infoblox

Threat Intel

MUDDLING MALSPAM: USO DE DOMINIOS SUPLANTADOS PARA ENVIAR SPAM MALICIOSO

Autores:
Stelios Chatzistogias
Laura da Rocha
Renée Burton

ÍNDICE

Al principio puede parecer una historia sobre una investigación fallida, pero en realidad es una historia sobre cómo la investigación puede buscar una cosa y acabar descubriendo algo totalmente distinto.

En marzo de 2024, publicamos un informe en nuestro blog sobre un actor al que llamamos Muddling Meerkat, que efectúa desconcertantes operaciones de DNS a través del Gran Cortafuegos chino. Habíamos invertido mucho tiempo en nuestra investigación pero no conseguíamos averiguar el propósito de estas operaciones plurianuales. En lugar de guardar el trabajo en un cajón, decidimos divulgar lo que sabíamos sobre la actividad para que otros compartieran sus propias percepciones y, colectivamente, llegar a comprender la verdadera naturaleza de Muddling Meerkat. ¡Y funcionó! El blog atrajo ideas tanto de profesionales de las redes como de la seguridad; algunos proporcionaron datos anónimos sobre su propia visión de Muddling Meerkat, o al menos de los llamados «dominios objetivo» que vemos en el DNS.

Muchas de las sugerencias para futuras investigaciones se centraron en las operaciones de spam. Algunas organizaciones habían recibido notificaciones de abuso de dominios de su propiedad, normalmente dominios internos que no utilizaban externamente. Los informes de abuso eran la prueba de la distribución de spam a gran escala a grandes proveedores de correo como Google y Yahoo, y en su inmensa mayoría, la IP de origen del spam se asignaba a China. Esto parecía concordar con las actividades de Muddling Meerkat, en las que observamos registros de servidores de correo (MX) falsos que provenían del espacio IP chino, así como consultas MX similares que llegaban a las redes corporativas a través de servicios de resolución abiertos.

Uno de los archivos de datos que nos compartieron nos condujo a una revelación: inosotros mismos teníamos varios dominios «objetivo» de Muddling Meerkat! Eso nos permitió utilizar los informes de abuso que nos enviaban para estos dominios, así como los registros de los servidores de nombres autoritativos del DNS, para comprender mejor la actividad relacionada con el spam desde la perspectiva del DNS. Pero también tenemos una buena colección de spam, y pudimos buscar campañas que mostraran el comportamiento de Muddling Meerkat a lo largo del tiempo.

Este documento es el resultado de nuestra búsqueda en el spam. Para ser honestos, no estamos seguros de estar más cerca de comprender Muddling Meerkat, lo cual a primera vista podría considerarse un fracaso. Sin embargo, al seguir esos hilos, aprendimos mucho sobre el uso de la suplantación de dominios en las campañas de spam malicioso (malspam) modernas. Vamos a compartir algunas de nuestras «detecciones», que muestran las formas más interesantes en las que los actores utilizan la suplantación de dominios hoy en día, todas ellas con algún comportamiento del tipo de Muddling Meerkat. Pudimos conectar estas campañas con los informes de abuso que recibimos de los destinatarios y nuestros registros de DNS autoritativos. Además, dado que poseemos algunos de los dominios suplantados, capturamos varios como rebotes hacia nuestros servidores de correo. Al alternar entre estas fuentes, también aprendimos más sobre la extensión de los dominios objetivo de Muddling Meerkat y ampliamos nuestro conjunto inicial de informes, de aproximadamente 20 a más de 650 dominios.

Lo más sorprendente es la omnipresencia de la suplantación de dominios en el spam. Hay varios mecanismos diseñados para proteger a los usuarios del spam en general y de la suplantación de identidad en particular, pero descubrimos que la suplantación de identidad sigue siendo muy utilizada. La mayoría de las campañas se envían desde direcciones IP chinas, y la variedad de tipos de campañas es bastante notable. Pese a las medidas de seguridad, el uso de dominios suplantados sigue siendo económicamente rentable. En este documento, examinaremos:

- Campañas modernas que utilizan códigos QR en archivos PDF adjuntos para robar a ciudadanos chinos,
- Suplantación de una marca popular dirigida a usuarios japoneses para robar credenciales de inicio de sesión,
- Campañas de extorsión antiguas, posiblemente impulsadas por restos de botnets, que intentan engañar a los usuarios para que envíen pagos a la criptocartera del actor de amenazas, y
- Campañas financieras misteriosas, que parecen no tener contenido malicioso, ni razón de ser.

Además, describiremos cómo utilizamos nuestros propios registros de servidores del DNS autoritativos para tratar de entender Muddling Meerkat, pero en su lugar detectamos estas campañas de spam.

SUPLANTACIÓN DE DOMINIO EN EL SPAM

Los actores de amenazas pueden falsificar (suplantar) la dirección del remitente de un correo electrónico. Lo hacen para que el correo electrónico parezca más legítimo. Al utilizar un dominio que lleva registrado muchos años, es más probable que superen los mecanismos de seguridad que comprueban la antigüedad del dominio del remitente para identificar spam malicioso. Por otro lado, si el actor suplanta un dominio conocido como `amazon[.]com`, hay varios mecanismos que el servidor de correo receptor puede utilizar para determinar cuándo un correo electrónico que usa uno de estos dominios ha sido suplantado. Creemos que este riesgo de detección es la razón por la cual los remitentes de spam utilizan dominios antiguos relegados, el mismo tipo de dominio que prefiere Muddling Meerkat para sus operaciones.

Cuando un servidor de correo recibe un mensaje, lleva a cabo varias comprobaciones en el DNS para validar el remitente. A continuación, compara esos resultados con los encabezados del mensaje. Estas comprobaciones incluyen acciones como verificar que la dirección IP desde la que se ha recibido el correo electrónico esté autorizada para enviar mensajes a para ese dominio. Algunas de estas comprobaciones dependen de registros específicos del DNS que a menudo no existen para dominios antiguos relegados, lo que puede provocar un fallo «soft».

Después de que el servidor efectúe las comprobaciones típicas y, posiblemente, aplique algoritmos de seguridad de correo adicionales, el mensaje puede marcarse como spam o ponerse en cuarentena. En otros casos, llegará a la bandeja de entrada del usuario. El actor de malspam espera que sus correos electrónicos sintéticos superen suficientes filtros de spam como para llegar a los usuarios y obtener su recompensa.

