Universidad de Buenos Aires
Facultades de Ciencias Económicas,
Cs. Exactas y Naturales e Ingeniería

Carrera de Especialización en
Seguridad Informática

Trabajo Final

Ataques y protección en el servicio de correo electrónico

Autor: Claudio Corbellini
Tutor: Julio Ardita

Año
2024

Cohorte del Cursante
2013

Declaración Jurada de origen de los contenidos

"Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual"

Nombre: Claudio Corbellini

DNI: 30340911

FIRMADO

Resumen

La confianza en el envío, recepción y confidencialidad del correo electrónico resulta hoy en día un aspecto de seguridad crítico en la infraestructura de comunicaciones de cualquier organización.

El correo electrónico se utiliza masivamente para la transmisión de todo tipo de comunicaciones, que incluye desde información pública y publicidad, hasta comunicaciones altamente confidenciales sobre transacciones de pago/cobro críticas en una organización.

Sin embargo su funcionamiento y la evolución técnica de su seguridad es una temática no tan conocida, y que no es fácil de hallar explicada de forma clara.

Los ataques de tipo Spoofing y Business Email Compromise (BEC), han tenido un crecimiento exponencial en los últimos años. Colocándolos entre los ataques con mayores pérdidas reportadas anualmente por el Centro de Crimen en Internet (IC3 - Internet Crime Complaint Center) del FBI de Estados Unidos.

Es imposible entender como estos ataques se mantienen aún tan efectivos, sin comprender como evolucionaron los protocolos, sistemas y clientes aplicativos de correo electrónico, y como todas estas capas de seguridad actualmente interactúan en una infraestructura moderna. Cuáles son los puntos fuertes y donde están los eslabones más débiles en todo el circuito de comunicación.

Se examinarán ataques típicos para entender la metodología y vectores utilizados. Así como se analizará cuáles son las debilidades técnicas que típicamente se encuentran en infraestructuras de correo electrónico corporativas.

El objetivo final es poder tener el conocimiento necesario para evaluar el nivel de seguridad en la que se encuentran las organizaciones, establecer medidas de seguridad específicas para aumentar el nivel de protección y disminuir el riesgo de ser un blanco vulnerable.

Palabras clave: correo, gateway, autenticación, dominio, spoofing, phishing, malware, spam, relay.

Tabla de contenidos

Nómina de abreviaturas

- BEC: Ataque de compromiso a los correos electrónicos corporativos ("Business Email Compromise")
- DKIM: Identificación de correos por claves de dominio (“DomainKeys Identified Mail”)
- DMARC: Autenticación, reportes y conformidad de mensajes basados en dominio (“Domain-based Message Authentication, Reporting and Conformance”)
- IMAP: Acceso a mensajes de Internet ("Internet Message Access Protocol").
- MUA: Agente de usuario de correo electrónico ("Mail User Agent")
- MDA: Agente de entrega de correos ("Mail Delivery Agent")
- MSA: Servicio de envío correo ("Mail Submission Agent ")
- MTA: Componente de transferencia de correo ("Mail Transfer Agent")
- MX: Servidor de intercambio de correos ("Mail Exchanger")
- POP: Protocolo de oficina de postal ("Post Office Protocol")
- SPF: Marco de convenio entre remitentes (“Sender Policy Framework”)
- SMTP: Protocolo para transferencia simple de correo (“Simple Mail Transfer Protocol”)
- SSL: Seguridad de la capa de transporte (“Secure Sockets Layer”)

Cuerpo introductorio

Los ataques al sistema de correo electrónico son una de las mayores causantes de pérdidas económicas en el ámbito de la seguridad informática, éstos tienen como principal objetivo desviar pagos realizados vía transferencias bancarias.

En los últimos 7 años he analizado en profundidad más de 40 casos de ataques en el ámbito corporativo de Business Email Compromise (BEC), Spoofing y Phishing, con el objetivo de entender cómo se realizó el ataque, dónde originó el compromiso de seguridad para obtener la primera cadena de correo electrónico, cómo se desviaron comunicaciones, determinar si se crearon dominios falsos para lograr la suplantación, efectuar los análisis de encabezados de correo, hacer investigación forenses de los documentos adulterados (facturas, comprobantes de transferencias, etc). Con el propósito adicional de proponer y ejecutar mejoras en las medidas de seguridad técnicas, procedimentales y de capacitación para reducir impacto y minimizar la probabilidad de ser sujeto nuevamente de ataques similares.

El objetivo es compilar un análisis de las capas de seguridad que se fueron sumando hasta llegar a una infraestructura de correo electrónico típica actual, el estudio de las metodologías de ataque más utilizadas en los últimos años y las recomendaciones específicas de cómo mejorar la protección en las organizaciones.

1 La evolución de la seguridad en el correo electrónico

1.1 El nacimiento del protocolo SMTP

En el año 1981 el correo electrónico tuvo su primer gran paso para convertirse en lo que los conocemos hoy, con la publicación de la RFC788 "Simple Mail Transfer Protocol" (SMTP).

Estructura de datos básica y ejemplo de una comunicación simple entre un cliente("C") y servidor de correo ("S"):

```
S: 220 smtp.ejemplo.com ESMTP Postfix
C: HELO relay.ejemplo.com
S: 250 Hola relay.ejemplo.com, en qué puedo ayudarte
C: MAIL FROM:<juan@ejemplo.com>
S: 250 Ok
```

```
C: RCPT TO:<julio@ejemplo.com>
S: 250 Ok
C: RCPT TO:<pedro@ejemplo.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: From: "Juan ejemplo" <juan@ejemplo.com>
C: To: "Julio ejemplo" <julio@ejemplo.com>
C: Cc: pedro@ejemplo.com
C: Date: Tue, 6 Feb 2024 13:01:53 -0300
C: Subject: mensage de prueba
C: Hola Julio,
C: Este es el cuerpo del mensaje.
C: Saludos.
S: 250 Ok: queued as 555
C: QUIT
S: 221 Bye
{Se cierra la conexión}
```

Simplificando los pasos son: un saludo (o "handshake") inicial, el detalle del remitente ("MAIL FROM"), la lista de destinatarios ("RCPT TO") y el contenido o datos del mail ("DATA"). Finalmente si no hay más correos a enviar, el cierre de la comunicación ("QUIT").

1.2 La arquitectura del correo electrónico

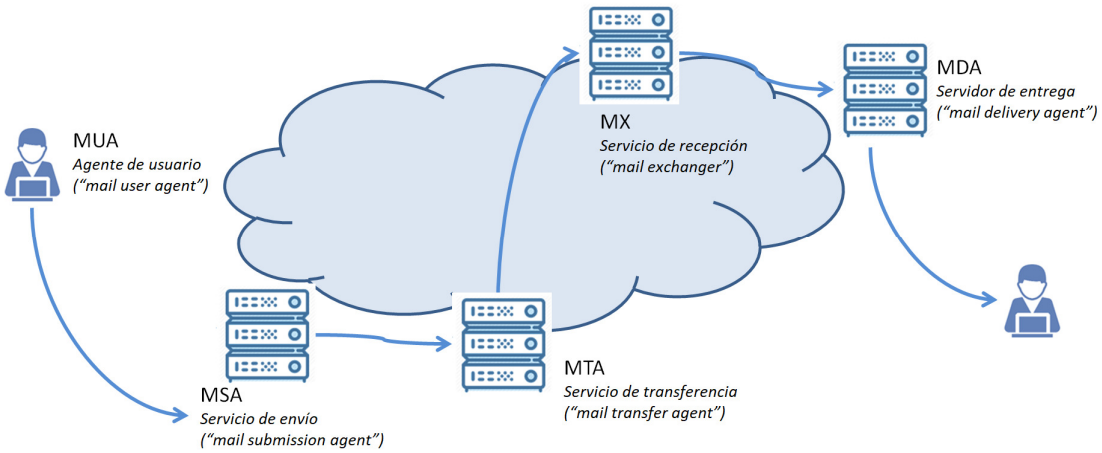
El correo electrónico tuvo como objetivo fundamental el reemplazo del correo físico, por lo que su lógica es similar, y cómo veremos más adelante, también arrastrará muchas de las debilidades de seguridad que son intrínsecas a este modelo de comunicación entre partes.

A continuación se describe el modelo conceptual más básico de envío de un correo electrónico. Lo cierto es que en una infraestructura moderna se han sumado varias capas y saltos adicionales, pero el circuito general se ha mantenido esencialmente igual.

En el modelo SMTP un agente de usuario de correo electrónico o "cliente" (MUA: mail user agent) envía datos a un servidor de envío correo

(MSA: mail submission agent). El MSA entrega el correo a un componente de transferencia de correo (MTA: mail transfer agent).

El MTA establece un circuito de comunicación con un servidor destino MX (mail exchanger), destino que podríamos generalizar diciendo que se encuentra publicado en Internet. El MX envía el correo a un servicio de entrega (MDA: mail delivery agent), que finalmente pondrá ser accedido por un cliente de correo por el usuario.



Modelo de conceptual del sistema de correo electrónico

El correo electrónico se transmite, en forma de "almacenamiento y reenvío", a través de agentes de transferencia de correo (MTA). Los MTA se comunican mediante SMTP y actúan como cliente y servidor, según el caso. Por ejemplo, un MTA puede actuar como servidor al aceptar un mensaje de correo electrónico del MUA de un usuario y luego actuar como cliente al transferir el mensaje al MTA del dominio del destinatario para ser entregado.

Lo más relevante de entender es que, a diferencia de otros mecanismo de comunicación el correo electrónico es un proceso siempre unidireccional y asincrónico. Por lo que la ¨respuesta¨ a un correo, es una nueva comunicación desde cero y que no utilizará exactamente el mismo circuito en sentido inverso, sino que podría seguir otro muy diferente.

1.3 Resumen de protocolos de acceso al correo electrónico

No se utiliza SMTP cuando se recuperan correo del buzón de un usuario, solo para enviarlo. Los MUA utilizan otro protocolo cliente-servidor para recuperar el correo de un servidor y mostrarlo en el sistema de un usuario final. Estos protocolos de acceso al correo pueden ser el protocolo de oficina postal (POP: "Post Office Protocol ") o el de acceso a mensajes de Internet (IMAP:"Internet Message Access Protocol").

