Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Múltiples ataques de Smishing a grandes organizaciones.

12/Agosto/2022

Contenido

INTRODUCCIÓN

La finalidad de este boletín es poder informarle a usted sobre campañas de Phishing mediante mensajes de texto (Smishing) que se están realizando contra industrias conocidas mundialmente de forma exitosa, esperamos que esta información sea de alta utilidad en su entorno.

MÚLTIPLES CASOS DE SMISHING.

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2022_08_12_01
Clasificación de alerta:	Noticia
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	08/12/2022
Es día cero (0 day):	NO

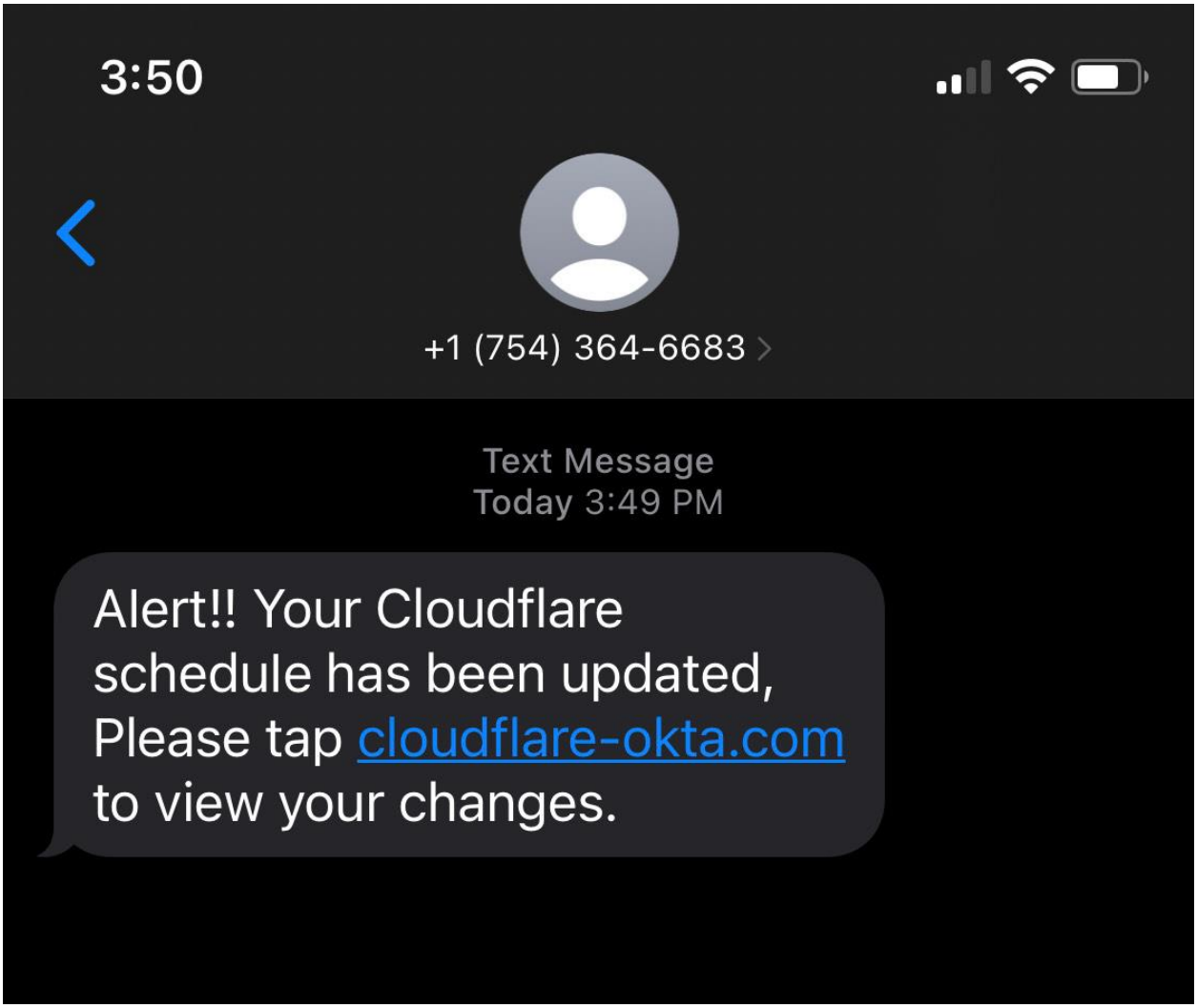
RESUMEN

A continuación, se presentan 3 casos recientes de Smishing que han significado un alto impacto en las organizaciones afectadas, se detallaran entidad por entidad.

