

Solución E5 Seguridad Office 365

Inteligencia Artificial



Identity & Access
Management



Threat
Protection



Information
Protection



Security
Management



INSTITUTO NACIONAL
DE LA VIVIENDA





INSTITUTO NACIONAL
DE LA VIVIENDA

Alertas por
actividad

Alerta de riesgo en equipo local

Microsoft Defender ATP New Informational Severity Alert Detected on scticdt09.invisd.local: 'Sality' malware was prevented

ⓘ Parte del contenido de este mensaje se ha bloqueado porque el remitente no está en la lista de remitentes seguros. [Confío en el contenido de wdatpntf@microsoft.com.](#) | [Mostrar contenido bloqueado](#)

🌐 Traducir mensaje a: Español | No traducir nunca de: Inglés

⌚ Etiqueta: Política Retención (5 años); fecha de vencimiento: Sáb 06/12/2025 11:37



Microsoft Defender ATP Alert Notification <wdatpntf@microsoft.com>

Lun 07/12/2020 11:37

Para: Seguridad Perimetral | Instituto Nacional de la Vivienda



Microsoft Defender Advanced Threat Protection - New alert

Customer	INSTITUTO NAC DE LA VIVIENDA
Title	'Sality' malware was prevented
Severity	Informational
Category	Malware
Detection source	Antivirus
Detection time	12/7/2020 3:37:47 PM UTC
Machine name	scticdt09.invisd.local
Alert page	https://securitycenter.windows.com/alert/da637429522671135145_-1124167004?tid=a1fdc8b0-1fe2-4a13-84e4-18c3688213ff

Evento-1

Alerta de riesgo almacenamiento en la nube

Medium-severity alert: Unusual volume of file deletion




Office365Alerts@microsoft.com

Mar 08/12/2020 18:25

Para: Julio Manuel Reyes Leon; Jason Javier Infante Severino; Yarbert Ledesma; Edwin Eduardo Paniagua Montilla

A medium-severity alert has been triggered

 Unusual volume of file deletion

Severity: ● Medium

Time: 12/8/2020 10:20:00 PM (UTC)

Activity: FileDeleted

Details: 30 matched activities in 5 minutes.

[View alert details](#)

Evento-2

Alerta de riesgo de identidad

Azure AD Identity Protection Weekly Digest

Microsoft Azure <azure-noreply@microsoft.co>
Para Jason Javier Infante Severino
Directiva de retención Política Retención (5 años)
Expira 11/30/2025
Tue 12/1/2020 10:49 AM

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

Microsoft Azure

Azure AD Identity Protection Weekly Digest

INSTITUTO NACIONAL DE LA VIVIENDA

New risky users detected 1	New risky sign-ins detected (in real-time) 1
--------------------------------------	--------------------------------------------------------

User at risk detected

Microsoft Azure <azure-noreply@microsoft.co>
Para Seguridad Perimetral | Instituto Nacional de la Vivienda
Directiva de retención Política Retención (5 años)
Expira 11/30/2025
Tue 12/1/2020 11:13 AM

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

Microsoft Azure

User at risk detected

We detected a new user with at least high risk in your INSTITUTO NACIONAL DE LA VIVIENDA directory. This might be because we noticed suspicious account activity or we found their emails and passwords posted in a public location.

[View detailed report >](#)



INSTITUTO NACIONAL
DE LA VIVIENDA

Auto investigación
y corrección de los
eventos de
seguridad

EVENTO - 1

Alerts > 'Sality' malware was pre... > 'Sality' malware was prevented on one endpoint

Alerts (1) Devices (1) Investigations (1) Evidence (4) Graph **beta**

First activity ↑	Title	Severity	Sta...	Linked ...	Category
12/7/20, 3:31 PM	'Sality' malware was prevented	Informational	New		Malware