SERVIDORES DNS AUTORITATIVOS Y SPAM

Resulta que poseemos algunos dominios en desuso que no han alojado contenido de forma activa desde hace casi 20 años. Carecen de la mayoría de los registros del DNS, incluidos los que se utilizan normalmente para verificar la autenticidad del dominio de un remitente, por ejemplo, los registros del Sender Policy Framework (SPF). Los dominios son cortos y están en TLD de alta reputación: perfectos para Muddling Meerkat y remitentes de spam por igual.

Irónicamente, varios de nuestros antiguos dominios se citan habitualmente, por ejemplo, en la lista del millón de dominios principales de Tranco. Sospechamos que su popularidad se debe por completo al spam. Sin desviarnos demasiado del tema principal de este blog, la popularidad de nuestros dominios inactivos ilustra claramente una de las razones por las que las clasificaciones de las listas principales deben tomarse con cautela. Hemos dedicado mucho tiempo a estudiar la popularidad de los dominios y las amenazas; consulte nuestros documentos anteriores.[1,2] (Para leer las notas al pie, consulte este PDF en línea).

El DNS nos proporciona una perspectiva única sobre el abuso de nuestros dominios. Registramos las consultas de todos nuestros dominios en nuestro servidor de DNS autoritativo. Estos registros nos permiten ver una amplia gama de actividades del DNS, desde el escaneo de internet hasta la distribución de spam. En el caso del correo electrónico, el servidor de correo de un destinatario realizará varias consultas de DNS al servidor autoritativo sobre el dominio del remitente, incluidos los registros TXT del DNS. A partir de nuestros registros, podemos ver la dirección IP de los resolutores de DNS que utilizan esos servidores de correo y hacernos una idea de la distribución geográfica del spam que suplanta nuestros dominios.

También hemos configurado registros de DomainKeys Identified Email (DKIM) para que los proveedores que reciben spam de nuestros dominios puedan enviarnos informes de abuso por correo electrónico. Esos informes de abuso incluyen la dirección IP del remitente de spam y la marca de tiempo. Podemos combinarlos con las solicitudes de los registros TXT del DNS para obtener una visión bastante clara de cómo se nos asocia falsamente con la distribución de spam. Nuestros servidores de correo no envían mensajes; solo los reciben.

Dado que nos interesaba la posible actividad de spam de Muddling Meerkat, necesitábamos aislar las posibles consultas del actor de las demás. Hay mucho ruido en el DNS. Muchas organizaciones de investigación, como la nuestra, consultan el DNS para recopilar información y crear una huella sintética en registros históricos. Nuestros servidores no deberían recibir ninguna consulta en el DNS, porque todos los dominios están inactivos; sin embargo, reciben miles de consultas cada día, a veces decenas de miles. La Figura 1 compara el número de consultas recibidas en nuestro servidor autoritativo para cuatro dominios diferentes de Muddling Meerkat a lo largo del tiempo. El gráfico superior indica todos los tipos de registros y el inferior, las consultas de MX. Estos gráficos longitudinales indican que la actividad relacionada con el correo no está necesariamente correlacionada con la actividad general del DNS para los dominios.

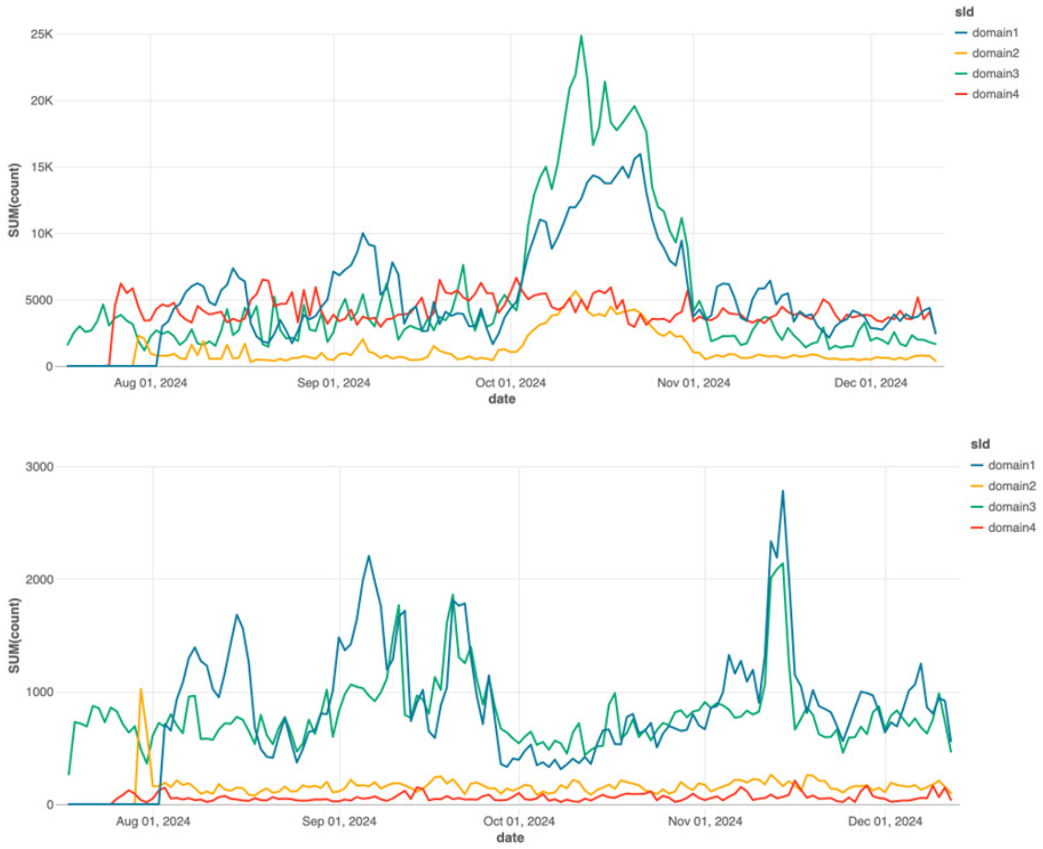

Figura 1. Gráfico superior: volumen de consultas para todos los tipos de registros del DNS en nuestro servidor autoritativo, por dominio; gráfico inferior: volumen de consultas para registros MX