CLOUDFLARE

El 20 de julio de 2022, el equipo de seguridad de Cloudflare recibió informes de empleados que recibieron mensajes de texto de aspecto legítimo que apuntaban a lo que parecía ser una página de inicio de sesión de Cloudflare Okta. Los mensajes comenzaron el 2022-07-20 a las 22:50 UTC. En el transcurso de menos de 1 minuto, al menos 76 empleados recibieron mensajes de texto en sus teléfonos personales y laborales. También se enviaron algunos mensajes a los familiares de los empleados. Todavía no se ha podido determinar cómo el atacante reunió la lista de números de teléfono de los empleados, pero se ha revisado los registros de acceso a nuestros servicios de directorio de empleados y Cloudflare confirma no haber encontrado signos de compromiso.

Los mensajes de texto recibidos por los empleados se veían así:



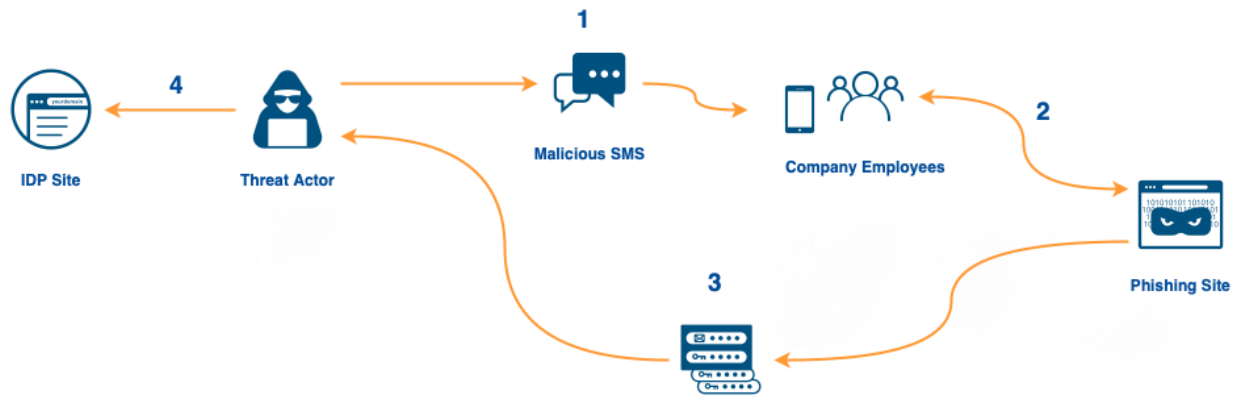
Provenían de cuatro números de teléfono asociados con tarjetas SIM emitidas por T-Mobile: (754) 268-9387, (205) 946-7573, (754) 364-6683 y (561) 524-5989. Señalaron un dominio de aspecto oficial: cloudflare-okta.com. Ese dominio se había registrado a través de Porkbun, un registrador de dominios, el 20 de julio de 2022 a las 22:13:04 UTC, menos de 40 minutos antes de que comenzara la campaña de phishing.

Suplantación de identidad en tiempo real

Cloudflare pudo analizar la carga útil del ataque de phishing en función de lo que recibieron sus empleados, así como el contenido publicado en servicios como VirusTotal por otras empresas que habían sido atacadas. Cuando una víctima completaba la página de phishing, las credenciales se transmitían inmediatamente al atacante a través del servicio de mensajería Telegram. Esta retransmisión en tiempo real era importante porque la página de phishing también solicitaría un código de contraseña de un solo uso basado en el tiempo (TOTP).

Presuntamente, el atacante recibiría las credenciales en tiempo real, las ingresaría en la página de inicio de sesión real de la empresa víctima y, para muchas organizaciones, generaría un código que se enviaría al empleado por SMS o se mostraría en un generador de contraseñas. Luego, el empleado ingresaría el código TOTP en el sitio de phishing y también se lo transmitiría al atacante. El atacante podría entonces, antes de que caducara el código

TOTP, usarlo para acceder a la página de inicio de sesión real de la empresa, derrotando a la mayoría de las implementaciones de autenticación de dos factores.



Se confirmo que tres empleados de Cloudflare cayeron en el mensaje de phishing e ingresaron sus credenciales. Sin embargo, Cloudflare no usa códigos TOTP. En cambio, cada empleado de la empresa recibe una clave de seguridad compatible con FIDO2 de un proveedor como YubiKey. Dado que las claves físicas están vinculadas a los usuarios e implementan el enlace de origen , incluso una operación de phishing en tiempo real sofisticada como esta no puede recopilar la información necesaria para iniciar sesión en cualquiera de sus nuestros sistemas. Si bien el atacante intentó iniciar con las credenciales de nombre de usuario y contraseña comprometidas, no pudo superar el requisito de la clave física.

Pero esta página de phishing no buscaba simplemente credenciales y códigos TOTP. Si alguien superaba esos pasos, la página de phishing iniciaba la descarga de una carga útil de phishing que incluía el software de acceso remoto de AnyDesk. Ese software, si se instala, permitiría a un atacante controlar la máquina de la víctima de forma remota.

