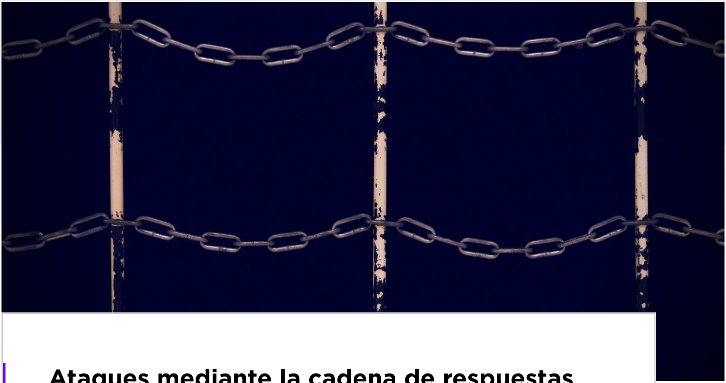
Experiencing a Breach? Consiga una demostración

SentinelOne blog

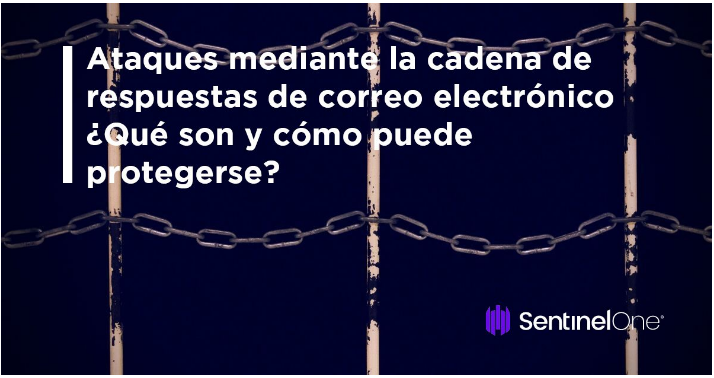
FREE DEMO



Ataques mediante la cadena de respuestas de correo electrónico | ¿Qué son y cómo puede protegerse?

junio 10, 2020
by SentinelOne

Como confirman los datos recientes, para las empresas, el phishing por correo electrónico sigue siendo el primer vector de infección por malware y los ataques BEC (Business Email Compromise) o fraudes del CEO representan la primera causa de pérdidas financieras provocadas por la ciberdelincuencia. Mientras los típicos ataques de phishing y phishing selectivo (o *spearphishing*) intentan suplantar la identidad del remitente con una dirección falsa, hay una variante más sofisticada que secuestra las cadenas legítimas de correo electrónico para insertar un mensaje de phishing en una conversación existente. Esta técnica, conocida con los nombres de «ataque mediante la cadena de respuestas» o «secuestro de la cadena de respuestas de correo electrónico» y «spam por secuestro del hilo de discusión», ha sido observada por los investigadores de SentinelLabs durante su análisis reciente del malware Valak. En este artículo, analizamos el funcionamiento de este tipo de ataques y explicamos cómo puede protegerse usted y su empresa contra esta táctica empleada por los ciberdelincuentes.



Ataques mediante la cadena de respuestas de correo electrónico ¿Qué son y cómo puede protegerse?

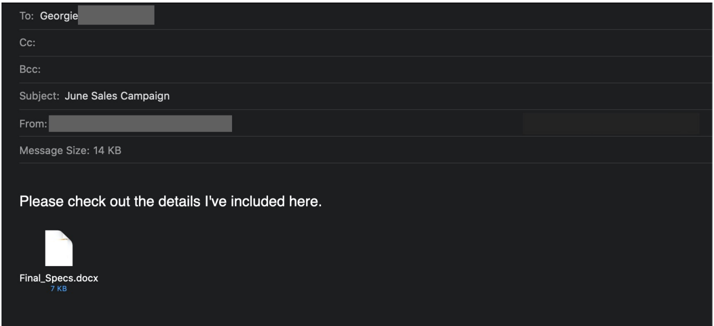
¿Cómo funcionan los ataques mediante la cadena de respuestas de correo electrónico?