La mayoría de las consultas que recibimos en nuestros servidores autoritativos no coinciden con los patrones de Muddling Meerkat, por lo que utilizamos varias huellas digitales basadas en investigaciones previas para aislar la posible actividad motivada por el actor. También comparamos esos hallazgos con los informes de abuso que recibimos por correo electrónico. Las consultas de Muddling Meerkat al DNS utilizan diferentes tipos de registros, pero las más inusuales desde el punto de vista de la investigación son las consultas de registros MX para subdominios aleatorios cortos. En el siguiente ejemplo, si el dominio objetivo es dominio.objetivo, la consulta tendría el siguiente aspecto:

```
<rand>dominio.objetivo
```

El término «objetivo» aquí es impreciso, como explicamos en nuestro documento anterior[3], porque el actor se dirige a estos dominios para usarlos en sus campañas, en lugar de atacar a los propietarios del dominio; el actor abusa de estos dominios que no posee con propósito desconocido. Limitamos nuestro análisis de las consultas a aquellas que tenían nombres de host que solo se veían como un subdominio de un solo dominio que servimos y buscamos tendencias. La longitud de los nombres de host observados con carácter único variaba, pero los de tres caracteres eran los más frecuentes; véase la Figura 2. Estos datos concordaban con los recibidos de otros titulares de dominios. También verificamos que las consultas provenían de proveedores de correo de amplio alcance, como Google, y de proveedores de seguridad de correo, como Proofpoint.

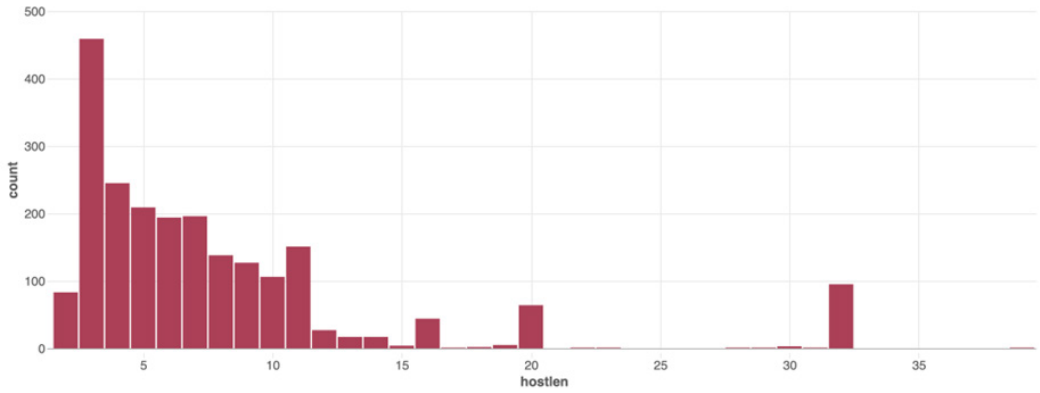

Figura 2. La longitud de los nombres de host observados de manera única en las consultas MX en nuestros servidores DNS autoritativos

Sabiendo que nuestros propios dominios eran utilizados por Muddling Meerkat y suplantados por actores de amenazas que realizaban campañas de malspam, buscamos campañas activas en nuestros filtros de spam.

DETECCIÓN N.º 1: CAMPAÑAS DE PHISHING CON CÓDIGOS QR

El mayor grupo de campañas de phishing que observamos suplantar nuestros antiguos dominios iba dirigido a residentes de China continental. Estas campañas operan de manera persistente desde al menos finales de 2022 y distribuyen archivos adjuntos con un código QR, que redirige a un sitio web de phishing; véase la Figura 3. Según nuestros datos del DNS, informes de abuso e información colateral, creemos que los ataques se originan en China continental. Las campañas emplean una táctica que requiere que el destinatario abra el archivo adjunto del correo electrónico y use WhatsApp para escanear el código QR que contiene. Este método en dos pasos plantea retos adicionales para proteger a los usuarios, ya que el atacante deriva a las víctimas desde el ordenador hacia una aplicación de chat cifrada, lo que sortea muchas de las medidas de seguridad habituales. Los actores de amenazas también emplean algoritmos de generación de dominios registrados (RDGA) para crear dominios aleatorios que permanecen activos solo durante un breve período.

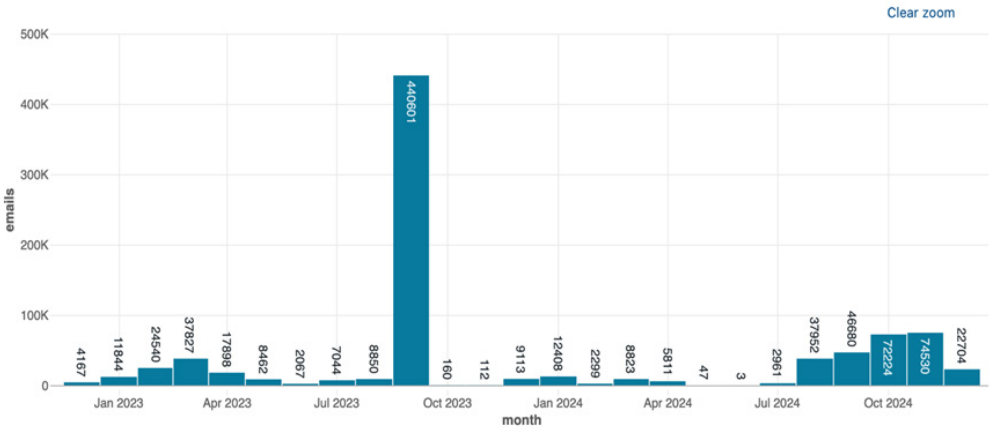

Figura 3. Volumen de correos electrónicos de phishing con códigos QR chinos a lo largo del tiempo

Estas campañas de malspam utilizan dominios de remitente falsificados, que incluyen un gran número de dominios objetivo confirmados como utilizados por Muddling Meerkat, incluidos los nuestros. A través del análisis de spam de estas campañas y la comparación de registros del DNS históricos, ampliamos el número de dominios objetivo que se sabe que son de Muddling Meerkat de aproximadamente 20 en marzo de 2024 a los más de 650 actuales. Las campañas de códigos QR, sin embargo, también contienen muchos dominios que podría estar utilizando Muddling Meerkat, pero que no podemos confirmar a través del DNS.

