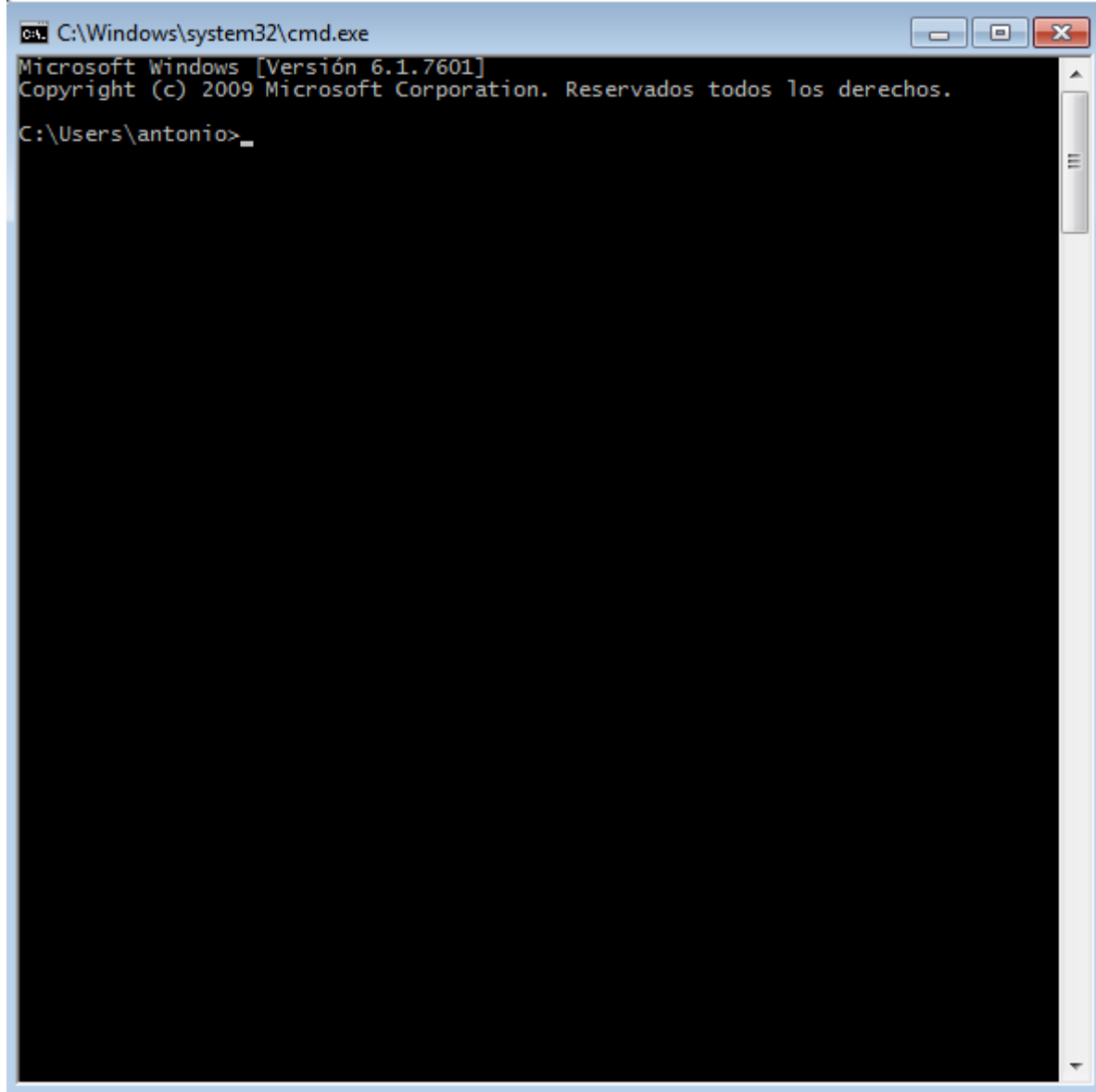
- Kernel Outlook PST Viewer (free)
- **!! Encontramos el correo !!**
- El correo ha sido **borrado**
- Encontramos el .doc **original**
- Firma distinta + Cabeceras: en-US