El POP versión 3 ("POP3") es el más simple de los dos protocolos y generalmente descarga todo el correo desde el servidor y luego elimina la copia, aunque existe la opción de mantenerla en el servidor. POP3 es similar a SMTP, en que el cliente se conecta a un puerto y envía comandos de texto, a los que el servidor responde.

IMAP es una alternativa a POP3, incluye más funciones. Los clientes IMAP pueden descargar mensajes de correo electrónico, pero los mensajes generalmente permanecen en el servidor. Esto y el hecho de que varios clientes puedan acceder al mismo buzón simultáneamente significa que los usuarios con múltiples dispositivos pueden mantener su correo electrónico sincronizado en múltiples dispositivos. Al igual que POP3, IMAP también tiene la capacidad de proteger la conexión con cifrado.

Además de POP3 e IMAP, existen otros protocolos propietarios que se utilizan en implementaciones corporativas. Los clientes de Outlook pueden utilizar la interfaz de programación de aplicaciones de mensajería (MAPI: "Messaging Application Programming Interface") para acceder a un buzón de Microsoft Exchange. Los proveedores de nube también ofrecen acceso al buzón utilizando un portal web en lugar de un cliente de correo electrónico dedicado. La mayoría de los portales web suelen utilizar internamente IMAP para acceder al buzón del usuario con la excepción de Outlook Web Access("OWA") de Microsoft. Para el usuario la migración a una interfaz Web significó un cambio de paradigma, que simplificó el uso al eliminar el cliente y sus configuraciones.

1.4 Debilidades del correo como método de comunicación

El objetivo del desarrollo del correo electrónico fue inicialmente el reemplazo de el correo físico, por lo que no pretendía tener mayores controles que éste.

En un correo papel tradicional el destinatario y remitente son datos aportados por quién lo escribe, y no existe validación posible sobre si son correctos o reales. En SMTP esto no varía y el remitente es un campo de texto en la que se puede indicar cualquier cadena de texto.

Por lo que la suplantación de identidad fue posible desde el inicio del correo electrónico, igual que en su par, el correo papel. Para garantizar la autenticidad del remitente de un correo físico se han usado diferentes medidas de seguridad como: sellos, marcas de agua, membretes, tipos de papel, etc. Siempre con el objetivo de dar mayores garantías del contenido para quién lo abra, pero sin controles específico para quién lo distribuye y entrega. (servicio de correo/cartero)

En el correo electrónico, con sólo el protocolo inicial SMTP no se brindaba ninguna medida de seguridad para asegurar que los datos del remitente fueran reales. Pero como en sus inicios era usado de forma muy reducida en ámbitos académicos y de investigación, el riesgo era acotado y no era utilizado como mecanismo de comunicación para mensajes sensibles.

1.5 La irrupción del SPAM

El primer ataque o utilización no planeada ni deseada del correo electrónico fue el SPAM. El correo físico no solicitado siempre existió, pero se hizo más masivo a fines a partir de los años '70 aproximadamente con la reducción en el costo de impresión y envío de correo. El objetivo principal son las campañas de publicidad dirigidas a un grupo de potenciales clientes, generalmente con el objetivo de promocionar algún producto/servicio.

Con el correo electrónico las campañas de spam comenzaron a tener básicamente un costo cero, con lo cual resultaron más redituables que nunca. A fines de los '90, antes del la implementación de filtros específicos, el spam ya representaba un enorme volumen de tráfico de correos, y las listas de direcciones de correo electrónico comenzaron a tener valor monetario.

Si bien el spam correspondía mayormente a material promocional, comenzó a verse cada vez más como herramienta para distribuir contenido malicioso. Aprovechando su debilidad de no verificación de remitente, que resultaba en un virtual anonimato de origen, resultó ser el método ideal para la distribución de diferentes tipos de ataques de Phishing y Malware/Virus.

El SPAM comenzó a ser mitigado de forma más eficiente con la evolución de las funciones más avanzadas de los Gateway de correo, como los filtros de reputación y análisis del emisor. Pero para lograr mejores resultados debe poder garantizase el origen del correo electrónico, aspecto donde SMTP tiene debilidades intrínsecas de diseño.

1.6 La suplantación del origen

Como se explicó, el correo electrónico no fue diseñado originalmente con conceptos de seguridad básicos en mente, por lo que la suplantación (Spoofing), solo requería introducir datos falsos en el remitente.

Cuando se envía un correo electrónico por SMTP, la conexión inicial proporciona dos datos de dirección que se denominan direcciones de sobre ("envelope"), una analogía con un sobre de papel tradicional:

- MAIL FROM: - generalmente se presenta al destinatario como el encabezado "Return-path": normalmente no es visible para el usuario y, por defecto, no se realizan verificación de si el sistema está autorizado para enviar en nombre de esa dirección.

- RCPT TO: especifica a qué dirección de correo electrónico se entrega el correo electrónico; normalmente tampoco es visible para el usuario final.

Luego de estos 2 datos del sobre ("envelope") el sistema emisor usa el comando "DATA" y envía varios elementos de encabezado incluidos como parte del cuerpo:

- "From": la dirección es visible para el usuario destinatario, pero nuevamente, de forma predeterminada no se realizan comprobaciones de que el sistema de envío esté autorizado a enviar con ese nombre.
- "Reply-to": generalmente no visible al usuario al menos hasta que se responde el correo con la función estándar del cliente.
- "Sender": generalmente campo interpretado por el cliente de correo, similar en uso al "From", pero permite usos específicos para funciones avanzadas como el "Behalf of" (en nombre de).

Como vemos hacer Spoofing en SMTP es directo y sencillo. Pero hay otros datos indirectos que se suman durante la comunicación TCP/IP, como la dirección IP de la computadora que envía el correo. Este simple dato será el pie para construir un nuevo protocolo para comenzar a brindar una capa de seguridad a SMTP.

1.7 El uso de SMTP con capa SSL

La primera mejora que se pudo aplicar para brindar mayor seguridad a la implementación de SMTP, sin afectar el protocolo, es hacer uso de un canal seguro SSL (Secure Sockets Layer). El puerto estándar TCP 25 de SMTP se cambió al TCP 587 para el llamado "SMTP Secure" o SMTPS.

Estableciendo la comunicación TCP/IP con SSL, la comunicación está ahora cifrada y asegura la confidencialidad de forma confiable. Pero

esto no modifica las debilidades que permiten la suplantación de identidad que facilitan el Spam y el Phishing.

Es importante aclarar que al día de hoy no todas los servidores de correo se comunican mediante canales SSL, dejando librado al receptor aceptar, o no, el inicio de comunicaciones sin cifrado. Similar a los que ocurre con las páginas Web.

1.8 La introducción de Sender Policy Framework (SPF)

Después de casi 6 años pruebas de concepto y desarrollo, recién en el año 2006 el protocolo Sender Policy Framework (SPF) se publicó como RFC4408 experimental. En abril de 2014, el IETF incluyó a SPF en el RFC7208 como un "estándar propuesto".

SPF permite al dueño de un dominio de Internet publicar cuales direcciones IP están autorizadas para enviar un correo electrónico a su nombre, utilizando los ya existentes registros del Sistema de nombres de dominio (DNS) en un registro MX (Mail Exchanger record). Los receptores que verifiquen la información SPF ahora pueden rechazar mensajes de orígenes no autorizados antes de recibir el cuerpo del correo. Si el servidor acepta el dominio y posteriormente también acepta los destinatarios y el cuerpo del mensaje, debe insertar un campo "Return-Path" en el encabezado del mensaje para guardar la dirección de origen del sobre.

Ejemplo de un registro MX con SFP:

spf:afip.gob.ar

```
v=spf1 ip4:200.1.116.0/24 -all
```

Prefix	Type	Value	PrefixDesc
	v	spf1	
+	ip4	200.1.116.0/24	Pass
-	all		Fail

Resultado consulta SPF usando mxtoolbox.com para "afip.gob.ar"

Aquí podemos ver que la AFIP autorizó a que los correos que se reciban desde Internet con origen "@afip.gob.ar", sólo deben venir del rango IP 200.1.116.0/24. Si la dirección IP no coincide con el rango, en un contexto de control adecuado, el correo debe marcarse como "SPF FAIL".

Ejemplo de un registro SPF indicando otros nombres de dominio habilitados:

spf:bcra.gob.ar

```
v=spf1 include:mxsspf.sendpulse.com a mx ip4:45.235.96.5 include:spf.protection.outlook.com include:spf.myperfit.com -all
```

Prefix	Type	Value	PrefixDesc
	v	spf1	
+	include	mxsspf.sendpulse.com	Pass
+	a		Pass
+	mx		Pass
+	ip4	45.235.96.5	Pass
+	include	spf.protection.outlook.com	Pass
+	include	spf.myperfit.com	Pass
-	all		Fail

Resultado consulta SPF usando mxtoolbox.com para "bcra.gob.ar"

En este ejemplo del dominio de correo del BCRA, se habilita no sólo rangos de IPs, sino también los dominios outlook.com, sendpulse.com y myperfit.com. El hecho que se hayan registrado otros nombres de dominio nombres de dominio lanzará nuevamente consultas recursivas DNS/SPF hasta completar la relación con las IP habilitadas. El ser muy permisivo y habilitar a muchos terceros en un registro SPF, tiene su impacto en seguridad al aumentar el perímetro de exposición.

Un problema que surge con la aplicación de SPF, es que como sólo se puede verificar la IP que se comunica con el destino final, no se permite el reenvío ("forwarding") entre dominios. Escenario que suele ocurrir en entornos con retrasmisión ("relay") de correos, es decir en los que un servidor sólo actúa de agente de distribución de emails de terceros. Una práctica usada por varios motivos pero que siempre atentó contra la seguridad general, y que cada vez se utiliza menos.

1.9 El protocolo DomainKeys Identified Mail (DKIM)

En el año 2007 con la publicación de la RFC4870, y más tarde con la elaboración de la RFC6376 del año 2011, se agregó como estándar para Internet el protocolo DomainKeys Identified Mail (DKIM) para complementar la seguridad de los protocolos SMTP y SFP, utilizando infraestructura de clave pública (o "PKI").

DKIM permite al receptor verificar que un correo electrónico que afirma originarse en un dominio haya sido autorizado por el dueño de ese dominio al sumar una firma digital a cada correo saliente. El sistema destinatario lo verifica buscando la clave pública del remitente.