El secuestro de una cadena de respuestas de correo electrónico se inicia con la usurpación de una cuenta de correo electrónico. Los ciberdelincuentes acceden a una o varias cuentas de correo electrónico a través de un compromiso anterior y del volcado de credenciales o mediante técnicas como el relleno de credenciales o la difusión de contraseñas (credential stuffing y password-spraying). A continuación, empiezan a supervisar los hilos de conversaciones en busca de oportunidades para enviar malware o enlaces maliciosos a uno o varios de los participantes en una cadena de correspondencia en curso.

Esta técnica es especialmente eficaz, ya que aprovecha que ya se ha establecido un vínculo de confianza entre los destinatarios. El ciberdelincuente no se infiltra como nuevo interlocutor ni intenta usurpar la dirección de correo electrónico de alguien. Lo que hace es enviar su mensaje malicioso desde una cuenta legítima de uno de los participantes.

Al disponer de acceso a todo el hilo de la conversación, puede adaptar su mensaje de spam al contexto. Esto, además de que los destinatarios ya confían en el remitente, aumenta enormemente las posibilidades de que la víctima abra el adjunto malicioso o haga clic en un enlace peligroso.

A modo de ejemplo, supongamos que una cuenta que pertenece a «Sam» ha sido comprometida, y el ciberdelincuente ve que Sam y «Georgie» (y tal vez otros) hablan sobre una nueva campaña de ventas. Puede utilizar ese contexto para enviar a Georgie un documento malicioso que parece relacionado con la conversación que están manteniendo.



To: Georgie [redacted]

Cc:

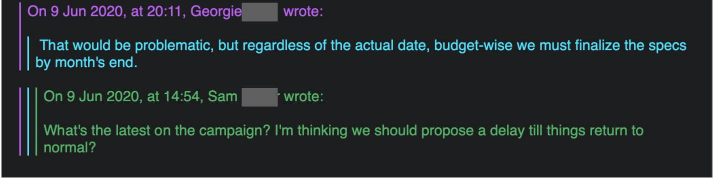
Bcc:

Subject: June Sales Campaign

From: [redacted]

Message Size: 14 KB

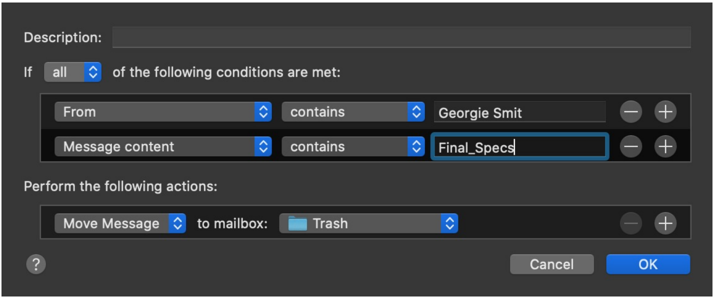
Please check out the details I've included here.



> On 9 Jun 2020, at 20:11, Georgie [redacted] wrote:
>
> > That would be problematic, but regardless of the actual date, budget-wise we must finalize the specs by month's end.
> >
> > > On 9 Jun 2020, at 14:54, Sam [redacted] wrote:
> > >
> > > What's the latest on the campaign? I'm thinking we should propose a delay till things return to normal?

Para que el propietario de la cuenta comprometida no advierta el comportamiento malicioso, los hackers utilizan a menudo una bandeja de entrada alternativa para recibir los mensajes.

Para ello, deben emplear las reglas del cliente de correo electrónico para redirigir mensajes específicos desde la bandeja de entrada habitual a una carpeta que el verdadero titular de la cuenta es poco probable que inspeccione, por ejemplo, la Papelera. Gracias a esta técnica, si Georgie, en nuestro ejemplo, responde al mensaje de correo electrónico de phishing de Sam, la respuesta puede desviarse de manera que el verdadero Sam no la vea jamás.