'Sality' malware was prevented

Informational **New**

Open alert page See in timeline Link to another incident

Automated investigation 14 triggered by this alert is: Partially investigated

Manage alert

Status: Resolved

Classification: True alert

Determination: Malware

Alert details

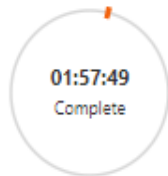
Incident	'Sality' malware was prevented on one endpoint
Detection source	Antivirus
Detection technology	Client
Detection status	Prevented
Category	Malware
First activity	Dec 7, 2020, 3:31:22 PM
Last activity	Dec 7, 2020, 3:35:15 PM
Generated on	Dec 7, 2020, 3:37:47 PM
Assigned to	(Unassigned)

'Sality' malware was prevented

Investigation #14 is complete - Encountered an Error Following New Leads

Tiempo transcurrido desde la detección del evento hasta la corrección de la alerta por parte de defender ATP

Started
Dec 7, 2020, 3:37:49 PM
Ended
Dec 7, 2020, 5:35:38 PM



Total pending time: 1:17m

Comments (0)

Investigation details

Status

Encountered an Error Following New Leads

The entities related to the alert were investigated but a problem stopped the investigation process on collateral entities.

Alert severity

Informational

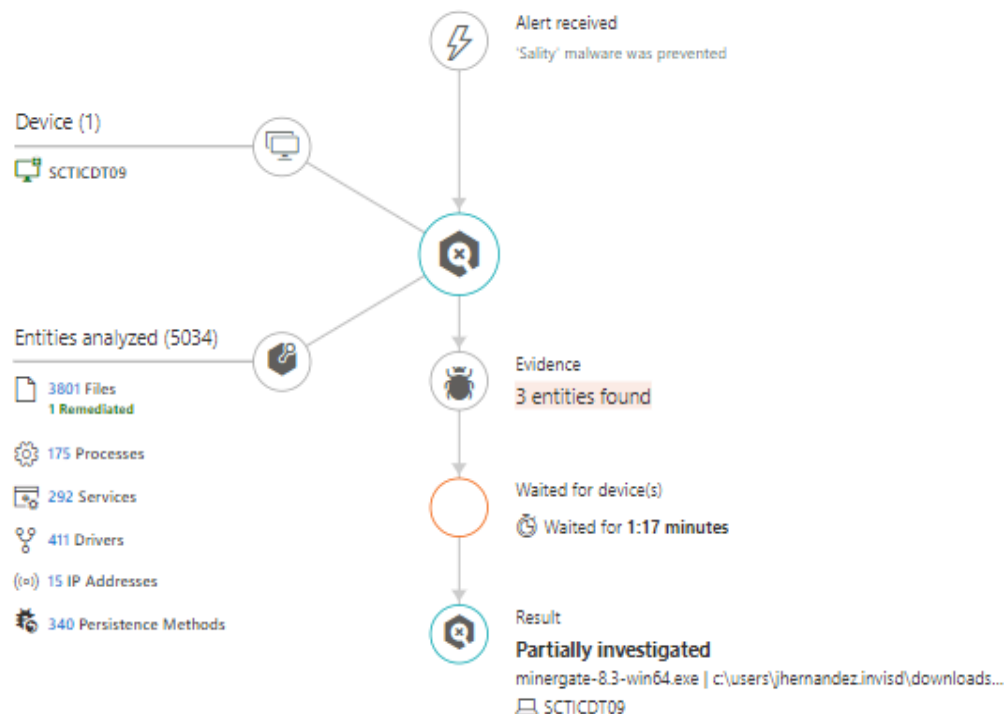
Category

Malware

Detection source

Antivirus

Investigation graph Alerts (1) Devices (1) Evidence (3) Entities (5,03k) Log (39)



'Sality' malware was prevented

Investigation #14 is complete - Encountered an Error Following New Leads

Started
Dec 7, 2020, 3:37:49 PM
Ended
Dec 7, 2020, 5:35:38 PM
Total pending time: 1:17m

01:57:49
Complete

Comments (0)

Investigation details

Status

Encountered an Error Following New Leads

The entities related to the alert were investigated but a problem stopped the investigation process on collateral entities.

Alert severity

Informational

Category

Malware

Detection source

Antivirus

Investigation graph Alerts (1) Devices (1) Evidence (3) Entities (5,03k) Log (39)

The following suspicious entities were investigated. The verdict for each is listed in the table below.

