Un actor de amenazas desconocido ha sido vinculado a una campaña de estafa masiva que aprovechó una mala configuración en el enrutamiento de correos electrónicos en las defensas del proveedor de seguridad de correo electrónico Proofpoint para enviar millones de mensajes que suplantaban a varias compañías populares como Best Buy, IBM, Nike y Walt Disney, entre otras.

> *«Estos correos electrónicos fueron enviados desde los relés de correo oficial de Proofpoint con firmas SPF y DKIM autenticadas, lo que permitió eludir las principales protecciones de seguridad, todo con el fin de engañar a los destinatarios y robar fondos y datos de tarjetas de crédito»,* dijo el investigador de Guardio Labs, Nati Tal, en un informe detallado.

La empresa de ciberseguridad ha bautizado la campaña como EchoSpoofing. Se cree que la actividad comenzó en enero de 2024, con el actor de amenazas explotando la brecha para enviar hasta tres millones de correos electrónicos por día en promedio, un número que alcanzó un pico de 14 millones a principios de junio cuando Proofpoint comenzó a implementar contramedidas.

> *«La parte más única y poderosa de este dominio es el método de suplantación, que deja casi ninguna posibilidad de darse cuenta de que no es un correo genuino enviado desde esas compañías»,* dijo Tal a la publicación.

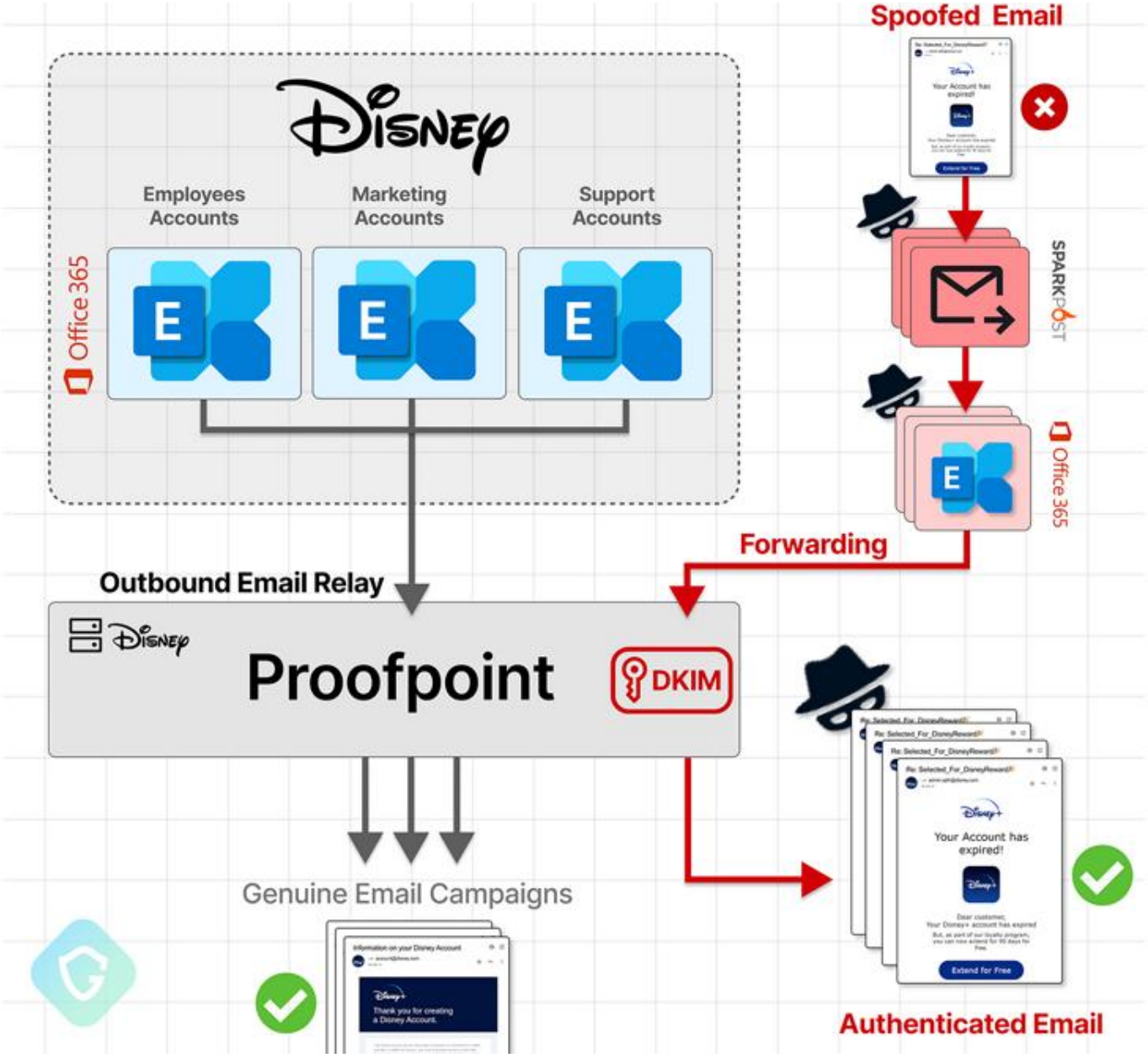
> *«Este concepto de EchoSpoofing es realmente poderoso. Es algo extraño que se esté utilizando para phishing a gran escala en lugar de una campaña de spear-phishing más selecta, donde un atacante podría tomar rápidamente la identidad de cualquier miembro del equipo de una empresa real y enviar correos electrónicos a otros compañeros de trabajo, y finalmente, a través de ingeniería social de alta calidad, obtener acceso a datos internos o credenciales y hasta comprometer toda la empresa.»*