Description:

If all of the following conditions are met:

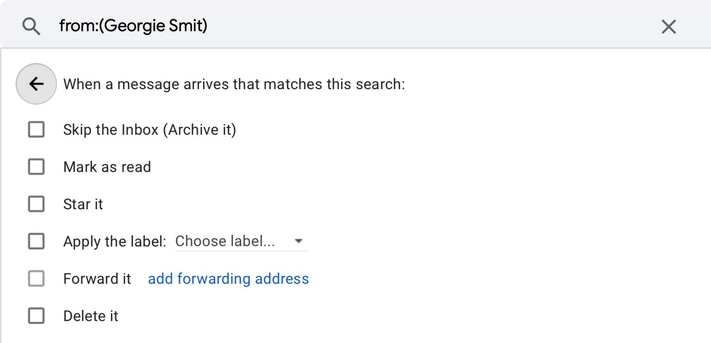
From contains Georgie Smit

Message content contains Final_Specs

Perform the following actions:

Move Message to mailbox: Trash

Otra opción es que, cuando un hacker consigue hacerse con el control de una cuenta, utilice la configuración del cliente de correo electrónico para reenviar los mensajes de determinados destinatarios a otra cuenta.



from:(Georgie Smit)

When a message arrives that matches this search:

☐ Skip the Inbox (Archive it)

☐ Mark as read

☐ Star it

☐ Apply the label: Choose label...

☐ Forward it add forwarding address

☐ Delete it

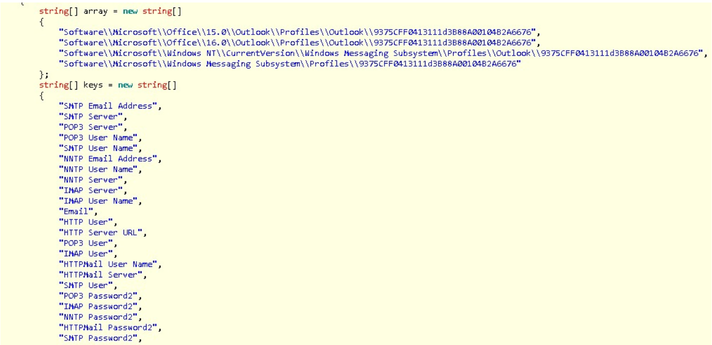
Otro truco que puede ayudar a mantener al titular de la cuenta en la más absoluta ignorancia consiste en crear una regla de correo que busque palabras clave como «phish», «phishing», «piratería» y «hacker» o «pirata» en los mensajes entrantes y los elimine, o bien responda automáticamente con un mensaje predefinido. De esta forma, se impide que cualquier compañero sospechoso o preocupado alerte al titular de la cuenta con mensajes como «¿te han pirateado?» u otros similares.

¿Qué familias de malware han utilizado ataques mediante la cadena de respuestas?

Los ataques mediante la cadena de respuestas de correo electrónico aparecieron en 2017. En 2018, las campañas del troyano bancario Gozi ISFB/Ursnif comenzaron a utilizar también esta técnica. Aunque en algunos casos la propia cadena de correspondencia se falsificaba sencillamente para añadir legitimidad, en otros los ciberdelincuentes comprometieron cuentas legítimas y las utilizaron para piratear hilos de conversación existentes y para enviar spam a otros destinatarios.

Los adjuntos maliciosos pueden aprovechar VBScript y PowerShell a través de macros de Office para distribuir cargas útiles como Emotet, Ursnif u otro malware, por ejemplo, un cargador o un malware troyano bancario.