Estas campañas utilizan direcciones de correo electrónico de remitentes que tenían una estructura coincidente con lo observado en las consultas de Muddling Meerkat al DNS. El nombre de usuario del remitente era una cadena corta y aleatoria con la forma `<rand>@suplantación[.]dominio`. La Tabla 1 muestra un ejemplo de las direcciones de correo electrónico del remitente de la campaña a lo largo del tiempo. Dominios como `jx[.]com` y `hm[.]com` ya eran conocidos como dominios objetivo de Muddling Meerkat.

dm@**jx**[.]**com**	ino@**jjnywnd**[.]**com**
ab@**hm**[.]**com**	gwhy@**isathtooy**[.]**net**
zb@**iizlopn**[.]**com**	atmrp@**kym**[.]**net**
mu@**ibqg**[.]**net**	qivlzn@**kt**[.]**com**
xzu@**iejzhopjx**[.]**org**	atmrp@**kym**[.]**net**
iud@**irnvasa**[.]**net**	

Tabla 1: Muestra de direcciones de remitentes para la campaña de códigos QR; la dirección electrónica del remitente sigue el patrón
<2-9 caracteres aleatorios>@<suplantación[.]dominio>

El correo electrónico suele incluir un anzuelo relacionado con los impuestos en chino mandarín y comenzó en diciembre de 2022 o antes. Estos parecen proceder del espacio de IP chino, principalmente 4134 (Chinanet) y 56046 (China Mobile). La Figura 4 muestra algunas de las líneas de asunto de los mensajes, con su traducción al inglés.

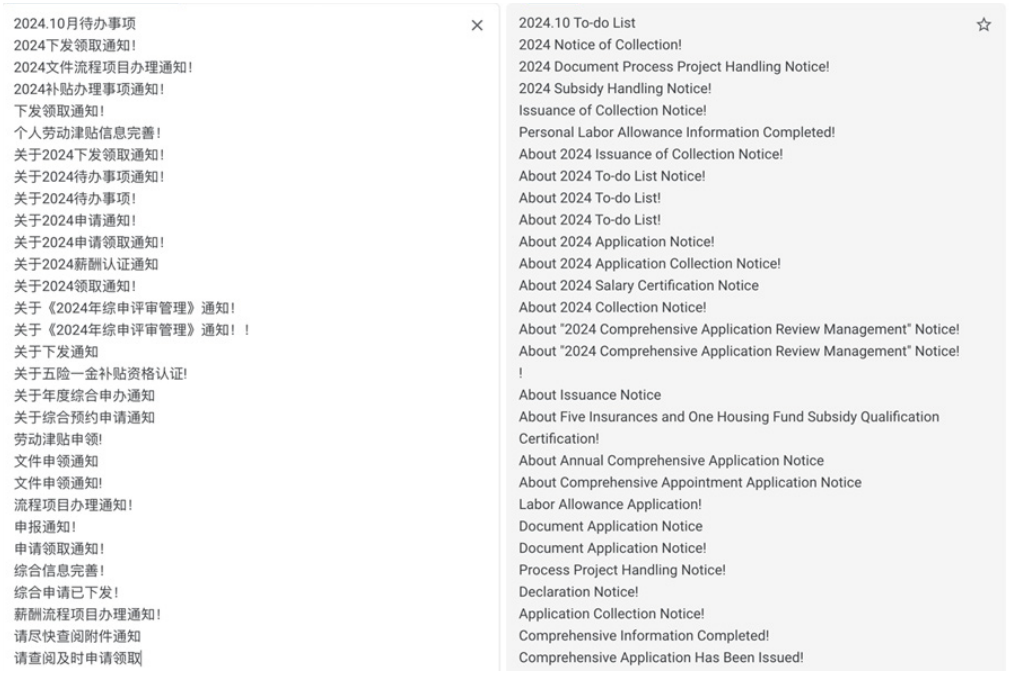

Figura 4: Muestra de asuntos de correo electrónico de la campaña de códigos QR, traducidos al inglés

Otra característica distintiva de este malspam es que la mayoría de los documentos con código QR están cifrados con una contraseña de cuatro dígitos, que se incluye en algún lugar del cuerpo del mensaje, pero no de manera uniforme. A veces está entre paréntesis y otras, delimitada por símbolos. La Figura 5 muestra dos ejemplos de cómo se incluyen las contraseñas en los correos electrónicos.

Figura 5. Dos ejemplos de cómo la contraseña de cuatro dígitos puede variar en valor y formato en diferentes correos electrónicos; los cuadros rojo y verde destacan las diferentes formas en que la contraseña está presente en un correo electrónico

Los archivos adjuntos contienen un código QR con un logotipo incrustado e instrucciones para que el destinatario utilice AliPay/WeChat para escanear el documento; véase la Figura 6. Estos correos electrónicos no son distintos de los que vemos que utilizan los ciberdelincuentes en todo el mundo para explotar a personas vulnerables con promesas de subsidios y beneficios económicos.

Figura 6. Contenido y traducción del archivo adjunto; la parte resaltada incluye la instrucción de usar Alipay/WeChat para escanear el código QR

Los usuarios de Twitter han denunciado el engaño. Según el tuit de la Figura 7, a un usuario se le pidió que introdujera un número de tarjeta e información de identificación tras escanear el código QR. Después, se le indicó que introdujera el importe y el código de verificación, que pensaba que correspondía a un pago enviado a su cuenta. Poco después, un SMS le alertó de que había pagado 590 € de su tarjeta al atacante. ¡Un correo electrónico de spam sin duda rentable!

Figura 7. Tweet de un usuario que fue engañado por la estafa de phishing con código QR

Esta estratagema se basa en dominios de phishing de segunda etapa con una vida útil muy corta, que parecen estar geolocalizados. No tienen resolución en el DNS al cabo de aproximadamente un día y pertenecen a TLD abusados habitualmente, como sbs, shop, life, bond y cn. Estos dominios están formados por un conjunto aleatorio de caracteres, por ejemplo, `aaaefiuibew[.]cn` o `6ttox81[.]sbs`.

No podemos afirmar si esta actividad proviene de Muddling Meerkat o no. Parece más probable que se trate de un sistema común de Phishing-as-a-Service (PhaaS). Aunque las campañas utilizan los dominios relegados que observamos en Muddling Meerkat, parecen suplantar dominios aleatorios en general, incluso algunos que no existen. El actor puede emplear esta técnica para evitar repetir correos electrónicos del mismo remitente. Pese a los esfuerzos por proteger a los usuarios del spam malicioso, algunas de estas suplantaciones rebasan las barreras y son sin duda lo suficientemente rentables como para mantenerlas.