- Análisis forense → Equipo **limpio**
- ¿Cómo se ha **enviado** el correo?
- Exchange **comprometido** + posible
- Insistimos sobre **EventHistoryDB**





- Terminal de Windows



- Terminal de Windows
- 80 columnas de ancho

- Terminal de Windows
- 80 columnas de ancho
- ... y ésta es la salida

```

Símbolo del sistema
RecipientCount :
RelatedRecipientAddress :
Reference :
MessageSubject :
enal :
Sender :
ReturnPath :
MessageInfo :
MessageLatency :
MessageLatencyType :
EventId : [ItemEntryId, 00-00-00-00-7A-33 -A1-9F-C8-EB-3E-48-97-BA-E9-DA-15-8E-89-05-07-00-6E-E8 -F2-4A-22-A7-78-49-B7-DF-DF-BF-6B-CE-80
6a8da], [ItemEntryId, 00-00-00-00-7A-33
-A1-9F-C8-EB-3E-48-97-BA-E9-DA-15-8E-89-05-07-00-6E-E8
-F2-4A-22-A7-78-49-B7-DF-DF-BF-6B-CE-80

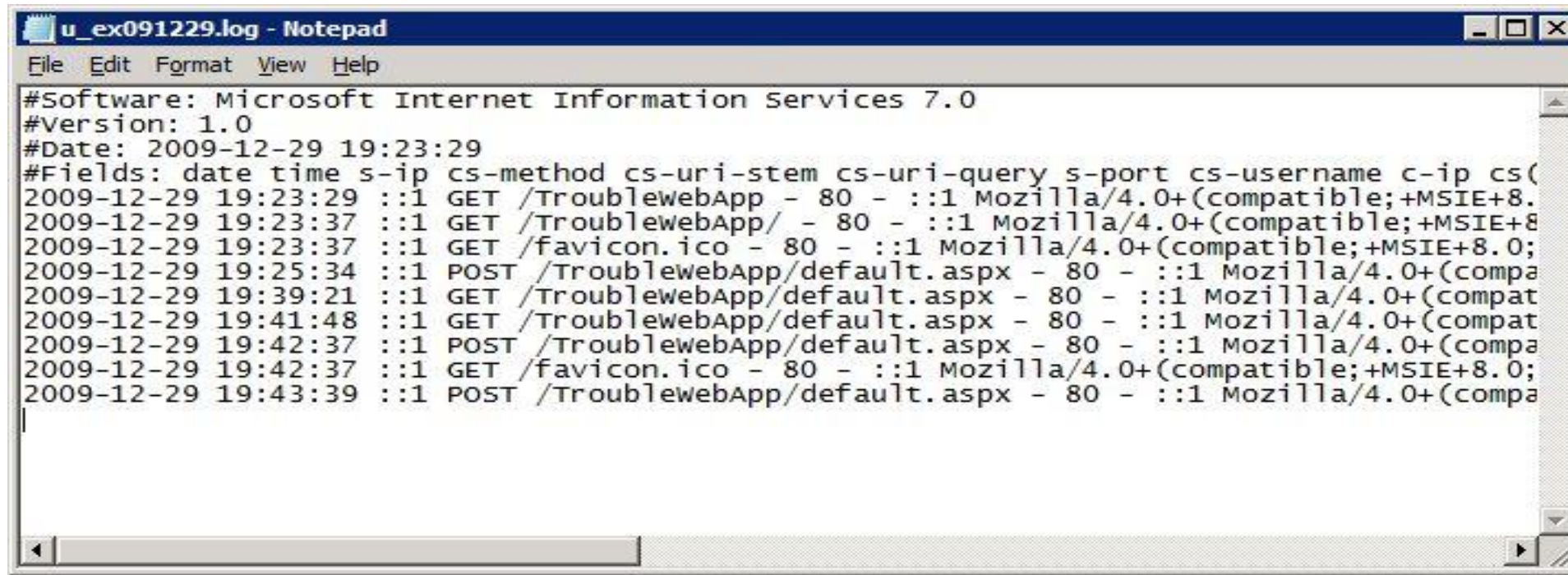
RunspaceId :
Timestamp :
ClientIp :
ClientHostname :
ServerIp :
ServerHostname :
SourceContext :
ConnectorId :
Source :
EventId :
InternalMessageId :
MessageId :

Recipients :
RecipientStatus :
TotalBytes :
RecipientCount :
RelatedRecipientAddress :
Reference :
MessageSubject :
enal :
Sender :
ReturnPath :
MessageInfo :
MessageLatency :
  