Type	Status	Device	Path	Impacted entity	Action	Detection type	Detection source
File	Unknown	SCTICDT09.INVISD.LOCAL	g:\system volume information.exe	system volume information.exe		Alert	'Sality' malware was prevented
File	Not found	SCTICDT09.INVISD.LOCAL	g:\system volume information.exe	system volume information.exe		Alert	'Sality' malware was prevented
File	Remediated	SCTICDT09.INVISD.LOCAL	c:\users\jhermandez.invisd\downloads\minerg:	minergate-8.3-win64.exe	The file was quarantined	Investigation	Get downloaded executable files

'Sality' malware was prevented

Investigation #14 is complete - Encountered an Error Following New Leads

Started
Dec 7, 2020, 3:37:49 PM
Ended
Dec 7, 2020, 5:35:38 PM
Total pending time: 1:17m

01:57:49
Complete

Comments (0)

Investigation details

Status

Encountered an Error Following New Leads

The entities related to the alert were investigated but a problem stopped the investigation process on collateral entities.

Alert severity

Informational

Category

Malware

Detection source

Antivirus

Investigation graph Alerts (1) Devices (1) Evidence (3) **Entities (5,03k)** Log (39)

Evidence summary (5,034)

- Files (3,801)
- Processes (175)
- Services (292)
- Drivers (411)
- IP Addresses (15)
- Persistence Methods (340)

All evidence (5,034)

Entity type	Total	Remediated	Malicious	Suspicious	Verified	No threats found	Unknown	Not found	Unremediated
Files	3801	1	-	-	-	3,688	102	10	-
Processes	175	-	-	-	-	165	10	-	-
Services	292	-	-	-	-	292	-	-	-
Drivers	411	-	-	-	-	408	3	-	-
IP Addresses	15	-	-	-	-	3	12	-	-
Persistence Methods	340	-	-	-	-	204	136	-	-

EVENTO - 2

- Inicio
- Alertas
- Permisos
- Clasificación
- Prevención de pérdida de datos
- Administración de registros
- Gobierno de información
- Supervisión
- Administración de amenazas

Inicio > Alertas > Ver alertas

Ver alertas



<input type="checkbox"/>	Gravedad	Nom
<input type="checkbox"/>	Media	Unusu

"1 elementos cargados.

Unusual volume of file deletion

✓ Resolver

⊘ Suprimir

Gravedad

● Media

Hora

8 dic. 2020 18:20:00

Actividad

Se ha eliminado el archivo

Recuento de actividades

30 ⓘ

[Ver lista de actividades](#)

Detalles

This alert is triggered when the volume of files deleted in your organization becomes unusual -V1.0.0.1

Estado

Activo

[Editar](#)

Comentarios

New alert

Cerrar

Listado de actividad,
describe:
el usuario, tipo y nombre del archivo eliminado, tiempo exacto de eliminación y la localización en donde office 365 envía los documentos para su almacenamiento provisional, hasta confirmar si el evento fue malicioso o no.

Lista de actividades

✉ Notificar a los usuarios

🔍 Buscar actividades similares

↓ Exportar

<input type="checkbox"/>	Fecha	Actividad	Usuario:	Elemento	Dirección IP
<input type="checkbox"/>	8 dic. 2020 22:16:04	FileDeleted	j.dieguez@invi.go...	Camino playa Ro...	186.6.135.7
<input type="checkbox"/>	8 dic. 2020 22:16:05	FileDeleted	j.dieguez@invi.go...	Formulario de Re...	186.6.135.7
<input type="checkbox"/>	8 dic. 2020 22:16:05	FileDeleted	j.dieguez@invi.go...	MEMORIA DESCR...	186.6.135.7
<input type="checkbox"/>	8 dic. 2020 22:16:05	FileDeleted	j.dieguez@invi.go...	ANEXOS AL FOR...	186.6.135.7
<input type="checkbox"/>	8 dic. 2020 22:15:54	FileDeleted	j.dieguez@invi.go...	10-06-CAMINO L...	186.6.135.7
<input type="checkbox"/>	8 dic. 2020 22:15:54	FileDeleted	j.dieguez@invi.go...	10-04-CAMINO L...	186.6.135.7

"30 elementos cargados.