Con un control de integridad, la firma garantiza que el encabezado del correo electrónico tiene el origen que indica y no haya sido modificado. Las firmas DKIM no son visibles para los usuarios finales, sólo sirven a los efectos de la verificación que se realiza internamente en la infraestructura de correo electrónico.

Para admitir múltiples claves públicas simultáneas por dominio, el espacio de nombres clave se subdivide mediante "selectores".

selector = sub-domain *("." sub-domain)

El número de selectores correspondientes para cada dominio lo determina el propietario del dominio. Pueden usar un solo selector, o pueden optar por administrar varios selectores y pares de claves distintos en diferentes servidores de correo.

Ejemplo de una firma DKIM de un correo emitido por eventbrite.com:

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=event.eventbrite.com; s=scph0420; t=1708552236; i=@event.eventbrite.com; bh=4flu4cjAoTiigjNl1rEf58an9ZlK3Qul8i7p3PEa+kY=; h=Content-

Type:Subject:From:To:Date:Message-ID:From:To:Cc:Subject;
b=tG8f2Q+GNCSYW6TXqN0qmO8r4u/t/Qyx+jw5smBAEbae6n...

En este ejemplo podemos ver los datos más relevantes de la estructura de datos:

"v" versión.

"a": Algoritmo de firma.

"d" Identificador de dominio de firma (SDID).

"i" Identificador de Agente o Usuario (AUID).

"s" Selector.

"t" Marca de tiempo de firma (o timestamp).

"h" Campos del encabezado que han sido firmados.

"bh" hash del cuerpo (o body hash).

"b" firma de encabezado.

Ejemplo del registro DKIM, publicado para el dominio emisor "event.eventbrite.com", selector "scph0420":

dkim:event.eventbrite.com:scph0420

```
v=DKIM1; k=rsa; h=sha256; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNAD
```

Tag	TagValue
v	DKIM1
k	rsa (Length: 1024 bits)
h	sha256
p	MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC9S1d1JYD8/C ZxvOqmvyXsRQ89OG22tYiv5RysvWUMNCWR4RxzT2qJcQIDAQAB

Resultado consulta DKIM usando mxtoolbox.com para "event.eventbrite.com"

Siendo cada valor:

Tag	Nombre	Descripción
v	Versión	Identifica el registro recuperado como un registro DKIM. Debe ser la primera etiqueta del registro.
k	Tipo de Clave	El tipo de clave utilizada por la etiqueta (p).
h	Algoritmo de Hash	Una lista separada por dos puntos de algoritmos hash que podrían usarse.
p	Clave Pública	La sintaxis y la semántica de este valor de etiqueta antes de codificarse en base64 están definidas por la etiqueta (k).

2 Un protocolo para gobernarlos a todos

2.1 El nacimiento del protocolo DMARC

Con una adecuada implementación de los protocolos SFP (para autenticación de servidor origen) y DKIM (para control de integridad y verificación de encabezado), usando un canal SSL (cifrado punta a punta), el correo electrónico tiene todos los aspectos de seguridad necesarios para una comunicación de alta seguridad.

El problema es que el correo electrónico adquirió todas estas capas de seguridad mucho después de que fuera ampliamente utilizado. Y en todos los casos estos nuevos protocolos se montaron sobre el protocolo SMTP existente, siempre como características optativas, y como todo lo que ocurre en Internet, cada organización es libre de adoptar a su gusto.

Años después de la publicación, ya como estándares oficiales, SPF y DKIM seguían sin ser prácticamente utilizados. Para este momento los ataques de Spoofing, Phishing, Spam y BEC eran un dolor de cabeza para toda la comunidad de Internet, y comenzaban a generar severas pérdidas económicas.

El problema es que la implementación de SPF y DKIM no es resulta tan sencilla, y sólo agrega seguridad cuando tanto el emisor como el receptor la cumplen y tienen una estricta política de aceptación/rechazo de correos verificados/no verificados.

En el año 2015 la Internet Engineering Task Force's (IETF), ideó un plan para que SPF y DKIM, finalmente fueran adoptados por la comunidad de forma paulatina. Se creó un tercer protocolo de seguridad de correo electrónico llamado: Autenticación de Mensajes Basada en Dominios, Informes y Conformidad (Domain-based Message Authentication, Reporting and Conformance, o "DMARC").

DMARC no agregaba ni más cifrado, ni autenticación, ni más seguridad. Todo esto ya había sido resuelto. Su objetivo era mucho más puntual: lograr que todas las organizaciones pudieron implementar SPF y DKIM de forma paulatina, sin perder en ningún momento conectividad con otros dominios y usando el mecanismo más seguro que cada uno dispone hasta llegar al nivel de seguridad más elevado mediante niveles de adopción.

2.2 Lógica y funcionamiento del protocolo DMARC

DMARC tiene 2 funciones básicas, por un lado tiene que ver con la publicación por parte de cada dominio de su política de seguridad en cuanto a los correos que emite, y la segunda función está asociada a la publicación de direcciones para un sistema automático de notificaciones para controlar que los receptores están recibiendo los correos correctamente, sin fallas en los controles de seguridad y alertar de posibles intentos de spoofing.

Con DMARC una nueva entrada en el registro DNS/MX se agrega a las anteriores. El dominio emisor debe definir y publicar en qué estado se encuentra básicamente en cuanto a su nivel de implementación de SFP y DKIM.

Cada administrador de dominio de correo debe elegir entre 3 políticas posibles que reflejan el estado actual en cuanto a su nivel de seguridad de correo electrónico:

- "None" (Ninguno): es la política de nivel de entrada. Los receptores saben que el emisor no es seguro por lo que no deben rechazar los emails sin seguridad, pero permite que un dominio reciba informes de monitoreo de las recepciones.
- "Quarantine" (Cuarentena): pide a los receptores que traten con sospecha los mensajes que no pasan la verificación de seguridad. Los diferentes receptores tienen diferentes medios para implementar esto, por ejemplo marcar mensajes con algún "tag" o entregarlos , por ejemplo, en una carpeta especial.
- "Reject (Rechazar): pide a los receptores que rechacen por completo los mensajes que no superen la verificación DMARC (SPF y DKIM).

Estas 3 políticas están asociada al grado de avance en la implementación DMARC. Con la política "None" los terceros sabrán que el dominio tiene intención de avanzar para mejorar su seguridad (porque al menos tiene publicado un registro DMARC), pero que aún no avanzó en

verificar que sus registros SPF sean correctos, ni que todos sus mails salgan firmados con DKIM. Por lo que se comunica que el nivel de seguridad del dominio emisor es bajo.

Cuando se publica una política "Quarantine", lo que se está trasmitiendo a todos los receptores es que si bien la mayor parte de los correos del dominio estarían cumpliendo con los estándares de seguridad no hay garantías de que todavía algunos mails no tengan origen en servidores debidamente registrados o estén firmados digitalmente. Por lo que se pide no descartar los mensajes que no pasen la verificación SPF o DKIM, sino marcarlos o identificarlos como sospechosos, pero dejar que el administrador o usuario lo revise manualmente de forma individual.

Finalmente la política "Reject", que es el objetivo final de una implementación DMARC, y la única política que brinda alta seguridad. Con esta configuración se le comunica a todos los receptores en Internet que el dominio emisor garantiza que todos los correos que salen con su nombre están cumpliendo con los orígenes designados en el registro SPF, y que todos sus correos están siendo firmados digitalmente con DKIM. Por lo que cualquier correo que no pase los chequeos de seguridad se trata de un intento de suplantación, debe ser rechazados, y se debe informar automáticamente al dominio que intentan impostar para que toma las medidas pertinentes.

Para poder ir monitoreando el avance desde una política insegura "None" hasta llegar a una de alta seguridad "Reject", DMARC ofrece un sistemas de notificaciones para estar al tanto de si los correos están pasando los controles del tercero correctamente, o si está fallando algunos de los controles SFP o DKIM.

Existe 2 tipos de reportes:

- RUA (reportes agregados o de resumen): se envían como archivos XML, normalmente una vez al día. El asunto menciona el "Dominio del informe", que indica el nombre de dominio DNS sobre el cual se generó el informe.

Contiene un resumen del total de las recepciones con ese dominio, con el resultado de las verificaciones de seguridad.

- RUF(reporte forense): Los informes forenses, también conocidos como informes de fallas, se generan en tiempo real y consisten en copias redactadas de mensajes individuales que fallaron SPF o DKIM. Permiten analizar individualmente cada caso. Especialmente útiles para analizar posible casos de suplantación por parte de un tercero.

Ejemplo de cómo se ve un registro DMARC, dominio "ypf.com":

dmarc:ypf.com

```
v=DMARC1; p=reject; rua=mailto:dmarc@ypf.com; ruf=mailto:dmarc-forensic@ypf.com; rf=afrf; sp=reject; fo=1
```

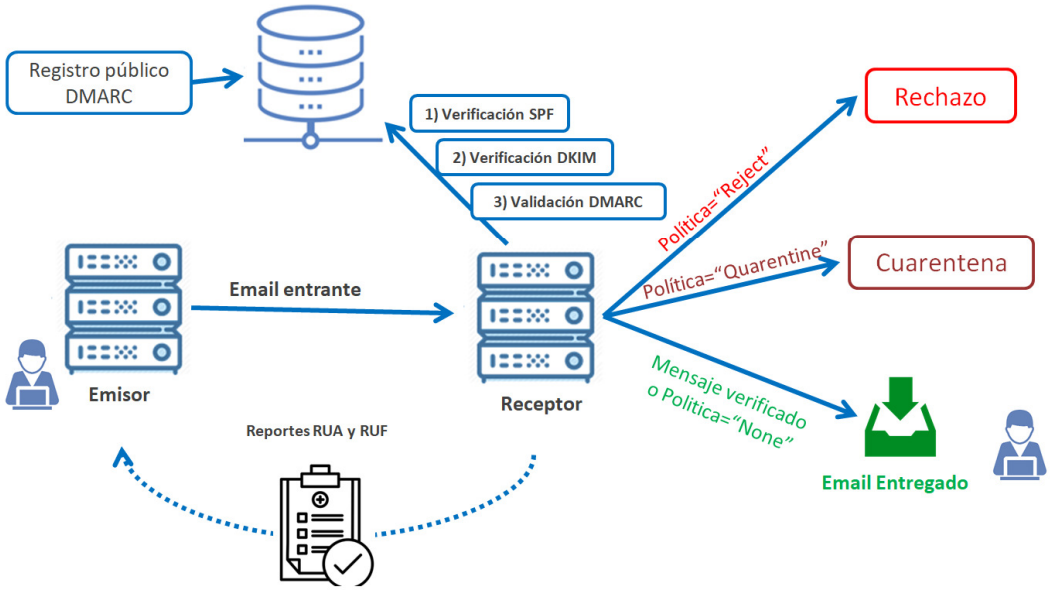
Resultado consulta DMARC usando mxtoolbox.com para "ypf.com"