En la Tabla 2 se muestran otros dominios de remitentes vistos en esta actividad.

len2	len3	len4	len5
jt[.]net	iac[.]com	idhs[.]org	ivkpc[.]net
hc[.]com	izr[.]com	jxrn[.]org	jbdct[.]net
kk[.]net	koh[.]com	jirh[.]org	jfctl[.]org
jg[.]com	jwq[.]org	ismh[.]com	irnpc[.]net
kx[.]com	kcy[.]org	ikat[.]com	lahuf[.]net
len6	**len7**	**len8**	**len9**
jxjfwz[.]net	kbgpnek[.]org	jqmyuxk[.]com	hfababhqf[.]org
jxnsdf[.]net	ipcwfrn[.]com	jwruoytd[.]org	jfrcjfqjr[.]com
jwnlhr[.]org	iouwttz[.]com	ktfnmbxa[.]org	jkdduscaj[.]net
kindhy[.]net	jhrzbuk[.]org	jlsiwslr[.]org	jkjiwbpki[.]com
khznrl[.]com	hrggzxa[.]com	hrfliqoj[.]net	kwbjjlygw[.]net

Tabla 2. Ejemplos de dominios suplantados observados en campañas de phishing con códigos QR

Cuando nos dimos cuenta de que las campañas de códigos QR falsificaban dominios que estaban fuera de lo que esperábamos de Muddling Meerkat, regresamos al DNS y a nuestra colección de spam para buscar campañas que pudieran estar asociadas al actor Muddling Meerkat.

DETECCIÓN N.º 2: CAMPAÑAS DE PHISHING JAPONESAS

En nuestros servidores autoritativos del DNS, observamos que un porcentaje inusualmente alto de las consultas relativas al correo incluían nombres de host de tres letras. Mientras intentábamos separar las consultas que podría generar Muddling Meerkat de las atribuibles a escáneres y otras fuentes, el volumen y la uniformidad de estas consultas nos parecieron una buena vía de investigación. Como resultado, buscamos pruebas de spam que tuvieran la misma estructura de consulta.

Detectamos una serie de campañas dirigidas a usuarios japoneses con mensajes que mencionaban marcas populares, como Electronic Toll Collection (ETC, utilizada en las autopistas de todo Japón) y Sumitomo Mitsui Banking Corporation (SMBC, uno de los mayores bancos de Japón), así como Amazon y Mastercard. Los correos electrónicos instan al usuario a iniciar sesión en el servicio debido a un problema de seguridad u otro problema. Un botón incluido en el correo electrónico lleva al usuario a un sistema de distribución de tráfico (TDS) y lo redirige a una página de inicio de sesión falsa, si se cumplen ciertos criterios. Este método es común en la publicidad maliciosa y se utiliza para ocultar la página de destino final y evitar la detección de las empresas de seguridad. La página de inicio de sesión falsa roba las credenciales de la víctima cuando las introduce. La Figura 8 muestra un ejemplo de estos correos electrónicos no deseados.

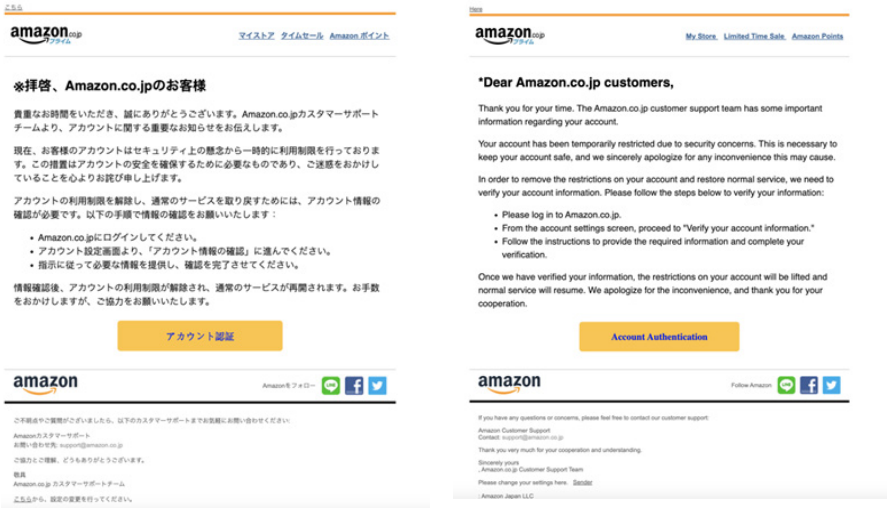

Figura 8. Ejemplo original de correo electrónico no deseado dirigido a usuarios japoneses con advertencias falsas de Amazon y traducción automática del correo

Una vez que el usuario hace clic en el botón «Autenticar cuenta»:

- Se le dirige a `ubrjubf[.]com`, que resuelve a la IP `43.128.150[.]42`
- Luego, se redirige al usuario a un dominio diferente `unpwple[.]com`, que resuelve a la IP `43.133.182[.]243`
- El usuario llega a una página de inicio de sesión falsa para cuentas de Amazon; véase la Figura 9

Figura 9. Página de inicio de sesión en Amazon falsa; referencia de la imagen: https://urlscan.io/result/5c9bbf63-883f-4eab-b4fc-45e2809a8ac2/

Hemos observado distintas variaciones de spam con temática de Amazon, así como anzuelos que utilizan Mastercard y SMBC Vpass.[6] Este actor utiliza una infraestructura de alojamiento dedicado y alterna campañas a lo largo de los mismos dominios y direcciones IP.[7] Las dos direcciones IP dedicadas observadas fueron `43.128.150[.]42` y `43.133.182[.]243`. En la Tabla 3 se incluye una lista de dominios RDGA utilizados en las campañas.