Los investigadores de SentinelLabs han demostrado que el malware Valak utiliza complementos especializados, diseñados para robar credenciales específicamente destinadas para su uso en ataques mediante la cadena de respuestas de correo electrónico.



```
        string[] array = new string[]
        {
            "Software\\Microsoft\\Office\\15.0\\Outlook\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676",
            "Software\\Microsoft\\Office\\16.0\\Outlook\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676",
            "Software\\Microsoft\\Windows NT\\CurrentVersion\\Windows Messaging Subsystem\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676",
            "Software\\Microsoft\\Windows Messaging Subsystem\\Profiles\\9375CFF0413111d3B88A00104B2A6676"
        };
        string[] keys = new string[]
        {
            "SMTP Email Address",
            "SMTP Server",
            "POP3 Server",
            "POP3 User Name",
            "SMTP User Name",
            "NNTP Email Address",
            "NNTP User Name",
            "NNTP Server",
            "IMAP Server",
            "IMAP User Name",
            "Email",
            "HTTP User",
            "HTTP Server URL",
            "POP3 User",
            "IMAP User",
            "HTTPMail User Name",
            "HTTPMail Server",
            "SMTP User",
            "POP3 Password2",
            "IMAP Password2",
            "NNTP Password2",
            "HTTPMail Password2",
            "SMTP Password2",
```

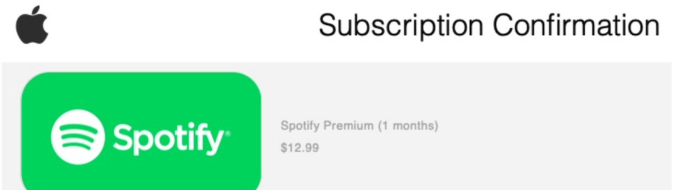
Tal y como señalan los investigadores:

> «Si quiere aprovechar los ataques mediante la cadena de respuestas de correo electrónico para sus campañas de spam, evidentemente necesita algunos datos de correo electrónico. Es interesante señalar que cuando las campañas empezaron a inclinarse por Valak, en detrimento de Gozi, es cuando surgió la incorporación de un complemento dedicado al robo de datos de intercambio».

¿Por qué son tan eficaces los ataques que emplean la cadena de respuestas de correo electrónico?

Aunque las campañas de phishing selectivo e incluso las campañas de phishing mediante spam siguen siendo un método de ataque fiable para los ciberdelincuentes, los ataques que usan la cadena de respuestas de correo electrónico complican todavía más la tarea a los equipos de seguridad.

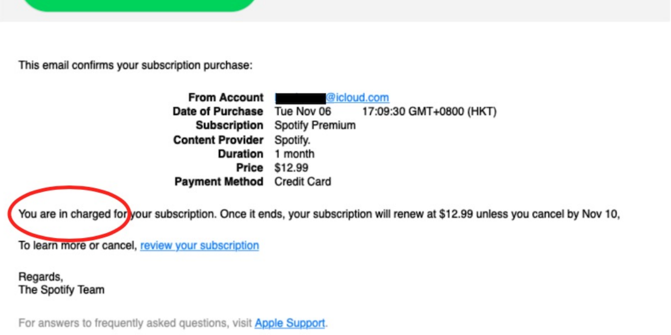
En ataques de phishing ordinarios, es habitual ver faltas de ortografía y gramaticales como el que se muestra a continuación.



Subscription Confirmation

Spotify Premium (1 months)

$12.99



This email confirms your subscription purchase:

From Account [redacted]@icloud.com
Date of Purchase Tue Nov 06 17:09:30 GMT+0800 (HKT)
Subscription Spotify Premium
Content Provider Spotify.
Duration 1 month
Price $12.99
Payment Method Credit Card

You are in charged for your subscription. Once it ends, your subscription will renew at $12.99 unless you cancel by Nov 10,

To learn more or cancel, review your subscription

Regards,
The Spotify Team

For answers to frequently asked questions, visit Apple Support.

Además, los asuntos o los cuerpos de los mensajes de correo masivo de falsificación (*spoofing*) rara vez son pertinentes para la mayoría de los destinatarios, lo que inmediatamente levanta sospechas.

Incluso en el caso de ataques selectivos con objetivos más concretos, la formación sobre concienciación en seguridad y las prácticas de uso seguro del correo electrónico (no hacer clic en enlaces, no abrir adjuntos de remitentes desconocidos o no responder a mensajes de correo electrónico no solicitados) pueden contribuir a reducir los riesgos. Sin embargo, en el caso de los ataques mediante la cadena de respuestas de correo electrónico, es posible que falten los indicadores de alerta habituales.