Siendo cada valor:

Tag	TagValue	Name	Description
v	DMARC1	Versión	Identifica el registro recuperado como un registro DMARC. Debe ser la primera etiqueta de la lista.
p	reject	Política	Política que se aplicará al correo electrónico que no pase la prueba DMARC. Los valores válidos pueden ser "ninguno", "cuarentena" o "rechazado".
rua	mailto:dmarc@ypf.com	Receptores	Direcciones a las que se enviarán reportes agregados(RUA). Lista de texto sin formato separada por comas de URI DMARC.
ruf	mailto:dmarc-forensic@ypf.com	Receptores forenses	Direcciones a las que se debe reportar información de error específica o forense del mensaje(RUF). Lista de texto sin formato separada por comas de URI DMARC.
rf	afrf	Formato forense	Formato que se utilizará para informes de errores específicos de mensajes. Los valores válidos son 'afrf' y 'iodef'.
sp	reject	Política de subdominio	Política de receptor de correo solicitada para todos los subdominios. Los valores válidos pueden ser "ninguno", "cuarentena" o "rechazado".
fo	1	Informes forenses	Proporciona opciones solicitadas para la generación de informes de fallas. Los valores válidos son cualquier combinación de caracteres '01ds' separados por ':'.

En el siguiente gráfico se resumen conceptualmente el funcionamiento de DMARC:

Diagrama funcionamiento de DMARC



En resumen, cuando un servicio receptor recibe un correo que afirma ser de un dominio, lo primero que se hace es descargar los registros públicos para ver: Registros SPF, Registros DKIM y Registros DMARC.

Con la verificación SPF, se compara el direccionamiento origen con la IP del servidor que le está hablando. Si el origen es válido ese mail que identificado con "SPF Pass".

Luego se consulta el registro DKIM, y se realiza la descarga de la clave pública correspondiente al "selector" indicado en ese mail en particular. Si la clave publica descifra correctamente el encabezado, este correo se identifica como "DKIM Pass".

Finalmente se consulta el registro DMARC, estos determinaran el comportamiento que el receptor debería seguir en caso de que alguna de las verificaciones de seguridad anteriores no haya sigo exitosa.

En caso de cualquier falla de validación SPF o DKIM, el receptor deberá cumplir con la política del emisor:

- Si la política del emisor es "Reject", el correo debe ser rechazado y descartado.
- Si la política es "Quarantine", el receptor deberá decidir que tratamiento le da a este correo sospechoso. Se recomienda enviarlo a un sistema de cuarentena para revisión manual por parte de un administrador o analista de sistemas.
- Si la política es "None", el correo debería ser entregado al usuario. El receptor es libre de por ejemplo identificar el correo con algún "tag" para advertir que el correo no tiene medidas de seguridad suficientes como para determinar su autenticidad. O podría simplemente enviarlo directamente al usuario sin advertirle. (lamentablemente esto es lo que suele hacerse)

2.3 Reportes y monitoreo continuo

Para ir evolucionando desde una política de baja seguridad a la más alta son necesarios los reportes de DMARC que los receptores envían resumiendo los controles de seguridad y su resultado, al emisor.

Los reportes RUA (reportes agregados), son un mail automático enviado a la casilla definida en el registro público, que tiene un archivo adjunto en formato .XML. En el adjunto se encuentra un resumen de todas las comunicaciones recibidas (de forma diaria por defecto), con el resultado de cada verificación de seguridad.

Con este reporte el emisor puede verificar que sus comunicaciones estén siendo aceptadas como seguras por los receptores. O sea

básicamente que esté pasando con éxito las verificaciones de seguridad SPF y DKIM.

A continuación se incluye un ejemplo ilustrativo de como se ve el contenido de un reporte RUA XML en formato de tabla:

org_name	email	report_id	domain	source_ip	count	dkim	spf	selector	result
Chase	dmarchelp@chase.com	1670031640	ejemplo.com	139.138.32.122	2	pass	pass	ejemplo-onmicrosoft	pass
Chase	dmarchelp@chase.com	1670031640	ejemplo.com	139.138.32.122	2	pass	pass	cer1	pass
Chase	dmarchelp@chase.com	1670031640	ejemplo.com	62.149.155.133	1	pass	fail	a1	pass

En este ejemplo se observa que se recibieron 5 email agrupados en 3 líneas (ya que comparten criterios comunes). Se usaron 3 selectores distintos (repositorios de certificados), todos los chequeos DKIM fueron exitosos, pero 1 chequeo SPF falló. Finalmente en la última columna "result", el receptor dio por válido todos los mails. En este caso ilustrativo como la política DMARC del emisor estaba configurada en "none", se requería a los receptores que los mails fueran aprobados como auténticos aún si tenían alguna falla de validación de seguridad. Con una política de alta seguridad ("reject"), esté último mail debería haber sido rechazado, y no ser entregado al usuario.

Con el análisis de los reporte RUA de casos en los que la verificación tuvo fallas, un emisor puede ir paulatinamente corrigiendo los errores de origen. Para finalmente llegar a una política de alta seguridad ("reject").

Una vez que la seguridad del emisor es alta, comienzan a ser más útiles el segundo tipo de reporte disponible, el reporte forense "RUF". Estos reportes también conocidos como de fallas, se generan en base a copias de mensajes individuales que fallaron en SPF o DKIM.

Los reportes RUF son especialmente útiles para identificar intentos de suplantación por parte de terceros que hacen uso ilegítimo de un dominio que no les pertenece. Su uso forma una red de monitoreo, soportada en forma colaborativa por todos los receptores posibles en Internet, y mantienen al tanto al dueño real del dominio con la información útil para investigar o denunciar servidores, direcciones y dominios, que están intentado hacer Spoofing.

En un reporte RUF, entre otros datos, se incluye:

- IP de conexión del envío
- From (dirección de origen que afirma tener)
- To (Destinatarios)
- Asunto del correo electrónico
- Resultados de autenticación SPF y DKIM
- Fecha/hora recibida
- Encabezados de mensajes que incluyen el host de envío, el ID del mensaje de correo electrónico, la firma DKIM y otra de encabezado personalizada.

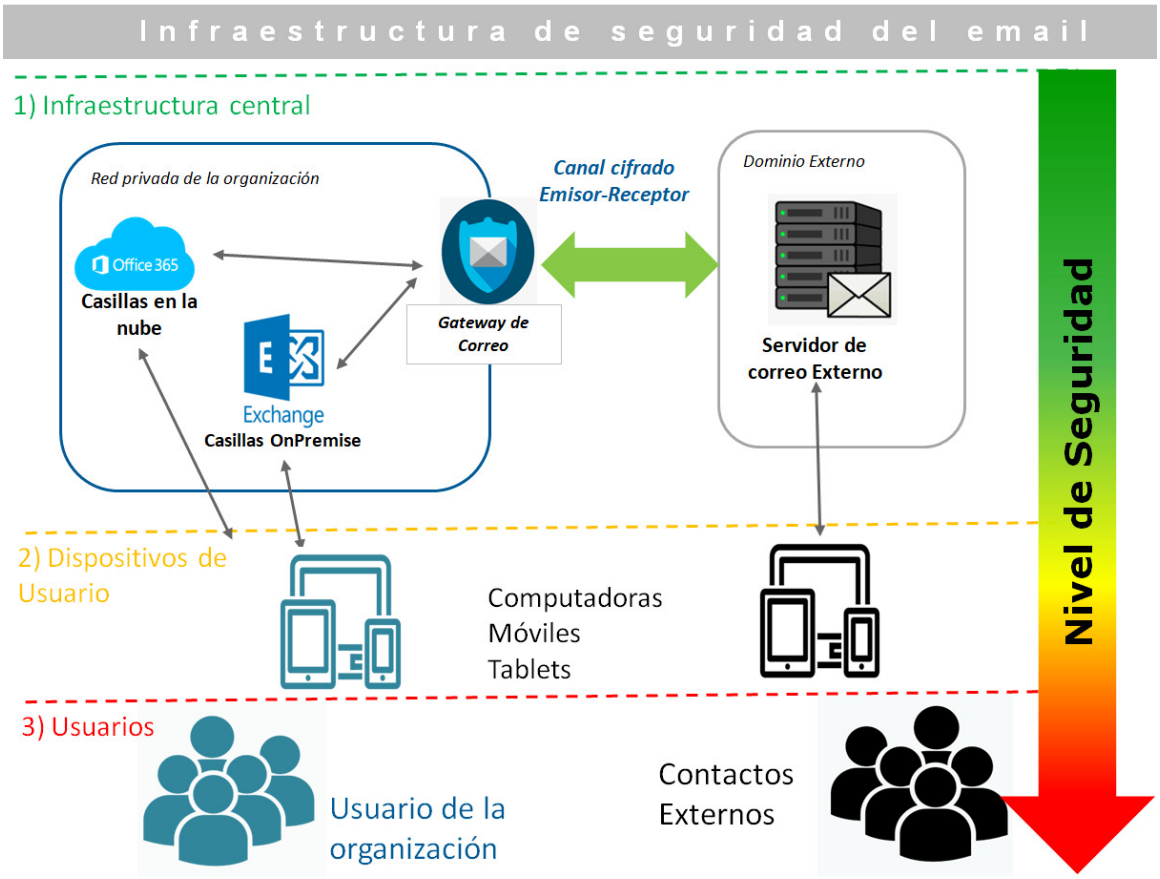
Con estos datos el verdadero propietario de un dominio podría iniciar denuncias de intento de suplantación en su nombre, canalizadas generalmente a través de los canales para informar abusos en el uso de dominios registrados, por medio de las casillas "abuse" de los registros que mantiene el Internet Corporation for Assigned Names and Numbers (ICANN)).