43.128.150[.]42	43.133.182[.]243
eujsubf[.]com, eujsxikw[.]com,	anzcinf[.]xyz, anzconc[.]xyz,
ikhcok[.]com, insjibr[.]com,	infkokf[.]com, omfkiht[.]xyz,
insjkf[.]com, khcpw[.]com,	omfkybg[.]xyz, inybinf[.]com,
maczplw[.]com, maczunf[.]com,	unpwple[.]com, inybubf[.]com,
pknribt[.]com, pknrinf[.]com,	pplaaej[.]com, eccteukx[.]com,
pknrinr[.]com, pknrohv[.]com,	espoeubf[.]com, unpwmlw[.]com,
pknrybg[.]com, pknrynf[.]com,	pplaaeu[.]com, ecctenje[.]com,
ubrjpnf[.]com, ubrjubf[.]com,	unpwibr[.]com, ecctepje[.]com,
unpwinf[.]com, uwkxubs[.]com,	pplaaep[.]com, pplaaea[.]com,
wkxaubf[.]com, wkxaunf[.]com	espoeunf[.]com, espoekwl[.]com

Tabla 3. Muestra de dominios RDGA con direcciones IP dedicadas, utilizados en campañas dirigidas a usuarios japoneses

Al igual que las campañas descritas en la sección anterior, los correos electrónicos de estas campañas utilizan dominios de remitente suplantados, incluidos los dominios pertenecientes a Threat Intel de Infoblox. Además, siguen el formato prevalente en nuestros servidores autoritativos del DNS, con un subdominio de tres caracteres, y en los informes de abuso que recibimos de los proveedores de correo. La Tabla 4 muestra un ejemplo de direcciones de correo electrónico de remitentes.

ak@fdd.**xpv[.]org**	iipnf@gvy.**zxdvrdbtb[.]com**
mh@thq.**cyxfyxrv[.]com**	zmrbcj@bce.**xnity[.]net**
mfhez@shp.**bzmb[.]com**	nxohlq@vzy.**dpyj[.]com**
gcini@vjw.**mosf[.]com**	

Tabla 4. Muestra de direcciones de remitentes de correos electrónicos de phishing japoneses con subdominios de tres letras; los nombres de host de tres letras están coloreados en rojo, mientras que el dominio suplantado está en negrita

Este no fue el único tipo de campaña que observamos dirigida contra usuarios japoneses. Otro anzuelo importante incluía MyEtherWallet, popular cartera de criptomonedas, y utilizaba dominios similares. Los mensajes de spam a veces incluyen texto en japonés, por ejemplo, «(重要なお知らせ) MyEtherWallet ご利用確認のお願い», que significa «[Aviso importante] Solicitud de confirmación del uso de MyEtherWallet», y piden a los usuarios que inicien sesión en su cuenta. Consulte la Figura 10 para ver un ejemplo de correo electrónico en inglés. Aunque el enlace parece ser el sitio web real, en realidad lleva a un dominio similar creado por el actor de amenazas.

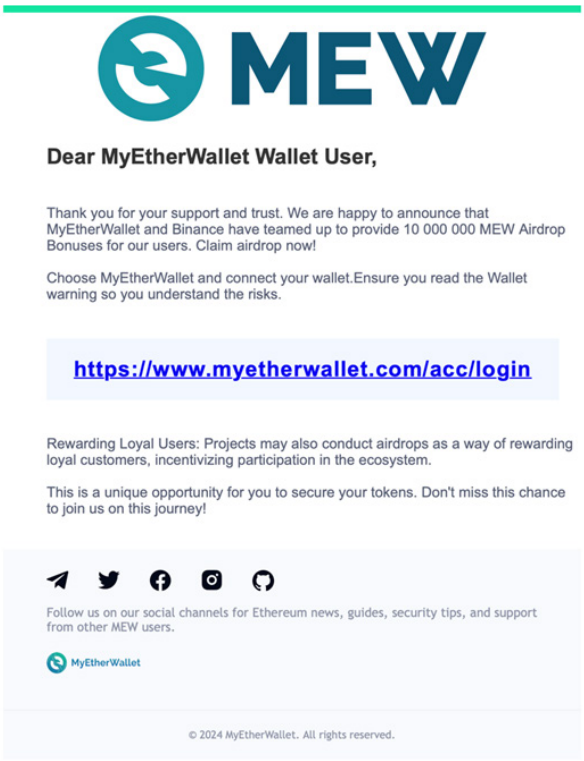

Figura 10. Ejemplo de campaña de spam dirigida a usuarios japoneses; este correo electrónico en particular usaba como asunto «Binance Distribution of MyEtherWallet (MEW) Airdrop» y dirigía al usuario a `myetherwallatak[.]org`

Los dominios similares conducían a una copia idéntica del sitio web MyEtherWallet y se utilizaban para robar las credenciales de los usuarios. Estos dominios utilizan varios TLD diferentes, incluidos .com y .org; consulte la Tabla 5 para ver un ejemplo.

myetherwalletie[.]com	myetherwalletih[.]com	myetherwalletik[.]com
myetherwalletiv[.]com	myetherwalletjp[.]com	myetherwalletrt[.]com
myetherwallettv[.]com	myetherewallet[.]org	myetherswallet[.]org
myetherwallata[.]org		

Tabla 5. Ejemplos de dominios similares utilizados para obtener credenciales de usuarios japoneses mediante phishing

En la campaña de phishing con códigos QR, se observaron los dominios de Muddling Meerkat en la dirección del supuesto remitente, es decir, la dirección de correo electrónico que ve el destinatario. Sin embargo, en la variante japonesa, los dominios se ven en la sección «received from» del mensaje, que se utiliza para la entrega técnica por SMTP. Nos encontramos con otro conjunto de campañas de spam maliciosas que utilizan los mismos dominios observados en las operaciones de Muddling Meerkat, incluido un formato de subdominio similar, pero no podemos verificar que sean obra de Muddling Meerkat. La Tabla 6 proporciona una muestra de los dominios suplantados.

len2	len3	len4	len5
xl[.]com	tgt[.]org	iddm[.]org	fhqqc[.]com
gz[.]net	paf[.]org	yqqb[.]org	mseur[.]com
ed[.]org	bcc[.]com	nvso[.]net	ofddy[.]com
df[.]org	zla[.]com	nqui[.]com	agejx[.]net
wx[.]com	tgf[.]net	duth[.]net	mlngi[.]com
len6	**len7**	**len8**	**len9**
kwwezx[.]net	gbiutoj[.]com	mitsxpjh[.]com	nxbfvjkhr[.]org
bwidqv[.]com	jeihdgt[.]com	wtfmbcvt[.]com	lkhyleslk[.]net
piuxic[.]com	qspdwhc[.]com	jgggzbmq[.]org	nmshofzmh[.]net
xdgzas[.]com	grjfgpw[.]net	qqegowhv[.]org	ykbhnoers[.]com
nwfffu[.]org	vudgfcm[.]net	invphyzf[.]com	mqnbqsygn[.]org

Tabla 6. Ejemplos de dominios suplantados observados en las campañas de MyEtherWallet

Una de las varias lagunas en la comprensión de estas campañas es que el número de dominios descubierto probablemente sea demasiado pequeño como muestra para validar que todos los dominios coincidan con Muddling Meerkat. Sin embargo, este conjunto de campañas es otro ejemplo de cómo utilizan los actores de amenazas vinculados a China la suplantación de dominios en sus operaciones de spam.