Este tipo de ataques están diseñados con esmero y los mensajes no contienen errores lingüísticos. Además, gracias a la credibilidad que consiguen al insertar una respuesta a un hilo existente de un remitente legítimo, incluso el empleado más prudente y mejor formado podría ser engañado por este tipo de táctica.

¿Cómo prevenir un ataque mediante la cadena de respuestas?

Dado que el origen del mensaje es legítimo y fiable, y que el ciberdelincuente cuenta con un historial de correo electrónico y con contexto de la conversación, puede ser difícil detectar un ataque de este tipo bien diseñado, en particular si aparece dentro (o parece formar parte) de un hilo largo con muchos participantes fiables.

Dicho esto, existen varias recomendaciones que puede seguir para evitar convertirse en víctima de este tipo de fraude.

En primer lugar, puesto que los ataques que usan la cadena de respuestas dependen del compromiso de cuentas, asegúrese de que todas las cuentas de correo electrónico respetan las mejores prácticas en materia de seguridad. Eso debe incluir autenticación de dos factores o multifactor (MFA), una contraseña diferente para cada cuenta y contraseñas con un mínimo de 16 caracteres. Se debe animar a los usuarios a que verifiquen regularmente la configuración de su cliente de correo electrónico y las reglas de correo, a fin de asegurarse de que no se redirijan o eliminen mensajes sin su conocimiento.

En segundo lugar, bloquee o prohíba por completo el uso de macros de Office siempre que sea posible. Aunque no son el único medio por el que los adjuntos maliciosos pueden comprometer un dispositivo, las macros siguen siendo un vector de ataque habitual.

En tercer lugar, puesto que la información es poder, le recomendamos complementar la formación de concienciación de sus empleados con una explicación de los ataques mediante la cadena de respuestas de correo electrónico, y su funcionamiento. Para ello, puede recomendarles que lean artículos como este. Los usuarios del correo electrónico deben conocer el funcionamiento de los ataques de phishing y cómo evolucionan las técnicas que emplean los ciberdelincuentes. Es esencial que comprendan por qué es importante tratar con cierta prudencia todas las solicitudes para abrir adjuntos o enlaces, con independencia de la fuente.

En cuarto lugar, asegúrese de que sus endpoints están protegidos con una solución de seguridad EDR moderna y fiable, capaz de bloquear la ejecución de código malicioso oculto en adjuntos o en enlaces, antes de se produzcan daños. Las suites antivirus tradicionales que dependen de la reputación y las reglas YARA no fueron diseñadas para hacer frente a los ataques polimórficos y sin archivos. En el panorama actual de amenazas de ciberseguridad debe disponer, como mínimo, de una plataforma de próxima generación automatizada e impulsada mediante la inteligencia artificial.

Conclusión

Los ataques mediante la cadena de respuestas de correo electrónico constituyen otra modalidad de ingeniería social utilizada por los ciberdelincuentes para conseguir sus objetivos. A diferencia del mundo físico, que se rige por leyes naturales inmutables, en el ciberespacio no existen reglas que no puedan modificarse mediante la manipulación de hardware o software, o del usuario. Sin embargo, esto vale tanto para los equipos de seguridad como para los ciberdelincuentes. Manteniendo el control de todos los aspectos de nuestro ciberentorno, podemos frustrar los ataques antes de que se produzcan o generen daños a largo plazo en la empresa. Proteja sus dispositivos, conciencie a los usuarios, forme a sus empleados, y deje que los ciberdelincuentes busquen a sus víctimas en otra parte.

¿Te gusta este artículo? Síguenos en LinkedIn, Twitter, YouTube or Facebook para ver el contenido que publicamos.

Lee acerca de Ciberseguridad

- Kubernetes: desafíos de seguridad, riesgos y vectores de ataque
- 10 maneras de proteger su Active Directory