La técnica, que implica que el actor de amenazas envíe los mensajes desde un servidor SMTP en un servidor privado virtual (VPS), es notable porque cumple con las medidas de autenticación y seguridad como SPF y DKIM, que son las siglas de Sender Policy Framework y DomainKeys Identified Mail, respectivamente, y se refieren a métodos de autenticación diseñados para evitar que los atacantes imiten un dominio legítimo.

Todo se remonta al hecho de que estos mensajes se enrutan desde varios inquilinos de Microsoft 365 controlados por adversarios, que luego son retransmitidos a través de las infraestructuras de correo electrónico de los clientes empresariales de Proofpoint para llegar a los usuarios de proveedores de correo electrónico gratuitos como Yahoo!, Gmail y GMX.

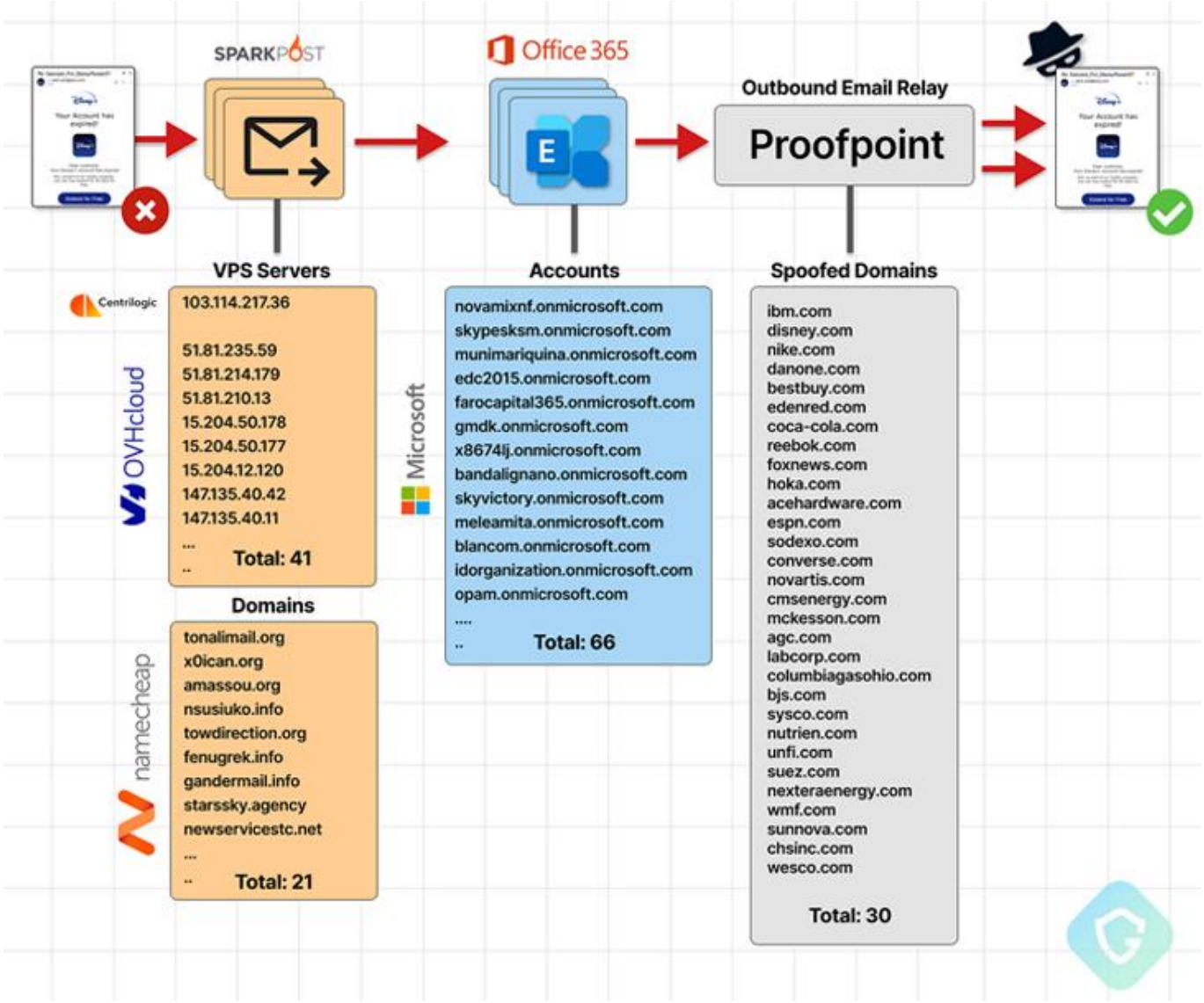
Esto es el resultado de lo que Guardio describió como una *«falla de configuración excesivamente permisiva»* en los servidores de Proofpoint («pphosted.com») que esencialmente permitió a los spammers aprovechar la infraestructura de correo electrónico para enviar los mensajes.