Con eso, nos dirigimos de nuevo a los filtros de spam.

DETECCIÓN N.º 3: CAMPAÑAS DE EXTORSIÓN CONOCIDAS

No solo detectamos suplantación de dominios en el código QR y en las campañas en japonés, sino también en campañas que explotaban conocidas técnicas de spam. Los correos electrónicos de extorsión que afirman que un hacker ha accedido al dispositivo del usuario y ha grabado actividades comprometedoras son un clásico en el ámbito del malspam. Nos sorprendió un poco descubrir que también utilizan dominios de remitente suplantados, pero con una novedad: el actor falsifica la dirección de correo electrónico del propio usuario y lo insta a que la verifique. El correo electrónico informa al usuario de que su dispositivo ha sido comprometido y, como prueba, el actor alega que el mensaje ha sido enviado desde la propia cuenta del usuario. Y, sin embargo, no es así; los encabezados de correo muestran que llega a través de direcciones IP chinas, no del usuario. Consulte la Figura 11 a continuación para ver un ejemplo del contenido del correo electrónico.

El correo electrónico solicita al usuario que envíe un pago al remitente a cambio de eliminar el malware de su dispositivo e incluye la dirección de una billetera de Bitcoin, que varía en los distintos mensajes de spam. No sabemos si se trata de un servicio de extorsión o si el mismo actor utiliza varias carteras. En los ejemplos que hemos recopilado, se pide a las víctimas que paguen 1.800 USD. Aunque pueda parecer sorprendente que muchos usuarios lean realmente estos correos electrónicos de spam, y aún más que actúen en consecuencia, la estafa aparentemente funciona. Al revisar el saldo de estas carteras con `bitref[.]com`, vimos que contenían fondos significativos; en una había casi 26.000 USD.

```
¡Muy buenas! Por desgracia, tengo malas noticias para ti. Hace un
tiempo, tu dispositivo se infectó con mi troyano privado, R.A.T (Remote
Administration Tool). Si quieres saber más al respecto, búscalo en Google.
El troyano me permitió acceder a tus archivos, a tus cuentas y a tu cámara.
Comprueba el remitente de este correo, lo he enviado desde tu misma cuenta
de correo. Para asegurarte de que lees este mensaje, lo recibirás varias
veces. Sin duda te gusta acceder a webs porno y ver vídeos guarros, mientras
te diviertes como perversiones. ¡TE GRABÉ (con la cámara de tu equipo)
TOCÁNDOTE! Después eliminé el malware para no dejar rastro alguno. Si dudas
de si hablo en serio, recuerda que me bastan un par de clics para compartir
el vídeo en el que sales con tus amigos, familiares, todos tus contactos
de correo electrónico, en las redes sociales y en la darknet. Todo lo que
te pido es una transferencia de 1800 USD en Bitcoin (BTC) a mi cuenta. Una
vez realizada la transacción, procederé a borrarlo todo. Ten por seguro que
cumplo mis promesas. Puedes comprar fácilmente Bitcoin (BTC) aquí: https://
cex.io/buy-bitcoins https://nexo.com/buy-crypto/bitcoin-btc https://bitpay.
com/buy-bitcoin/?crypto=BTC https://paybis.com/ https://invity.io/buy-crypto o
sencillamente buscar en Google otra plataforma de compraventa. Después envía
el importe en Bitcoin (BTC) directamente a mi cartera, o instala el software
gratuito Atomicwallet, o: Exodus wallet, recíbelo y envíalo a mi cartera.
Mi dirección de Bitcoin (BTC) es: 1GtGZpzfRkAVBL48F68mi8bTcatwpTZGm8 Sí, así
es la dirección, copia y pega mi dirección, distingue entre mayúsculas y
minúsculas. Tienes 3 días como máximo desde el momento en que abras este
correo electrónico. Como tengo acceso a tu cuenta, sabré si has leído el
correo o no. Todo el proceso será justo e imparcial. Te doy un consejo:
cambia con regularidad todas las contraseñas de tus cuentas y actualiza tu
equipo con los parches de seguridad más recientes.
```

Figura 11. Ejemplo de spam de extorsión con dominios de remitentes suplantados

Es probable que estas campañas, y posiblemente muchas otras que utilizan dominios de remitentes suplantados, se originen en bots de spam persistentes. Como mínimo, los atacantes no validan las direcciones de correo electrónico de las víctimas para asegurarse de que reciban o lean sus mensajes. Hay casos en los que la dirección de correo electrónico del destinatario estaba asociada a uno de nuestros dominios, que alojó contenido por última vez en 2007 y no había tenido usuarios de correo electrónico en más de 15 años. No hay registros de infiltraciones capaces de explicar por qué se activaron esos correos electrónicos y desconocemos si, en realidad, esos usuarios existieron alguna vez.

Esta y otras campañas de spam similares que hemos detectado recuerdan a los cañones de spam abandonados a la deriva en el espacio de internet. También observamos la transmisión de gusanos antiguos, otra señal de los restos de botnets que quedaron en funcionamiento mientras los remitentes de malspam avanzaban hacia técnicas como los códigos QR y las páginas de inicio de sesión falsas como las que hemos visto antes. Estas campañas, ahora probablemente en piloto automático, parecen ser más reminiscencias que el resultado reciente de un actor sofisticado como es Muddling Meerkat.

INCIDENTE Nº 4: MALSPAM MISTERIOSO

Todo este programa de investigación comenzó con un misterio, y concluiremos este artículo con otro: una campaña de spam muy activa que utiliza dominios de remitentes suplantados e incluye archivos adjuntos con hojas de cálculo de Excel aparentemente inocuas, sin finalidad evidente. No podemos explicar la razón de ser de estos correos, que suplantan los mismos tipos de dominios que utiliza Muddling Meerkat.