Cerrar

EVENTO - 3

Identity Protection | Risk detections

Search (Ctrl+/)

Learn more | Download | Refresh | Columns | Got feedback?

- Overview
- Protect
 - User risk policy
 - Sign-in risk policy
 - MFA registration policy
- Report
 - Risky users
 - Risky sign-ins
 - Risk detections**
- Notify
 - Users at risk detected alerts
 - Weekly digest
- Troubleshooting + Support
 - Troubleshoot
 - New support request

11/25/2020, 10:18:19 ...	Ing. Carlos Novas	45.56.200.185	Miami, Florida, US	Unfamiliar sign-in pro...	Dismissed	Medium	c113b563-f810-4252-..
11/19/2020, 12:54:52 ...	Domingo Contreras	181.36.206.170	Santo Domingo, Distri...	Unfamiliar sign-in pro...	Dismissed	Low	f771b80b-485d-4072-..
11/19/2020, 10:02:36 ...	Robert Eduardo Lapaix...	181.37.41.142	Santo Domingo, Distri...	Unfamiliar sign-in pro...	Dismissed	Low	9adfc5f1-b7a4-4cd7-9..

Details

- User's risk report
- User's sign-ins
- User's risky sign-ins
- Linked risky sign-in
- User's risk detections**

Detection type	Unfamiliar sign-in properties	Activity	Sign-in	Sign-in time	11/25/2020, 10:18 AM
Risk state	Dismissed	Detection time	11/25/2020, 10:18 AM	IP address	45.56.200.185
Risk level	Medium	Detection last updated	12/1/2020, 11:38 AM	Sign-in location	Miami, Florida, US
Risk detail	Admin dismissed all risk for user	Token issuer type	Azure AD	Sign-in client	Mozilla/5.0 (iPhone; CPU iPhone OS 14_3 like Mac OS X)
Source	Identity Protection	Sign-in request id	c113b563-f810-4252-9ecd-b72aa327f200		
Detection timing	Real-time	Sign-in correlation id	35a87f34-a3a6-4685-bdae-7cdc14e78e32		

Usuario Bloqueado: Debido al comportamiento inusual en el login del usuario este fue bloqueado.

Descripción del evento

Identificación de la solicitud	Tiempo de detección
fdbed23201d5d55e466f976ec109098d7	Tiempo real
Identificador de correlación	Actividad
35a87f34-a3a6-4685-bdae-7cdc14e78e32	Inicio de sesión
Tipo de detección	Activity time
Propiedades de inicio de sesión desconocidos	2020-11-25T14:18:19.5945919Z
Estado de riesgo	Detection time
Confirmado comprometido	2020-11-25T14:18:19.5945919Z
Nivel de riesgo	Detection last updated
Medio	2020-12-01T15:18:07.6390818Z
Detalle de riesgo	User object ID
El administrador confirmó el inicio de sesión comprometido	2b0b5a32-a296-4247-9e4f-33c10e49a65e
Fuente	Usuario
Protección de la identidad	Ing. Carlos Novas
UPN	IP address
Cnovas@invi.gob.do	45.56.200.185
Location	Miami - Florida - US
<p>Nota: El caso fue evaluado. Según verificamos con el Sr. Carlos Nova, el mismo nos comunico que estaba utilizando un cliente VPN en su equipo móvil, en donde tiene registrada la cuenta de la institución. Le comunicamos que este tipo de acción hace que la cuenta se bloquee.</p>	



INSTITUTO NACIONAL
DE LA VIVIENDA

Protección de correos

Inicio

Alertas

Permisos

Clasificación

Prevención de pérdida de datos

Administración de registros

Gobierno de información

Supervisión

Administración de amenazas

Inicio > Panel

Conclusiones y recomendaciones principales [Ver todo](#)



Usuarios que son objetivo de campañas de suplantación de

Revise la lista de usuarios que han sido objeto del mayor número de campañas de suplantación de identidad.