```

- Terminal de Windows
- 80 columnas de ancho
- ... y así es la salida
- **! VARIAS LINEAS !**



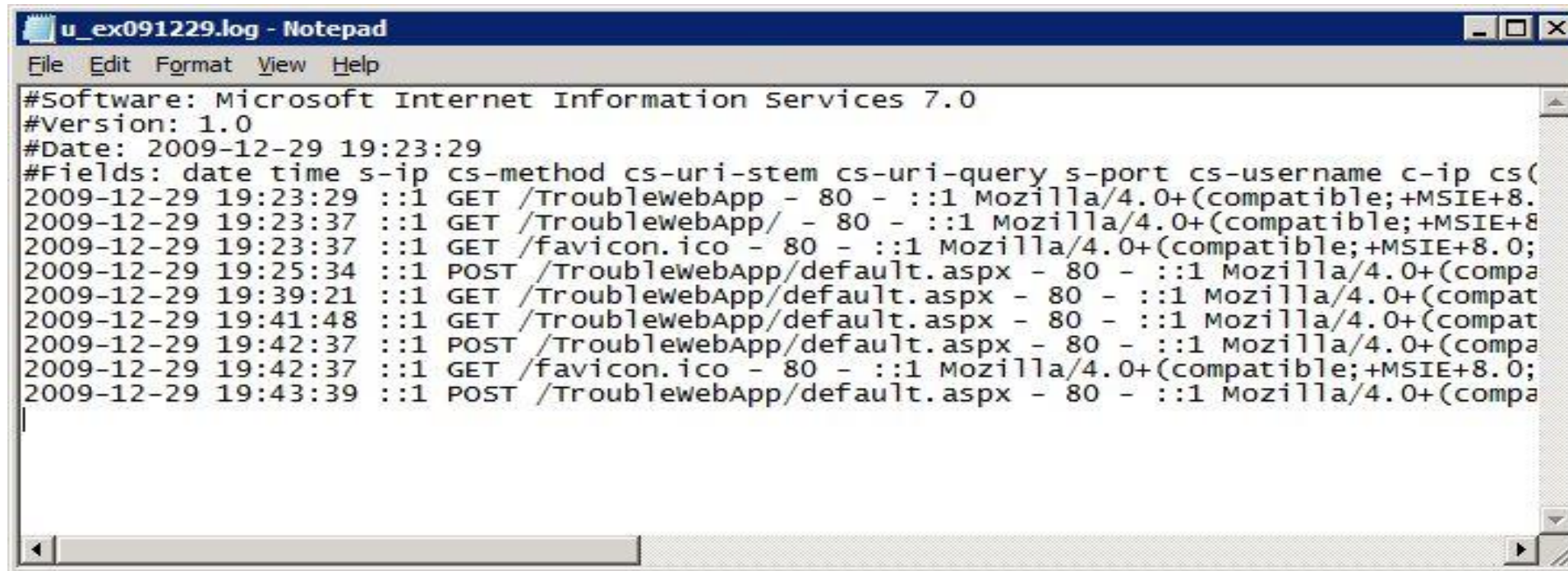
- $t=0$: Object Created
- $t+5\text{min}$: MailSubmitted
- $t+6\text{min}$: ObjectDeleted
- !!!!! ... vía **OWA** !!!!!



```

u_ex091229.log - Notepad
File Edit Format View Help
#Software: Microsoft Internet Information Services 7.0
#Version: 1.0
#Date: 2009-12-29 19:23:29
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(
2009-12-29 19:23:29 ::1 GET /TroublewebApp - 80 - ::1 Mozilla/4.0+(compatible;+MSIE+8.
2009-12-29 19:23:37 ::1 GET /TroublewebApp/ - 80 - ::1 Mozilla/4.0+(compatible;+MSIE+8
2009-12-29 19:23:37 ::1 GET /favicon.ico - 80 - ::1 Mozilla/4.0+(compatible;+MSIE+8.0;
2009-12-29 19:25:34 ::1 POST /TroublewebApp/default.aspx - 80 - ::1 Mozilla/4.0+(compa
2009-12-29 19:39:21 ::1 GET /TroublewebApp/default.aspx - 80 - ::1 Mozilla/4.0+(compat
2009-12-29 19:41:48 ::1 GET /TroublewebApp/default.aspx - 80 - ::1 Mozilla/4.0+(compat
2009-12-29 19:42:37 ::1 POST /TroublewebApp/default.aspx - 80 - ::1 Mozilla/4.0+(compa
2009-12-29 19:42:37 ::1 GET /favicon.ico - 80 - ::1 Mozilla/4.0+(compatible;+MSIE+8.0;
2009-12-29 19:43:39 ::1 POST /TroublewebApp/default.aspx - 80 - ::1 Mozilla/4.0+(compa
  