3 Capas en una Infraestructura de correo electrónico

En una infraestructura de correo electrónico moderna se relacionan una gran cantidad de elementos distintos, pero resumiendo los más relevantes son:

- Servidores de correo del emisor y receptor. (ya sea en Cloud/On Premise)
- Gateway de correo. (enrutador con funciones avanzadas específicas en el perímetro de la red)
- Dispositivos de usuario (que tienen las aplicaciones de cliente de correo)
- Los usuarios (las personas y el factor humano)

En el siguiente gráfico se muestra la relación típica entre estos elementos que conforman una infraestructura de correo, y el nivel de seguridad que generalmente hayamos desde: 1) la infraestructura central (más controlada), 2) pasando por los dispositivos de usuario (más difícil de controlar), 3) llegando hasta los usuarios (los más vulnerables):



Como vemos podemos distinguir 3 capas generales de seguridad. Desde los dispositivos centrales de comunicación (servidores, gateway, red) que tiene un gobierno más rígido y controles elevados, luego los dispositivos de usuarios (PC, laptops, móviles, etc) cuyos parques se intentan mantener actualizados y medianamente controlados con diversos controles de efectividad irregular. Finalmente las personas que acceden a estos dispositivos, capa más vulnerable y que requiere de un permanente programa de capacitación y concientización que es difícil de mantener en un nivel de entrenamiento alto.

3.1 Seguridad de la Infraestructura central

Si bien decimos que en general la seguridad en la infraestructura central de correo electrónico en las organizaciones suele ser el eslabón más robusto de la comunicación, también es importante aclarar que una debilidad en este nivel sería critico y que podría afectar todas las comunicaciones o cuentas en su conjunto.

Los servidores de correo, servicios en la nube, gateway de correo, etc, tienen complejas configuraciones que deben mantenerse adecuadamente gestionadas siguiendo las mejoras prácticas para cada tecnología. La aplicación constante de parches y actualizaciones es esencial para los sistemas OnPremise administrados. Múltiples vulnerabilidades se reportan y corrigen en los sistemas de correo más utilizados de todos los proveedores de tecnología.

A los efectos de este trabajo no profundizaremos en este tipo de vulnerabilidades en servidores ya que no son el recurso más usado por los atacantes, que se enfocan principalmente en las capas más débiles: Dispositivos y Usuarios. Si analizaremos las políticas del protocolo DMARC que se están aplicando a nivel infraestructura, que nos darán una visión general de cuál es su postura/nivel de seguridad.

4 Ataques clásicos al correo electrónico

Existen muchos tipos de técnicas de uso malicioso del correo electrónico, y lo cierto que se suelen ver combinadas al mismo tiempo en la mayoría de los ataques. Pero se tuviéramos que identificar los 4 tipos generales más comunes serían:

- Spoofing: Es el ataque de suplantación de identidad. Podríamos decir hay 2 tipos generales:
    1. Suplantación original: correos electrónicos que dicen ser de un dominio pero que provienen de otra dirección. Si logran eludir los controles de seguridad técnicos, se ven exactamente como un correo electrónico auténtico. (no puede ser identificado por el usuario)
    2. Correos electrónicos con un nombre de dominio de origen que se parece al real, pero que se escribe ligeramente diferente. (engañan al usuario con nombres similares confusos)

- Phishing: El objetivo es engañar la víctima para que ingrese a un link fraudulento, instale malware en su equipo u obtener información valiosa aportada por el usuario. Generalmente es combinada con una técnica de Spoofing.

- Spam: Es el correo electrónico no solicitado. En la mayoría de los casos el spam es sólo publicidad, pero que reduce la eficiencia del medio de comunicación. Sin embargo, también se utiliza como método de distribución de ataques de virus/malware y phishing. La mayor parte del spam proviene de servicios de distribución de publicidad, pero también puede provenir de equipos infectados por un virus o malware. Estos equipos comprometidas con malware suelen también provocar la saturación de casillas, lo que produce una denegación del servicio de correo a estos usuarios.

- BEC: El compromiso de las correos corporativas (Business Email Compromise, BEC), es uno de los más sofisticados y que mayor daño produce en pérdidas económicas. Se basa en la obtención de cadenas de correos y contactos privados, para con esta información hacer diversos fraudes, con foco en el desvío de transferencias de pago electrónicas.

El ataque de tipo BEC (Business Email Compromise), supone la combinación de diversas técnicas y metodologías, para lograr hacerse de correos entre privados. Algunos separan la variante en la que el compromiso es de la totalidad de la cuenta del usuario, abreviada EAC ("Email Account Compromise"), pero generalmente se considera a BEC/EAC como un mismo grupo.

5 El ataque tipo BEC

5.1 Impacto económico de los ataques

Los ataques a los sistemas de correos electrónicos relacionados a tipos BEC, están teniendo un crecimiento sostenido en los últimos años convirtiéndose en uno de los que mayores pérdidas monetarias produce. Al no existir una organización mundial oficial que pueda estimar dichos daños, para entender la dimensión del problema, lo más confiable es remitirnos a los pérdidas que pudo confirmar el Centro de Crimen en Internet (IC3 - Internet Crime Complaint Center) del FBI de Estados Unidos.

Dentro de todos los tipo de ataques y crímenes realizados vía Internet, según el último reporte disponible del año pasado, se encuentra segundo en total de pérdidas reportadas por BEC con la suma de más de 2700 millones de dólares sólo durante el año 2022.

By Victim Loss			
Crime Type	*Loss*	*Crime Type*	*Loss*
Investment	$3,311,742,206	Lottery/Sweepstakes/Inheritance	$83,602,376
BEC	$2,742,354,049	SIM Swap	$72,652,571
Tech Support	$806,551,993	Extortion	$54,335,128
Personal Data Breach	$742,438,136	Employment	$52,204,269
Confidence/Romance	$735,882,192	Phishing	$52,089,159
Data Breach	$459,321,859	Overpayment	$38,335,772
Real Estate	$396,932,821	Ransomware	*$34,353,237
Non-Payment/Non-Delivery	$281,770,073	Botnet	$17,099,378
Credit Card/Check Fraud	$264,148,905	Malware	$9,326,482
Government Impersonation	$240,553,091	Harassment/Stalking	$5,621,402
Identity Theft	$189,205,793	Threats of Violence	$4,972,099
Other	$117,686,789	IPR/Copyright/Counterfeit	$4,591,177
Spoofing	$107,926,252	Crimes Against Children	$577,464
Advanced Fee	$104,325,444		

Reporte FBI IC3 2023 - perdidas confirmadas por tipo en el año 2022. (*)Según el informe las pérdidas por Ransonmware puede estar subestimadas por la ausencia de denuncia de rescates efectivamente pagados.

5.2 Vectores de ataques BEC

El ataque de compromiso de correos corporativo (BEC), requiere que el atacante logre hacerse de comunicaciones privadas, que deberían estar aseguradas. Como mencionamos anteriormente, si se utiliza para el correo un canal SSL, el cifrado debería estar asegurado y sería imposible la intercepción de correos electrónico durante su transmisión por Internet.

Como los atacantes no puede generalmente penetrar la infraestructura central de correo (servidor y canales de comunicación), lo que hacen es enfocarse en las capas más débiles: los dispositivos de usuarios y las personas. Con los objetivos de comprometer las credenciales de los usuarios a sus casillas personales, o también de comprometer la seguridad de los dispositivos que utilizan para acceder a su cliente de correo. Se puede resumir los tipo de ataques en:

Ataques con el objetivo de comprometer las credenciales del usuario y obtener acceso a la cuenta de correo electrónico:

- Ingeniería social
- Phishing (enlaces de autenticación falsos)

Ataques con el objetivo de comprometer el dispositivo del usuario (Windows, Mac, Android, iOS, etc.) y acceder a los correos electrónicos de los usuarios en el dispositivo mediante un virus:

- Spyware (monitoreo/duplicación remota de comunicaciones)
- Malware (acceso remoto a la terminal)

En los ataques de compromiso de dispositivo el objetivo muchas veces son las bases de datos donde los correos se almacenan cuando son descargados desde el servidor de correo hacia el cliente local. En el ámbito corporativo el blanco típico son los archivos ".OST" y ".PST", para sistemas basado en Microsoft Exchange/Outlook.

5.3 Metodología del ataque BEC

Si bien puede existir múltiples objetivos en este tipo de ataques, el principal blanco que suelen apuntar son las comunicaciones en las que existe un reclamo de un cobro por un servicio o producto ya entregado.

Como ejemplo ilustrativo, la conversación que suele verse en un típico ataque BEC de desvío de transferencia es así:

Durante el intercambio de comunicaciones un atacante que está monitoreando alguna de las casillas, intercepta la conversación en la que hay un reclamo de una cuenta por cobrar.

El atacante toma la conversación y la continúa haciendo un ataque de Spoofing, en este caso de ejemplo desde una dirección similar para confundir al usuario.

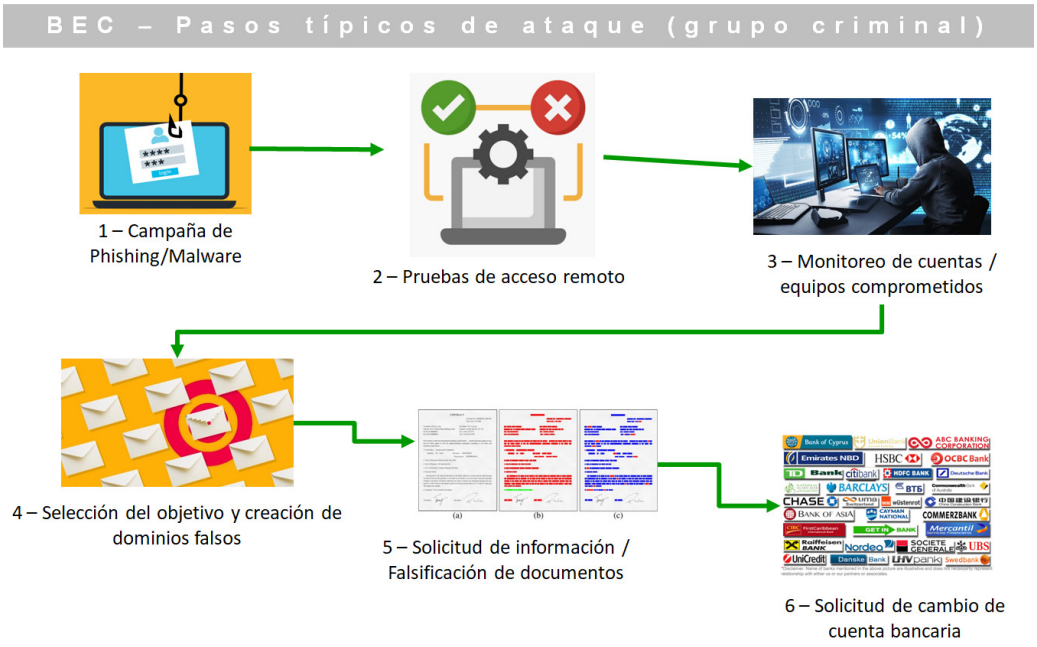
La intención del atacante es en muchos casos que la victima responda a sus correos con el objetivo de obtener más información, y para establecer una cadena de comunicación continua que superponga al interlocutor original. Esto lo deben hacer de la forma subrepticia para no hacer evidente que hay dos contactos en simultáneo.