Más conclusiones próximamente...

Las conclusiones que se muestran se basan en el análisis de la configuración y las recomendaciones para optimizar y mejorar las características de seguridad.



Dominios probablemente suplantados en los últimos 7

Es probable que 128 dominios se vieran afectados en su organización por el intento de algunos remitentes de suplantar la identidad (spoofing).

53

Dominios sospechosos

La inteligencia contra la suplantación de la identidad ha recibido señales importantes que indican que estos dominios pueden ser sospechosos.

75

Dominios no sospechosos

La inteligencia contra la suplantación de la identidad recibió señales significativas que indicaban que estos dominios deberían pasar por comprobaciones de autenticación.

Informes disponibles



Suplantaciones en los últimos 7 días

La inteligencia de suplantación protegió a los usuarios y dominios que se indican a continuación.

0

Dominios suplantados

La protección de dominios incluye dominios de tu propiedad y dominios personalizados.

4

Usuarios suplantados

Es necesario configurar los usuarios protegidos en la directiva de suplantación.



Panel protección inteligente: Office 365 toma medidas según el comportamiento de dominios y cuentas maliciosas

¿Necesita ayuda?

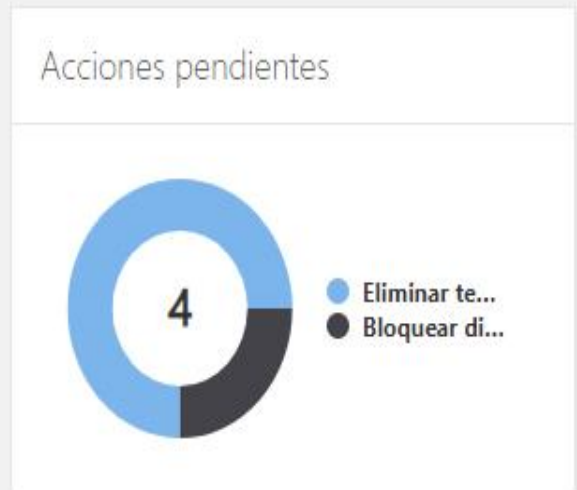
Enviar comentarios

- Inicio
- Alertas
- Permisos
- Clasificación
- Prevención de pérdida de datos
- Administración de registros
- Gobierno de información
- Supervisión
- Administración de amenazas

Inicio > Panel de seguridad

Resumen de investigaciones

No hay datos disponibles



Principa

Cebo purg

Cómo hemos protegido su organización frente a las amenazas en los últimos 7 días

Configurar archivos adjuntos seguros

Configurar protección para SPO, ODB y Teams para la protección contra malware de día cero

Protección contra amenazas avanzadas de malware de día cero en mensajes de correo electrónico y archivos de SharePoint, OneDrive y

13

mensajes detectados de phishing avanzada

Protección contra amenazas avanzadas de suplantación de identidad y phishing de objetivo definido

Configurar vínculos seguros

para la protección en el momento del clic

Vínculos maliciosos bloqueados en mensajes entrantes y en el ámbito de su organización mediante la protección en el momento del clic de Vínculos seguros

Informe de protección de ...

Detecciones de amenazas globales semanales



- Inicio
- Alertas
- Permisos
- Clasificación
- Prevención de pérdida de datos
- Administración de registros
- Gobierno de información
- Supervisión
- Administración de amenazas
- Flujo de correo
- Privacidad de los datos
- Buscar

Inicio > Explorador

Explorador es una herramienta eficaz y casi en tiempo real para ayudar a los equipos de operaciones de seguridad a investigar y responder a amenazas en el Centro de seguridad y cumplimiento. Obtenga más información sobre [Explorador](#).