```

- Varios cientos de Mb
- Detectamos User-Agent : **Firefox**
- ... no desplegado en la Organización



```
u_ex091229.log - Notepad
File Edit Format View Help
#Software: Microsoft Internet Information Services 7.0
#Version: 1.0
#Date: 2009-12-29 19:23:29
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(
2009-12-29 19:23:29 ::1 GET /TroublewebApp - 80 - ::1 Mozilla/4.0+(compatible;+MSIE+8.
2009-12-29 19:23:37 ::1 GET /TroublewebApp/ - 80 - ::1 Mozilla/4.0+(compatible;+MSIE+8
2009-12-29 19:23:37 ::1 GET /favicon.ico - 80 - ::1 Mozilla/4.0+(compatible;+MSIE+8.0;
2009-12-29 19:25:34 ::1 POST /TroublewebApp/default.aspx - 80 - ::1 Mozilla/4.0+(compa
2009-12-29 19:39:21 ::1 GET /TroublewebApp/default.aspx - 80 - ::1 Mozilla/4.0+(compat
2009-12-29 19:41:48 ::1 GET /TroublewebApp/default.aspx - 80 - ::1 Mozilla/4.0+(compat
2009-12-29 19:42:37 ::1 POST /TroublewebApp/default.aspx - 80 - ::1 Mozilla/4.0+(compa
2009-12-29 19:42:37 ::1 GET /favicon.ico - 80 - ::1 Mozilla/4.0+(compatible;+MSIE+8.0;
2009-12-29 19:43:39 ::1 POST /TroublewebApp/default.aspx - 80 - ::1 Mozilla/4.0+(compa
```

- **Pivotamos sobre el User-Agent**
- **Encontramos una IP pública de la Org.**
- **... y encontramos lo siguiente**



Microsoft®
Outlook® Web App

Security ([show explanation](#))

☒ This is a public or shared computer
☐ This is a private computer
☐ Use the light version of Outlook Web App

User name:

E-mail Address:

Password:

[Sign in](#)

Connected to Microsoft Exchange
© 2010 Microsoft Corporation. All rights reserved.