Estos tipo de desvío de fondos son tan redituables que actualmente grandes grupos criminales organizados se dedican a estas estafas. Aunque es imposible saber exactamente como operan estas bandas, podemos suponer que utilizan una metodología bastante estándar que siguen más o menos los siguientes 6 pasos:

1. Crean una campaña masiva de phishing para distribuir un enlace de robo de credenciales o un malware diseñado para monitorear las actividades de correo electrónico en los dispositivos de los usuarios.

2. Los atacantes prueban los accesos obtenidos para cada cuenta comprometida.
3. Centralizan y monitorean la actividad de todos los usuarios afectados (probablemente miles), buscando correos electrónicos con palabras clave como “pago”, “transferencia”, “factura”, etc.
4. Después de identificar a una víctima potencial, crean un dominio falso para iniciar una suplantación de identidad y desviar la comunicación con el atacante. O directamente utilizan las credenciales robadas.
5. Escriben a la víctima para recabar información (facturas, importes, etc). En algunos casos también se inicia una comunicación con el tercero (proveedor/cliente). Falsifican documentos como: facturas (si incluyen información bancaria), certificados bancarios, cheques, otros correos electrónicos, etc.
6. En algún momento, envían información sobre una nueva cuenta bancaria para desviar los pagos.

En resumen el circuito suele tener esta secuencia:



Se sospecha que estos grandes grupos utilizan herramientas de analíticas para hacer el monitoreo de todas las cuentas/equipos comprometidos. Muy posiblemente con alertas automatizadas para la búsqueda de palabras clave para ser analizadas luego manualmente por un operador humano.

5.4 El arte del “Typosquatting”

Anteriormente se mencionó que el ataque de Spoofing puede realizarse falsificando el origen del correo, o bien engañando al usuario con un nombre de dominio similar al real pero alterado. Con este objetivo los atacantes utilizan técnicas de denominadas de "Typosquatting" (o error tipográfico). Estas técnicas están basadas en la forma que el cerebro interpreta un texto cuando se le presta poca atención a la lectura.

Técnicas clásicas de "Typosquatting"

Los atacantes que hacen uso de técnicas combinadas durante un ataque BEC, muchas veces intentan desviar las comunicaciones hacia un dominio falso, para poder seguir la conversación, evitando tener que suplantar o seguir interceptando comunicaciones contra el domino real, lo que podría despertar en algún momento sospechas en las víctimas.

5.5 Como investigar un ataque de BEC

En el caso que una organización sea víctima de un ataque BEC, en algún momento posterior a efectuar el pago a la cuenta del atacante, generalmente alguna de la partes (cliente, proveedor, u otro afectado) finalmente identifica que alguna de sus comunicaciones fue de alguna forma comprometida por un tercero y toma conciencia de que se ha caído en una estafa.

Cuando esto ocurre se debe lanzar una rápida investigación interna en la organización con los objetivos de corto plazo de:

- Identificar y evitar futuras comunicaciones con cualquiera de los atacantes.
- Comprender si el ataque tuvo éxito y cuantificar las pérdidas.
- Determinar si alguna cuenta o computadora de la organización puede estar comprometida.
- Investigar la posibilidad de un fraude interno.
- Identificar qué usuario de la cadena de correos electrónicos fue el más probablemente comprometido.

Para entender como realmente fue la maniobra, se requiere de una investigación con el objetivo de establecer claramente lo ocurrido. Los pasos que podrían seguirse para comenzar una investigación interna podrían ser los siguientes:

- Obtener la mayor cantidad posible de mails de las cadenas, intercambiados entre la organización y el cliente/proveedor.
- Entrevista con las personas involucradas.

- Verificación de permisos de los usuarios, a fin de entender que accesos remotos utilizaban, y si tenían dispositivos móviles asignados.
- Analizar el encabezado de los mails a fin de entender cómo fue la secuencia, y poder distinguir indicios de Spoofing.
- Revisar permisos de casillas de correo de los usuarios involucrados.
- Analizar la meta data en archivos presumiblemente falsificados por el atacante. (generalmente se falsifican datos de pago dentro de las facturas)
- Análisis de dominios de correos fraudulentos. (si lo hubiera)
- Analizar el log de Internet de usuarios de la organización involucrados en busca indicios de tráfico de Spyware.
- Realizar las denuncias a los dominios fraudulentos que fueron usados para realizar los ataques.
- Analizar seguridad de dispositivos de usuario como : Computadoras, Laptops, Móviles, etc.. Revisión de status de Antivirus en dispositivos.

5.6 Análisis de encabezados de correos electrónicos

Se llama encabezado (o "header") de un correo electrónico a una estructura almacenada en texto en la que se almacenan tanto los datos básico de direccionamiento como también meta datos que se registran durante las diferentes etapas de transmisión del correo desde su origen hasta llegar al destino final.

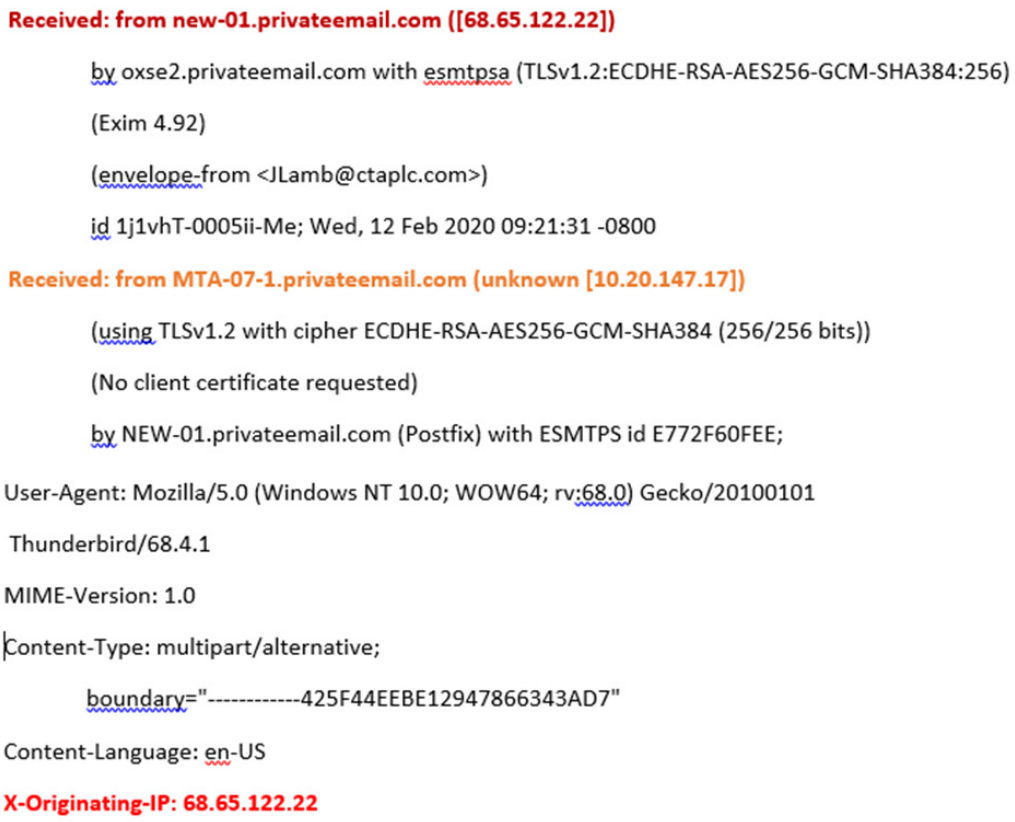
Los encabezados no son todos iguales. La mayoría de los datos que se encuentran son optativos, y difieren del tipo y configuraciones de los equipos por los que el correo fue pasando: Servidores de correo, Relays, Gateways, protección de Antivirus, filtros anti Spam, etc. Existen datos comunes que nos encontraremos en la mayoría de los encabezados, pero hay otros datos específicos que solo se registran en casos muy particulares.

Datos básicos del encabezado visible del correo:

- From: el nombre y/o la dirección de correo electrónico del remitente.
- To: El nombre y/o dirección de correo electrónico del destinatario.
- Date: la fecha y hora en que se envía el correo electrónico.
- Subject: El asunto del correo electrónico.

Meta datos más comunes registrados durante la vida del correo:

- “Message-ID”: Código identificador del correo electrónico, normalmente único.
- “Received: from”: Cada nombre de servidor/IP por el que ha pasado el correo.
- “Reply-To”: Dirección que se completará automáticamente cuando el usuario responda.
- “Return-Path”: Dirección donde regresará el correo electrónico en caso de falla.
- MIME-Version: (MIME significa Extensiones de correo de Internet multipropósito) Es un estándar de Internet que amplía las capacidades de formato del correo electrónico. El encabezado indica la versión que el correo electrónico utiliza.



Ejemplo de un extracto encabezado de correo electrónico, coloreado los datos más relevantes.

Ejemplo de metadatos útiles que podemos llegar a encontrar dependiendo del contexto y capacidades de seguridad:

- Authentication-Results: aquí es donde se registran los resultados de autenticación para SPF (marco de políticas del remitente), DKIM (correo identificado con claves de dominio) y DMARC (autenticación, informes y conformidad de mensajes basados en dominio). Si todas fueron exitosas, cada uno recibirá un mensaje de resultado "pass".
- User-Agent: este campo indica el cliente de correo electrónico que utilizó el remitente del mensaje.
- X-Originating-IP: la dirección IP de origen de un cliente que se conecta a la interfaz HTTP de un servicio de correo.