Estos correos electrónicos supuestamente provienen de **上海亚凯**, que se traduce como «Shanghai Yakai», el nombre de una empresa de transporte china. Las direcciones de correo electrónico son variopintas e incluyen nombres de usuario sintéticos como «Edward.Evelyn» y «Heidi.Gracie». Las campañas se observaron en dos de cada tres días en 2024, sin variaciones. La línea de asunto indica que el correo electrónico contiene nuevas actualizaciones de tarifas de flete y se adjunta una hoja de cálculo con un solo nombre: **上海亚凯国际运价表**.xlsx. No hemos encontrado contenido malicioso en estos archivos.

No hay llamada a la acción (CTA) en el correo electrónico. A todas luces, es simplemente un conjunto de tarifas de flete de una naviera china que se actualiza continuamente. Pero, ¿con qué propósito? Estos correos electrónicos no parecen enviarse a clientes que hayan olvidado cambiar su dirección de correo electrónico o darse de baja. El uso de la suplantación de dominios elimina cualquier resquicio de legitimidad y no está claro por qué una empresa de transporte o un actor malicioso enviaría correos electrónicos como estos. La Tabla 7 muestra un ejemplo de los dominios remitentes.

len4	len5	len6	len7
igeb[.]net	accou[.]com	axegal[.]com	awpking[.]com
kwfm[.]com	drsmj[.]com	devsmx[.]com	comitis[.]com
pqhh[.]com	eddim[.]com	glypix[.]com	donmenn[.]com
rrbc[.]com	hetoo[.]com	gulart[.]net	fundsle[.]com
tkee[.]net	horek[.]com	jomila[.]net	karnege[.]com
tnmc[.]com	memsz[.]com	mzylla[.]com	mtrplay[.]com
ukei[.]net	svard[.]net	okayme[.]com	rajprem[.]com
utpz[.]com	tapli[.]net	theiwl[.]com	techsox[.]com
vbhh[.]com	uweko[.]com	vaites[.]com	tjipbpo[.]com
wuwo[.]com	youbi[.]com	ynglet[.]com	wulthur[.]net

Tabla 7. Muestra de dominios de remitentes suplantados utilizados en el spam del flete de Shanghai Yakai.

Se observó una técnica de campaña similar en el spam personal, pero en lugar de mensajes de una empresa de transporte, el correo electrónico proporciona valores de fondos de inversión de una empresa india. Estos mensajes, que Google Mail marca como sospechosos de spam, también contienen una hoja de cálculo inocua y un archivo PDF. En este caso, el nombre de usuario del remitente es un antiguo conocido, y parece probable que su cuenta de correo electrónico haya sido hackeada en algún momento para utilizarla en operaciones de spam. Sin embargo, al igual que el spam del flete chino, no está claro qué valor aportan estos mensajes al remitente de spam.

VISTA DESDE EL SERVIDOR AUTORITATIVO DEL DNS

Muddling Meerkat efectúa operaciones extrañas en el DNS desde hace más de seis años. Estas operaciones incluyen respuestas falsas del Gran Cortafuegos chino y el uso de dominios relegados fuera de su control. Aunque su actividad en el DNS incluye varios tipos de registros, las respuestas falsas son de registros MX del dominio base u objetivo. Por ejemplo, se observan respuestas del DNS con registros MX para `kb[.]com` desde direcciones IP chinas, aunque `kb[.]com` no tiene registros MX. Además, estos registros falsos incluyen un nombre de host corto y aleatorio que solo se observa una vez, por ejemplo, `x4rd.kb[.]com`, que podría ser un registro MX observado para `kb[.]com`. Cuando lo publicamos por primera vez en marzo de 2024, habíamos identificado unos 20 dominios de este tipo, pero ahora hemos confirmado varios cientos más.

Además de buscar pruebas de operaciones de spam por parte del actor, también analizamos los registros del DNS en nuestros servidores autoritativos y tratamos de compararlos con las respuestas de DNS falsas observadas en los datos colaterales de los dominios de nuestra propiedad. La hipótesis era que, si podíamos ver una consulta para uno de los dominios de registro MX falsos, por ejemplo, `x4rd[.]nuestro[.]dominio`, podríamos utilizar la dirección IP del consultante para entender mejor las operaciones de Muddling Meerkat. Por desgracia, no pudimos asociar los registros de Muddling Meerkat con las consultas a nuestros servidores.

¿Qué significa que no se pueden asociar? En realidad, implica que quien sea que reciba las respuestas MX falsas, por ejemplo, `x4rd[.]nuestro[.]dominio`, no utiliza esas respuestas en ninguna consulta posterior al DNS y no parece usarlas para spam. Esta ausencia de un motivo claro desacredita la noción de que un botnet reciba dominios para usar en correos electrónicos suplantados. Entonces, ¿para qué se utilizan las respuestas? Ni idea. Muddling Meerkat sigue siendo un misterio. ¿Tiene alguna idea o una perspectiva diferente? Somos todo oídos.

CONCLUSIÓN

No pudimos determinar a qué se dedica Muddling Meerkat, pero nuestra investigación dio frutos: aprendimos mucho sobre la forma en que los actores utilizan dominios suplantados para malspam, lo que puede servir de base para ponerles fin. Para los investigadores de amenazas como nosotros, esa información es a menudo tan importante como conocer las intenciones subyacentes.

Uno no siempre puede conseguir lo que quiere, pero tal vez descubra que ha conseguido lo que necesita.[8]

THREAT INTEL DE INFOBLOX

Threat Intel de Infoblox es la principal iniciativa de inteligencia sobre amenazas del DNS, cuya originalidad la distingue entre un mar de agregadores. ¿Qué nos diferencia? Dos cosas: increíbles habilidades en DNS y una visibilidad incomparable. El DNS es muy difícil de interpretar y detectar, pero nuestros profundos conocimientos y nuestro acceso exclusivo nos proporcionan una potente herramienta para detectar las ciberamenazas. Somos proactivos más que defensivos y utilizamos nuestros conocimientos para erradicar la ciberdelincuencia de raíz. Además, creemos en la puesta en común de los conocimientos para ayudar a la comunidad de seguridad en general, por lo que damos a conocer investigaciones detalladas y publicamos indicadores en GitHub. Por otra parte, nuestra información se integra a la perfección en las soluciones de detección y respuesta del DNS de Infoblox, por lo que nuestros clientes se benefician de ella automáticamente, además de contar con tasas de falsos positivos despreciables.

Sede corporativa
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054 (EE. UU.)

+1.408.986.4000
www.infoblox.com

Versión: 20241223v1