> *«La causa raíz es una función modificable de configuración de enrutamiento de correo electrónico en los servidores de Proofpoint que permite la retransmisión de mensajes salientes de las organizaciones desde inquilinos de Microsoft 365, pero sin especificar qué inquilinos de M365 permitir»*, dijo Proofpoint en un informe de divulgación coordinada.
>
> *«Cualquier infraestructura de correo electrónico que ofrezca esta función de configuración de enrutamiento de correo electrónico puede ser abusada por spammers.»*



En otras palabras, un atacante puede aprovechar esta deficiencia para configurar inquilinos de Microsoft 365 falsos y enviar mensajes de correo electrónico suplantados a los servidores de retransmisión de Proofpoint, desde donde se *«retransmiten»* como mensajes digitales genuinos que impersonan los dominios de los clientes.

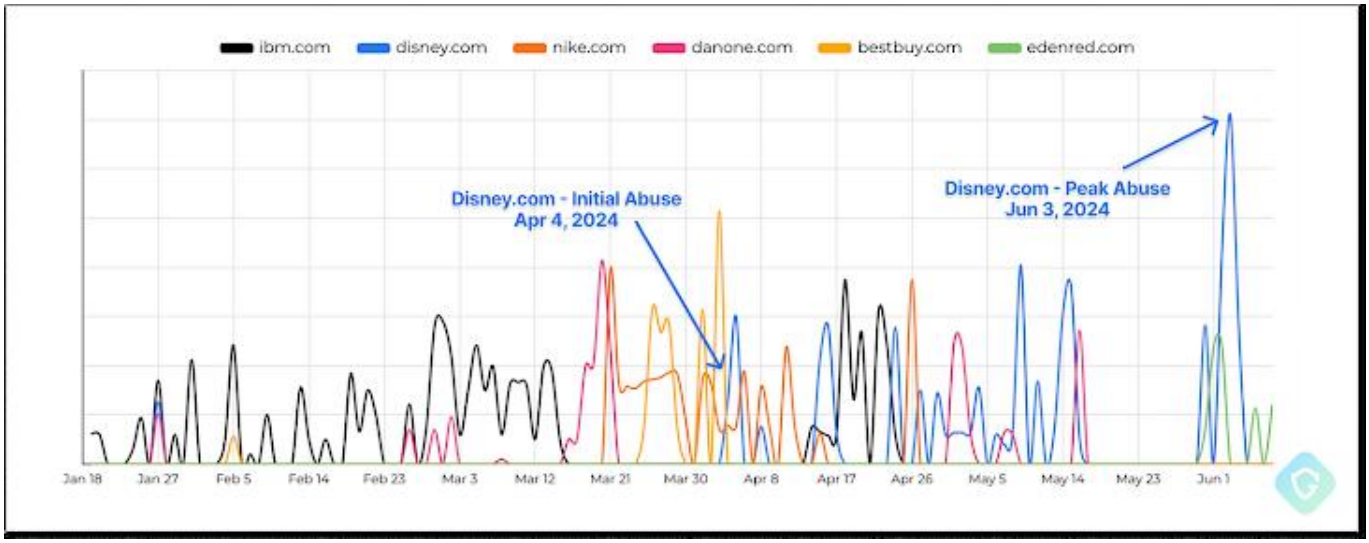
Esto, a su vez, se logra configurando el conector de correo saliente del servidor Exchange directamente al punto final vulnerable «*pphosted.com*» asociado con el cliente. Además, se utiliza una versión pirateada de un software legítimo de entrega de correo electrónico llamado PowerMTA para enviar los mensajes.