- X-MS-Exchange*: Todo un grupo de meta datos específicos de servicios Microsoft Exchange, que pueden resultar de utilidad.
- X-Microsoft-Antispam: Contiene información adicional sobre correo masivo y phishing en entornos Microsoft.

Si bien existen herramientas que ayudan al análisis de los encabezados, debido a su naturaleza de ser todos distintos con contenido imprevisible, en una buena investigación se debe realizar de forma manual.

El análisis de los encabezados es más un arte que una metodología simplemente repetible. La complejidad con la que nos podemos encontrar es elevada, y es en los pequeños detalle en la que pueden obtenerse datos significativos en un investigación forense. Un buen investigador forense puede distinguir fácilmente un correo que utiliza técnicas de Spoofing, y con suerte puede establecer algún patrón de cliente/IP común que le permita presumir algún dato de identificación del atacante.

Algunos de los patrones que se buscan para identificar Spoofing y signos de posible origen del ataque son:

- Origen de dominio definido en "From", distinto a la primera entrada registrada en "Received: from".
- “Return-Path” diferente al dominio definido en "From".
- “Reply-To” a un dominio nuevo sin relación al origen.
- Patrón de generación de la cadena “Message-ID”, no coincidente con patrones comunes para el tipo de agente indicado en "User-Agent".
- "X-Originating-IP" con origen en países inusuales o de posibles salidas de VPN/TOR.

Estos son sólo algunos ejemplos, pero cada caso es único y se deben analizar artesanalmente. Lo cierto es que debido a estos patrones irrepetibles, un investigador forense puede distinguir rápidamente un correo electrónico que no perteneció a una cadena de comunicaciones normal. Lo

que resulta útil para rápidamente distinguir una falsificación ("forgery"), que intentó desviar una cadena existente.

6 Medidas de protección contra los ataques

Existen múltiples medidas que las organizaciones pueden tomar para reducir su nivel de exposición a ataques BEC.

Como se viene explicando es importante que primero se tenga una infraestructura tecnológica de correo robusta que cumpla las mejores prácticas anti-Spoofing con la implementación de SPF, DKIM y la política "Reject" de DMARC.

Como parte de la infraestructura también es recomendable la utilización de un Gateway de correo, que evite la exposición directa del servidor de correo, y que además provea funciones avanzadas de seguridad. Un Gateway de correo moderno puede incorporar funciones como :

- Filtro anti-Spam
- Filtro de reputación por dominio/IP
- Funciones anti-Virus
- Reglas de contenido y clasificación personalizables
- Módulo anti-Malware/AMP (funciones específicas más avanzadas que el anti-virus ("Advance Malware Protection") como Sandboxing e inspección de reputación por hash de archivos adjuntos)
- Funciones DLP (("Data Loss Prevention") prevención de fuga de datos en correos salientes)
- Monitoreo y filtros "Outbreak" (módulo de detección de eventos simultáneos que indique un "brote" de ataques con patrón común)

6.1 Medidas contra el robo de credenciales

A lo anterior debemos agregar medias especificas contra los vectores de ataque más utilizado para el robo de credenciales realizados mediante Ingeniería Social o Phishing (enlaces de autenticación falsos), mitigándolos con:

- ✓ Concientización ("Awareness")
  Campañas dirigidas específicamente contra los grupos más vulnerable como lo son el personal de cuentas de pagar/cobrar y los comerciales.

- ✓ Inspección de correo electrónico anti-Phishing (desde el gateway de correo)
  Se pueden detectar y eliminar o redirigir a un portal controlado los links dentro del cuerpo de cada mail, que lleven al sitio de un atacante.

- ✓ Navegación en Internet por medio de Proxy seguro
  Para evitar que el usuario caiga en links malicioso, o que malware se comunique a Internet de forma directa.

- ✓ Autenticación multifactor (MFA: "Multi Factor Authentication")
  Posiblemente la mayor y mejor protección contra el robo de credenciales, evitando el que atacante puede ingresar solamente por tener el nombre de usuario y la contraseña obtenida.

6.2 Medidas contra el compromiso de dispositivos

Medidas de protección contra el compromiso del dispositivo del usuario (Windows, Mac, Android, iOS, etc.) que accede a los correos electrónicos del usuario:

- ✓ Antivirus en el dispositivo ("EndPoint") instalado.
- ✓ Sistema operativo y aplicaciones actualizadas.
  Esto es particularmente difícil de mantener en equipos Móviles, debido a la rápida obsolescencia y al soporte irregular por parte de los fabricantes.
- ✓ Privilegios mínimos asignados al usuario en el sistema operativo a los usuarios finales.
  Con el objetivo de mantener una buena segmentación de los niveles de seguridad y evitar los escalamientos por parte de Malware.

6.3 Monitoreo de creación de dominios

Otra de las medidas que pueden tomar las organizaciones más grandes es la contratación de servicios de monitoreo de creación de dominios fraudulentos. Esto sirve para los casos de los ataques de Spoofing que utilizan dominios similares al impostado, pero escritos levemente diferente para confundir al usuario. Utilizando las técnicas mencionadas anteriormente de "Typosquatting".

Estos servicios de monitoreo están permanentemente rastreando la creación de nuevos dominios en Internet, cuyos nombres contengan patrones similares a la marca a proteger. En caso que se detecte un nuevo dominio que cumpla las condiciones de similitud establecidas, se alerta al administrador del dominio protegido para que tome acciones.

Lo que suele realizarse primero es la denuncia del dominio fraudulento por uso indebido de marca registrada(en caso que la similitud sea evidente). También se puede avanzar con solicitar la baja del dominio por posible abuso o uso malicioso contactando por correo o teléfono al contacto definido en el registro DNS y publicado en el campo "Abuse contact". La rápida baja del dominio impostor puede evitar que los atacantes inicien o continúen conversaciones con las victimas previniendo que se llegue a la instancia de un intento de desvío de pago.

6.4 Monitoreo de comunicaciones con terceros

Con el uso de los registros históricos (Logs) de comunicaciones de un gateway de correo (o de un tracking Log Exchange) es posible ver el intercambio de correos entre los usuarios corporativos y los dominios externos con los que se comunican.

Estos datos son altamente sensibles, pero con una adecuado marco de control, pueden ser utilizados para realizar analíticas con el objetivo específico de identificar posible desvío de comunicaciones con terceros hacia dominios fraudulentos. Esto es, identificar si los usuarios de la organización comienzan a tener intercambio de correos con dominios externos que parecen similares a clientes o proveedores reales, pero que se tratan de dominios fraudulentos creados para engañar a los usuarios.

Para estos se pueden utilizar diversas metodologías analíticas, las más básicas serian primero identificar dominios nuevos (que la organizaciones no solía dirigir correos) y ver si éstos tienen una similitud de nombre con dominios que históricamente suelen ser destinatarios. También se pueden buscar específicamente cadenas desviadas. Esto sería un hilo de conversaciones identificado por Asunto, Destinatarios y otros datos, que de repente comienzan a ser originados desde otro dominio inusual. Entre muchas otros patrones que podrían analizarse.

6.5 Uso de portales para proveedores y clientes

Uno de los aspectos que permiten que los ataques BEC con el objetivo de desvío de pagos tengan tanta efectividad es el uso del correo electrónico como medio para el intercambio de información crítica de pagos o de datos bancarios.

La información comercial y de pagos/cobros entre organizaciones debería ser intercambiada por otras vías como los portales web, o bien, para

el intercambio entre dos grandes organizaciones, los sistemas de integración conocidos como B2B ("Business to Business").

El uso de portales para proveedores o clientes, brinda un marco de control y de seguridad mucho mayor a las comunicaciones por correo electrónico. En estos portales se pueden agregar sistemas de autenticación robusta como el MFA (factor de autenticación múltiple), monitoreo de operaciones, control de IP de origen, circuitos de autorizaciones, entre muchos otros controles.

Los portales proveen un mecanismo seguro para que proveedores puedan hacer la actualización de datos bancarios según su necesidad sin tener que iniciar conversaciones que pueden ser capturadas. También los clientes pueden hacer descargas de facturas y visualizar pagos pendientes de realizar, sin tener que estar intercambiando correos de consultas, o enviar estos datos en adjuntos.

7 Conclusiones

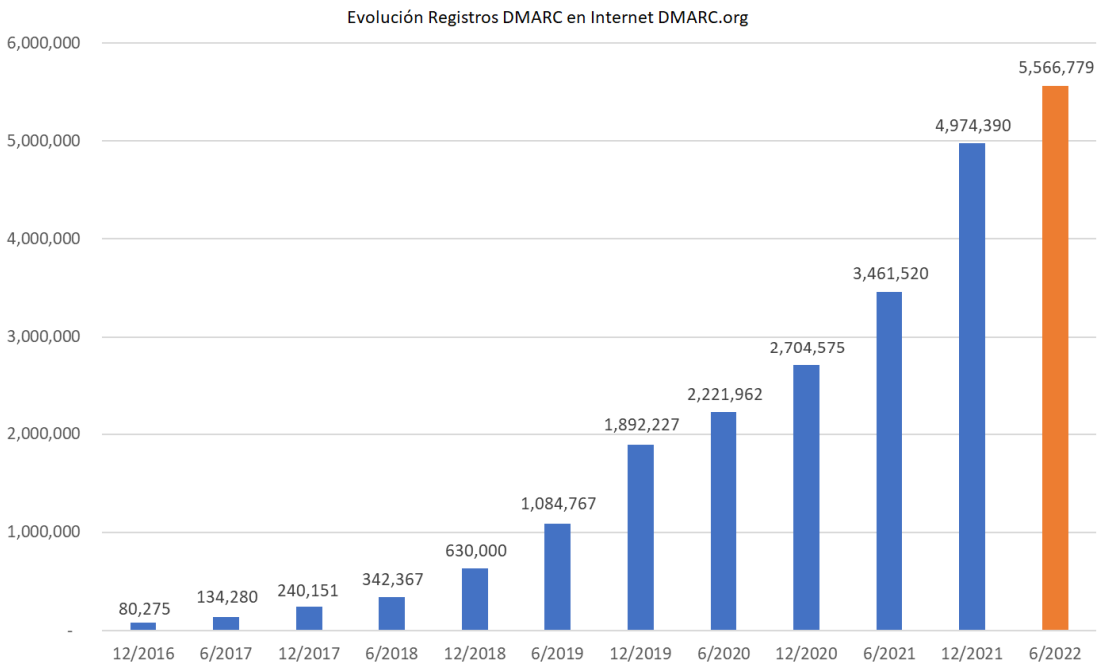
7.1 El uso del protocolo DMARC a nivel global

Uno de los principales motivos que permiten a los atacantes explotar aún hoy las vulnerabilidades en los sistemas de correo electrónico se debe a la baja inversión y la falta de profesionales con sólida experiencia técnica en el ámbito.