Ver [Suplantar identidad](#)

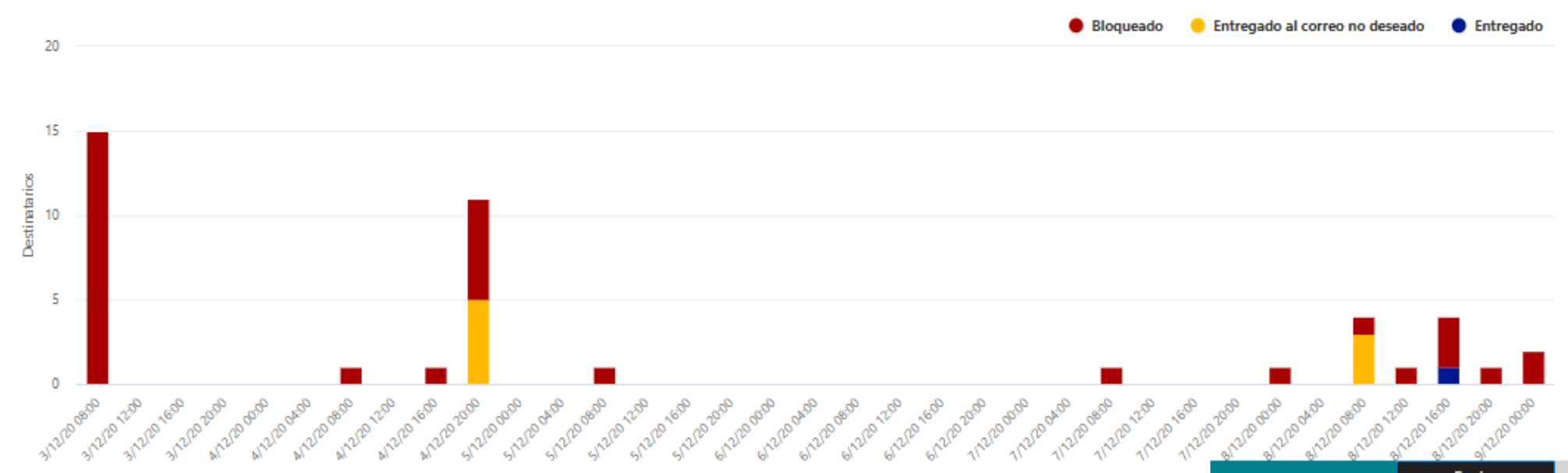
Esta vista muestra información sobre los mensajes de correo electrónico identificados como mensajes con amenazas de phishing. También puede tener una vista de las direcciones URL y los clics en las direcciones URL dentro de los correos electrónicos. Esta vista muestra características, como filtros útiles para la búsqueda de amenazas en mensajes de correo electrónico, así como capacidad para exportar hasta 9.990 registros para su análisis sin conexión. [Mostrar más](#)

|
 |
 |

Utilice comas (,) para separar varias entradas. Haga clic en

-

Acción de entrega



Zona horaria del gráfico: (UTC -04:00)

- [Inicio](#)
- [Alertas](#)
- [Permisos](#)
- [Clasificación](#)
- [Prevención de pérdida de datos](#)
- [Administración de registros](#)
- [Gobierno de información](#)
- [Supervisión](#)
- [Administración de amenazas](#)
- [Flujo de correo](#)
- [Privacidad de los datos](#)
- [Buscar](#)










Mensaje de correo electrónico
 Clics en la dirección URL
 Direcciones URL
 Principales usuarios de destino
 Origen de correo electrónico
 Campaña

+ Acciones

Opciones de columna

<input type="checkbox"/>	Fecha (UTC -04:00) ...	Asunto	Destinatario	Etiquet...	Remitente	A... Última ubicación de ...	Ubicación de entrega...
<input type="checkbox"/>	9/12/20 02:12	invi_rd Paid Sponsorship	j.reyes@invi.gob.do	-	influenceenhance@gmail.com	- Cuarentena	Cuarentena
<input type="checkbox"/>	9/12/20 02:12	invi_rd Paid Sponsorship	j.hernandez@invi.gob.do	-	influenceenhance@gmail.com	- Depositado	Depositado
<input type="checkbox"/>	8/12/20 20:33	Cuenta APAPenLine@ Restringida	transparencia@invi.gob.do	-	servicioalcliente@apap.com.do	- Cuarentena	Cuarentena
<input type="checkbox"/>	8/12/20 19:28	1 new voice caller on 08 Decemb...	k.garcia@invi.gob.do	-	frecom@frecom.com	- Cuarentena	Cuarentena