- Acceso para los **móviles**
- ActiveSync + **OWA**
- **TODA** la Org. tiene acceso

- **Pivotamos sobre la IP**
- **3 usuarios comprometidos**
- **Otra IP (backup móviles)**

2. Contención



- Cerramos OWA 2 y 3
- Cambiamos passwords

3. Erradicación



- Revisamos los logs
- Múltiples intentos de login
- Revisamos correo de otros usuarios
- Revisamos equipos

4. Recuperación

Impacto del incidente





- Auditoria de **contraseñas**
- **Concienciación** de usuarios
- **Monitorización** de logs
- **Lista blanca** de móviles

5. Lecciones aprendidas

Atacantes siempre a las puertas



Revisa el perímetro



Usa doble factor de autenticación (2FA)



Conciencia a tus usuarios



Los logs son tus mejores amigos



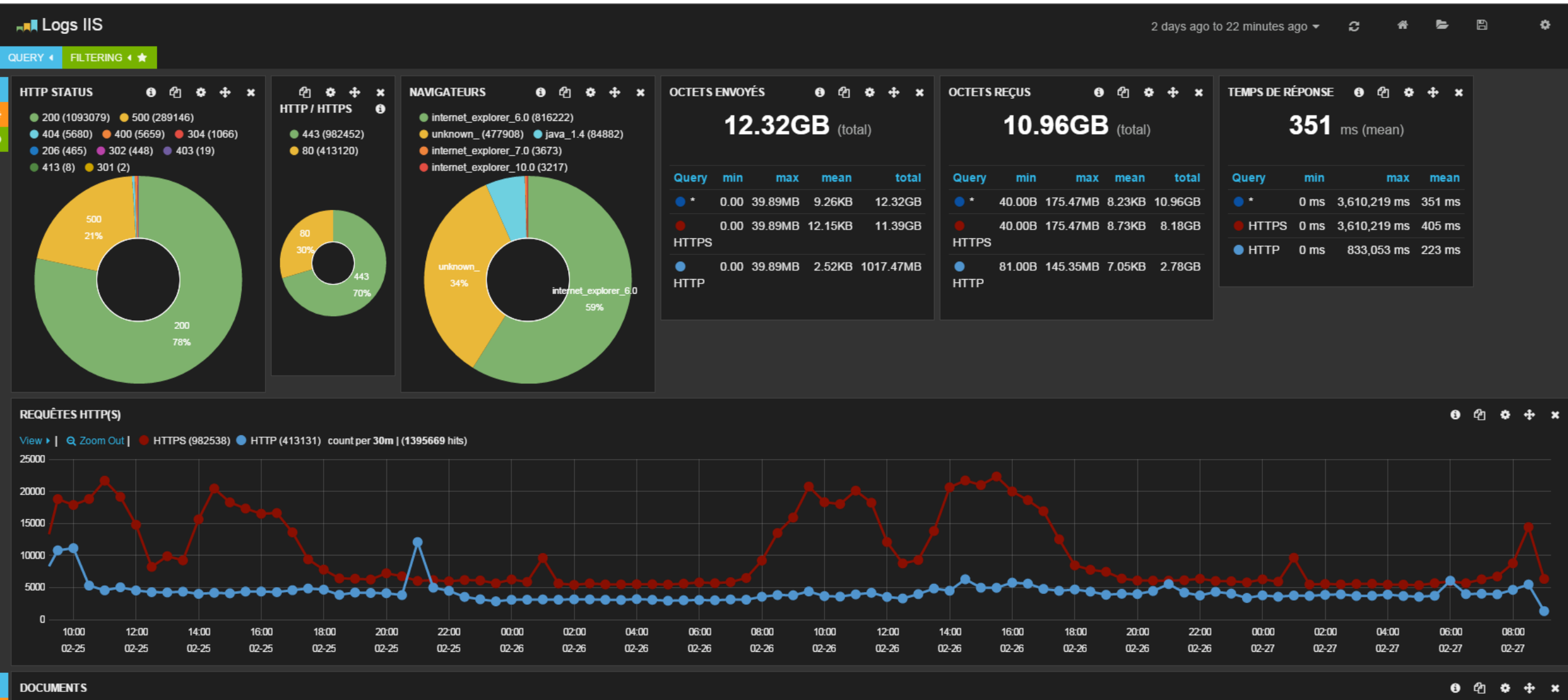
106 días*

dwel time

* FireEye M-Trends 2017 Report

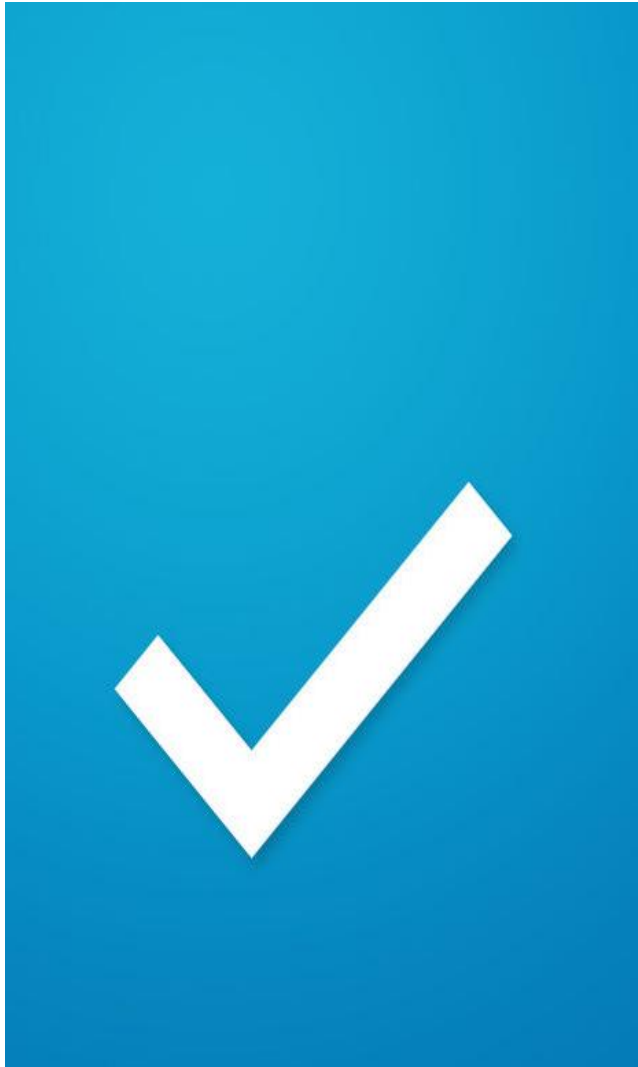
ASSUME
(106 days)
BREACH_

Recoge & Vigila





Exchange: Qué tienes que hacer HOY



- Verifica TODOS los accesos
- 2FA en los accesos externos
- Incrementa logging (EventHistory)
- Aumenta Elementos Recuperables
- Activa AuditLog para usuarios VIP
- Revisa tus logs

Referencias

EventHistory Table

<https://blogs.technet.microsoft.com/exchange/2013/06/24/adventures-in-querying-the-eventhistory-table>