Un número de los ataques se basan en la realización de Spoofing que sólo puede ser prevenidos con la implementación rigurosa de los protocolos de seguridad SPF, DKIM y gobernados por DMARC. Sin embargo nos encontramos que el nivel de implementación de este protocolo que ya tiene casi 10 años desde publicado, tiene un nivel de implementación mixto.

Si bien la cantidad de registros DMARC aumenta año a año, indicando que las organizaciones están paulatinamente mejorando su seguridad de correo electrónico, falta mucho para tener un alto nivel de

adopción y que se implementen la políticas segura ("Reject"), que es el objetivo final deseado.



Evolución en la cantidad de registros totales de DMARC publicados en Internet (fuente DMARC.org)

7.2 Análisis de seguridad de correo electrónico en Argentina

Conociendo ahora exactamente cómo fue la evolución de los protocoles de correo electrónico, como funcionan cada uno los protocolos de seguridad, las configuraciones disponibles y las implicancias que tiene cada uno, podemos hacer un análisis para comprender de en qué estado está el ámbito local en cuanto a las mejores prácticas.

Sabemos que DMARC requiere que se publique cuál es la política de seguridad que cada dominio tiene sobre los correos que emite. Por lo que es muy fácil verificar en qué condición y nivel de seguridad se encuentra cada organización, sin necesidad de tener mayor información, ni realizar ningún escaneo de red.

Para el siguiente análisis usamos herramientas gratuitas disponibles en el sitio MXtoolbox.com. Para consultar cada registro MX y detalle DMARC de los dominios de interés.

En el contexto Argentino, tomando una muestra ilustrativa de 22 organizaciones relevantes, por tamaño, importancia, y 3 facultades de la UBA, se puede ver que más de la mitad mantiene políticas de seguridad de correo electrónico inseguras, una señal de falta de inversión, pero también de recursos especializados:

Nombre de la organización	Nombre de Dominio	Registro DMARC	Política de seguridad
Banco Galicia	bancogalicia.com.ar	SI	"Reject"
Ejercito Argentino	ejercito.mil.ar	SI	"Reject"
Fuerza Aerea Argentina	faa.mil.ar	SI	"Reject"
Mercadolibre	mercadolibre.com.ar	SI	"Reject"
Prefectura Naval Argentina	prefecturanaval.gov.ar	SI	"Reject"
YPF	ypf.com	SI	"Reject"
Molinos Río de la Plata	molinos.com.ar	SI	"Quarantine"
Policia Federal Argentina	policiafederal.gov.ar	SI	"Quarantine"
Transportadora de Gas del Sur	tgs.com.ar	SI	"Quarantine"
Anses	anses.gob.ar	SI	"None"
Arcor	arcor.com	SI	"None"
Banco Central de la República Argentina	bcra.gob.ar	SI	"None"
Banco de la Nación Argentina	bna.com.ar	SI	"None"
Facultad de Exactas UBA	fcen.uba.ar	SI	"None"
Facultad de Ingeniería UBA	fi.uba.ar	SI	"None"
Gobierno de la Ciudad de Buenos Aires	buenosaires.gob.ar	SI	"None"
Presidencia de la Nación Argentina	presidencia.gov.ar	SI	"None"
AFIP	afip.gob.ar/afip.gov.ar	NO	-
Armada Argentina	armada.mil.ar	NO	-
Banco Macro	macro.com.ar	NO	-
Facultad de Econónicas UBA	fce.uba.ar	NO	-
Lomanegra	lomanegra.com	NO	-

Alta Seguridad

Buena Seguridad

Inseguro

Inseguro(Sin registro publicado)

Política de seguridad de correo electronico (DMARC) publicadas a Febrero de 2024. Consultas realizadas utilizando MXtoolbox.com

El no tener una política DMARC segura implica que cualquiera de estos dominios de correo electrónicos (ejemplos en amarillo y naranja

marcados como "inseguros") pueden ser fácilmente suplantados en Internet lo que los exponen a ser blancos de ataques de Spoofing/BEC a terceros.

El hecho que estas organizaciones no esté aún cumpliendo con una buena política DMARC, nos dice que muy posiblemente no estén cumpliendo tampoco con los anteriores protocolos de seguridad SPF y DKIM. Ya que si no podrían directamente publicar una política "Reject" segura en cuestión de minutos.

Un grupo que se dedica a ataques al correo electrónico, lo primero que verá es cuáles son los dominios con políticas de seguridad débil, que es señal de infraestructuras sin adecuado mantenimiento.

En caso de fraude a un tercero, estas organizaciones también están más expuestas a ser sujeto de litigios, ya que las victimas pueden fácilmente probar que las políticas de seguridad del dominio suplantado eran insuficientes y no alineadas a las mejores prácticas de mercado. Es común que en casos judicializados de fraudes basados en BEC, las pérdidas irrecuperables por caer en el fraude terminen siendo divididas en base al nivel de responsabilidad comprobado entre las partes que fueron víctimas (la victima directa y el suplantado).

Si una de las partes no cumple con buenos estándares de seguridad, es más difícil poder realizar una defensa robusta y más probable que se termine definiendo una participación en las pérdidas monetarias por probarse negligencia.

7.3 Conclusiones finales

El correo electrónico siempre fue el medio de comunicación más utilizado en Internet. Esta larga trayectoria y popularidad sin embargo no tuvo un correlato directo en su nivel de seguridad, que dejó este aspecto algo relegado a fin de evitar interrupciones, incompatibilidades y mantener su espíritu de sistema simple y eficiente.

La creciente complejidad técnica de las infraestructuras de correo en las organizaciones que tienen que dar solución a: casillas personales; notificaciones automáticas generadas por sistemas; casillas genéricas; acceso para proveedores; listas de distribución; múltiple distribución geográfica; infraestructuras híbridas; entre otros, ha ido atentando contra la velocidad de adoptar las recomendaciones de mayor seguridad nacidas de la evolución de los protocolos emitidos por la Internet Engineering Task Force's (IETF). Especialmente en la implementación de la triada: SPF, DKIM y DMARC.

A esto se le agrega la gran cantidad de formas de acceso que los usuarios han ido sumando para sus casillas. Que ahora pueden ser accedidos vía Web o desde clientes implementados para Windows, MAC, Android, IOS, etc. Cada cliente con sus bases de datos locales, tokens de sesión y su propia forma de proteger los datos según el sistema operativo. Todas estas capas y opciones aumentan la superficie de exposición a ataques, ya que cualquier vulnerabilidad en cualquiera de las combinaciones de plataforma/cliente/versión exponen a los correos a ser capturados por un Malware o virus. El costo de mantener este variado parque de dispositivos móviles renovado, con soporte vigente, y con todas las actualizaciones al día es tan grande que la mayoría de las organizaciones no logran resolverlo con éxito.

La transmisión de datos bancarios vía correo electrónico es una práctica que se debe intentar reducir al mínimo, especialmente en el caso del ámbito corporativo, haciendo mayor uso de Portales de auto gestión para proveedores/clientes. Pero estas buenas prácticas son siempre difíciles de llevar a cabo en entonos atomizados con muchos clientes o proveedores pequeños.

En este contexto no es sorpresa que los ataques BEC sigan manteniendo tanta vigencia y generen enormes pérdidas anuales de forma transversal a todo tipo de industrias en todo el mundo. El hecho que se haya convertido en un negocio para grandes grupos criminales organizados supone un enorme riesgo para las organizaciones. Que tendrán que lidiar

por mucho tiempo contra avanzadas herramientas de robo de datos de correo (malware/spyware), campañas de Phishing para robo de credenciales, y técnicas de ingeniería social siempre en evolución. Estos grupos criminales tienen a su disposición cientos de cuentas bancarias en todo el mundo para realizar los desvíos fraudulentos, ubicadas en países especialmente seleccionados por ser casi imposible hacer una denuncia policial o iniciar una investigación por este tipo de delitos.

La inversión con mejor relación costo/beneficio que se puede adoptar son las campañas de concientización, para que el personal con más contacto con pagos y cobros esté al tanto de las técnicas que utilizan los atacantes para llevar a cabo las estafas. Y como mejoras a nivel de procedimientos, al menos, poner controles más rígidos a los cambios de datos bancarios para los proveedores.

Pero no podemos dejar de lado las inversiones que se necesitan realizar en la seguridad de las infraestructuras de correo, cuyo mayor dificultad es la falta de profesionales que tengan conocimiento técnicos avanzados de estas temáticas. La muy lenta adopción de políticas seguras en DMARC son un fiel reflejo de esta realidad, en donde las organizaciones quedan públicamente expuestas del bajo nivel seguridad adoptado para sus respectivas infraestructuras de correos electrónicos.

8 Bibliografía

NIST Special Publication (800-177) - Trustworthy Email (Scott Rose, J. Stephen Nightingale, Simson Garfinkel, Ramaswamy Chandramouli 2019)

Federal Bureau of Investigation's Internet Crime Report 2022 (FBI - Internet Complaint Center 2023)

RFC788 - Simple Mail Transfer Protocol (Jonathan B. Postel 1981)

RFC5321 - Simple Mail Transfer Protocol (J. Klensin 2008)

RFC7208 - Sender Policy Framework (S. Kitterman 2014)

RFC4871 - DomainKeys Identified Mail (DKIM) Signatures (E. Allman (Sendmail), J. Callas (PGP Corporation), M. Delany and M. Libbey (Yahoo! Inc), J. Fenton and M. Thomas (Cisco Systems))

RFC6376 - DomainKeys Identified Mail (D. Crocker, T. Hansen, M. Kucherawy 2011)

RFC7489 - Domain-based Message Authentication, Reporting and Conformance (M. Kucherawy, E. Zwicky 2015)