> *«El spammer utilizó una serie rotativa de servidores privados virtuales (VPS)*

> *alquilados de varios proveedores, usando muchas direcciones IP diferentes para iniciar ráfagas rápidas de miles de mensajes a la vez desde sus servidores SMTP, enviados a Microsoft 365 para ser retransmitidos a los servidores de los clientes alojados por Proofpoint»*, dijo Proofpoint.
>
> *«Microsoft 365 aceptó estos mensajes suplantados y los envió a las infraestructuras de correo electrónico de estos clientes para ser retransmitidos. Cuando los dominios de los clientes fueron suplantados mientras se retransmitían a través de la infraestructura de correo electrónico correspondiente del cliente, también se aplicó la firma DKIM a medida que los mensajes transitaban a través de la infraestructura de Proofpoint, haciendo que los mensajes de spam fueran más entregables.»*

Se sospecha que EchoSpoofing fue intencionalmente elegido por los operadores como una forma de generar ingresos ilegales y evitar el riesgo de exposición durante períodos prolongados, ya que dirigirse directamente a las empresas mediante este modus operandi podría haber aumentado drásticamente las posibilidades de ser detectado, poniendo en peligro efectivamente todo el esquema.



Dicho esto, actualmente no se sabe quién está detrás de la campaña. Proofpoint afirmó que la actividad no coincide con ningún actor o grupo de amenazas conocido.

> *«En marzo, los investigadores de Proofpoint identificaron campañas de spam que se transmitían a través de la infraestructura de correo electrónico de algunos clientes de Proofpoint, enviando spam desde inquilinos de Microsoft 365. Todos los análisis indican que esta actividad fue realizada por un solo actor de spam, cuya actividad no atribuimos a una entidad conocida»,* explicó en un comunicado.

> *«Desde que descubrimos esta campaña de spam, hemos trabajado arduamente para proporcionar instrucciones correctivas, incluyendo la implementación de una interfaz administrativa simplificada para que los clientes especifiquen qué inquilinos de M365 pueden retransmitir, negando por defecto a todos los demás inquilinos de M365.»*

Proofpoint subrayó que no se expusieron datos de clientes, ni ninguno de ellos sufrió pérdida de datos como resultado de estas campañas. Además, señaló que se comunicó directamente con algunos de sus clientes para cambiar sus configuraciones y detener la efectividad de la actividad de spam de retransmisión saliente.

> *«A medida que comenzamos a bloquear la actividad del spammer, el spammer aceleró sus pruebas y se trasladó rápidamente a otros clientes. Establecimos un proceso continuo para identificar a los clientes afectados cada día, re-priorizando el alcance para corregir las configuraciones»,* destacó la compañía.

Para reducir el spam, está instando a los proveedores de VPS a limitar la capacidad de sus usuarios para enviar grandes volúmenes de mensajes desde servidores SMTP alojados en su infraestructura. También está solicitando a los proveedores de servicios de correo electrónico

que restrinjan las capacidades de los inquilinos de prueba gratuita y recién creados no verificados para enviar mensajes de correo electrónico masivos salientes, así como evitar que envíen mensajes que suplantan un dominio del cual no tienen propiedad comprobada.

> *«Para los CISOs, la principal lección aquí es cuidar especialmente la postura en la nube de su organización, específicamente con el uso de servicios de terceros que se convierten en la columna vertebral de los métodos de red y comunicación de su empresa. Específicamente en el ámbito de los correos electrónicos, siempre mantenga un ciclo de retroalimentación y control propio, incluso si confía plenamente en su proveedor de correo electrónico»,* dijo Tal.
>
> *«Y para otras compañías que brindan este tipo de servicios fundamentales, al igual que lo hizo Proofpoint, deben ser vigilantes y proactivos al pensar en todos los posibles tipos de amenazas desde el principio. No solo amenazas que afectan directamente a sus clientes, sino también al público en general.*
>
> *«Esto es crucial para la seguridad de todos nosotros y las compañías que crean y operan la columna vertebral de Internet, incluso si son de propiedad privada, tienen la mayor responsabilidad sobre ello. Como alguien dijo, en un contexto completamente diferente pero tan relevante aquí: 'Con grandes poderes, viene una gran responsabilidad.'»*