Message Tracking

[https://technet.microsoft.com/es-es/library/bb124375\(v=exchg.141\).aspx](https://technet.microsoft.com/es-es/library/bb124375(v=exchg.141).aspx)

Mailbox access audit

<https://michaelfirsov.wordpress.com/2012/06/16/exchange-2010-mailbox-access-auditing-part-i/>

Mailbox delegations

[https://msdn.microsoft.com/en-us/library/office/bb204081\(v=exchg.140\).aspx](https://msdn.microsoft.com/en-us/library/office/bb204081(v=exchg.140).aspx)

Mailbox export

[https://technet.microsoft.com/es-es/library/ff607299\(v=exchg.141\).aspx](https://technet.microsoft.com/es-es/library/ff607299(v=exchg.141).aspx)

Elementos recuperables

[https://technet.microsoft.com/en-us/library/ee364755\(v=exchg.141\).aspx](https://technet.microsoft.com/en-us/library/ee364755(v=exchg.141).aspx)

Kernel Outlook PST Viewer

<https://www.nucleustechologies.com/pst-viewer.html>

IIS Log Format (OWA)

[https://msdn.microsoft.com/en-us/library/ms525807\(v=vs.90\).aspx](https://msdn.microsoft.com/en-us/library/ms525807(v=vs.90).aspx)

FireEye M-Trends 2017 Report

<https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html>

➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

➤ Síguenos en