43 elemento(s) de 43 cargados

-  Administración de amenazas
-  Flujo de correo
-  Privacidad de los datos
-  Buscar
-  eDiscovery
-  Informes
- Panel
- Administrar
- programaciones
- Informes para su descarga
-  Garantía del servicio

Inicio > Conclusión de suplantación

La inteligencia de suplantación tuvo indicios importantes de que los siguientes correos son sospechosos. Según nuestro análisis, necesita revisar todos los intentos de suplantación siguientes y, si es necesario, agregarlos a la lista de suplantación permitida (si corresponde). Puede usar esta experiencia de conclusión para supervisar los posibles correos afectados. [¿Qué es la suplantación de usuario y de dominio?](#)

Nuestra recomendación: según nuestro análisis, la directiva está configurada correctamente (vea las directivas de suplantación).

Filtro de remitente, separado por "," Actualizar Exportar

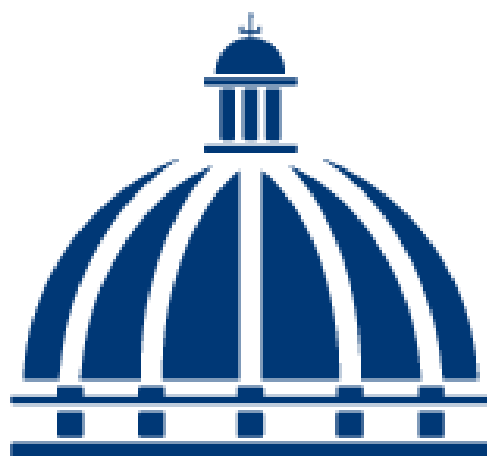
<input type="checkbox"/>	Remitente	N...	Tipo de suplantación	Tipo de usuario ...	Directiva	Suplantación permitida ...
<input type="checkbox"/>	raykamenam@gmail.com	2	Usuario en nombre para mostrar	Inteligencia de buzo...	Protección General	No
<input type="checkbox"/>	cn19-1353@unphu.edu.do	1	Usuario en nombre para mostrar	Inteligencia de buzo...	Protección General	No
<input type="checkbox"/>	elisamorel678@gmail.com	1	Usuario en nombre para mostrar	Inteligencia de buzo...	Protección General	No
<input type="checkbox"/>	paty_1837@hotmail.com	1	Usuario en nombre para mostrar	Inteligencia de buzo...	Protección General	No

- Inicio
- Alertas
- Permisos
- Clasificación
- Prevención de pérdida de datos
- Administración de registros
- Gobierno de información
- Supervisión
- Administración de amenazas

Inicio > Información de la inteligencia contra la suplantación de la identidad

La inteligencia contra la suplantación de identidad recibió señales importantes que indican que estos dominios pueden ser sospechosos. Revise cada par de dominios para encontrar falsos positivos y agréguelos a la Lista de permitidos si es necesario. Para obtener una lista completa de los pares de dominios protegidos por la inteligencia contra la suplantación de identidad, use el cmdlet `Get-PhishFilterPolicy`. [Obtenga más información sobre la inteligencia contra la suplantación de identidad.](#)

<input type="checkbox"/>	Dominio con identidad ...	Infraestructura	Número de mens...	Última visualizaci...	Tipo de suplanta...	Suplantación de
<input type="checkbox"/>	hotmail.com	constantcontact.com	16	3/12/2020	Externo	No
<input type="checkbox"/>	minurvi-lac.org	mailjet.com	12	3/12/2020	Externo	No
<input type="checkbox"/>	gmail.com	ymlopsvr.com	10	3/12/2020	Externo	No
<input type="checkbox"/>	eximediard.com	mandrillapp.com	9	3/12/2020	Externo	No
<input type="checkbox"/>	gmail.com	constantcontact.com	9	1/12/2020	Externo	No
<input type="checkbox"/>	wecraft.info	secureserver.net	7	5/12/2020	Externo	No



GOBIERNO DE LA
REPÚBLICA DOMINICANA

INVI