Acciones de Respuesta:

Bloquear el dominio de phishing con Cloudflare Gateway

Identificar a todos los empleados de Cloudflare afectados y restablecer las credenciales comprometidas

Identificar y eliminar la infraestructura de los actores de amenazas

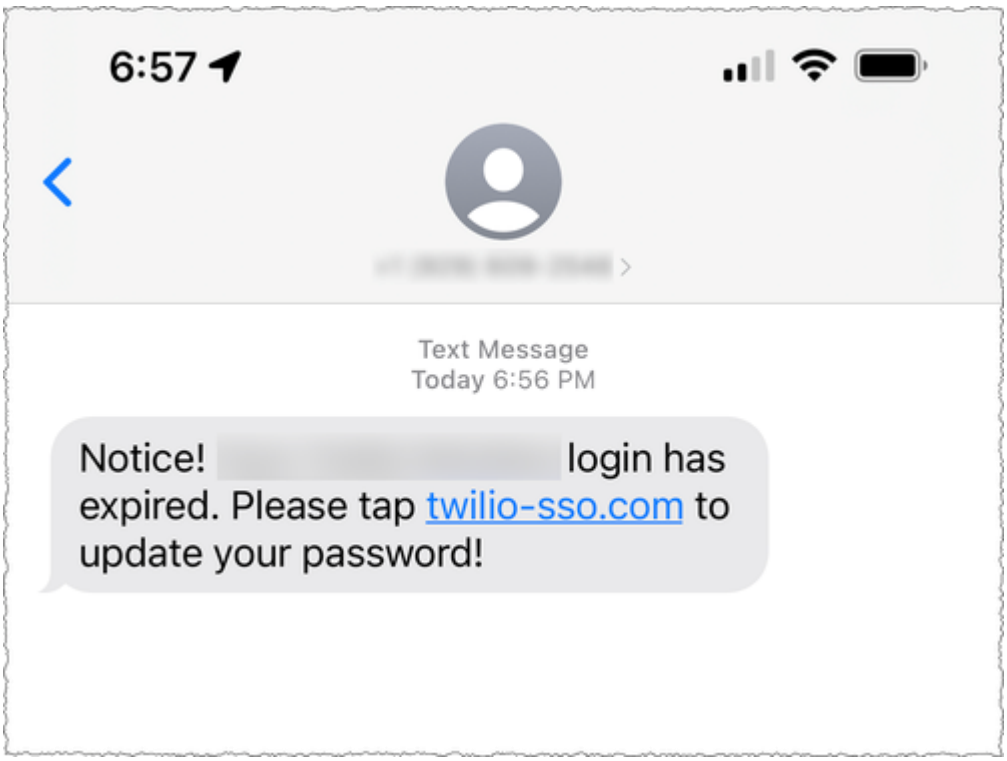
Actualizar los indicadores para identificar cualquier intento de ataque posterior

Auditoría de registros de acceso al servicio para cualquier indicación adicional de ataque.

Twilio

El 4 de agosto de 2022, Twilio se dio cuenta del acceso no autorizado a la información relacionada con un número limitado de cuentas de clientes de Twilio a través de un sofisticado ataque de ingeniería social diseñado para robar las credenciales de los empleados. Este amplio ataque contra sus empleados logró engañar a algunos empleados para que proporcionaran sus credenciales. Luego, los atacantes usaron las credenciales robadas para obtener acceso a algunos sistemas internos, donde pudieron acceder a ciertos datos de los clientes.

Más específicamente, los empleados actuales y anteriores informaron recientemente que recibieron mensajes de texto que pretendían ser del departamento de TI. Los cuerpos de texto típicos sugerían que las contraseñas de los empleados habían caducado o que su horario había cambiado y que necesitaban iniciar sesión en una URL que controla el atacante. Las URL usaban palabras como "Twilio", "Okta" y "SSO" para tratar de engañar a los usuarios para que hicieran clic en un enlace que los llevaba a una página de destino que se hacía pasar por la página de inicio de sesión de Twilio. Los mensajes de texto se originaron en las redes de operadores estadounidenses. Además, los actores de amenazas parecían tener habilidades sofisticadas para hacer coincidir los nombres de los empleados de las fuentes con sus números de teléfono.



Acciones ejecutadas por Twilio

Una vez que Twilio confirmó el incidente, revocó el acceso a las cuentas de los empleados comprometidos para mitigar el ataque. Contrató a una firma forense líder para ayudar en su investigación en curso.
Volvió a enfatizar su capacitación en seguridad para garantizar que los empleados estén en alerta máxima ante ataques de ingeniería social, y han emitido avisos de seguridad sobre las tácticas específicas que utilizan los actores malintencionados desde que comenzaron a aparecer hace varias semanas.

Como los actores de la amenaza pudieron acceder a un número limitado de datos de cuentas, se ha notificado a los clientes afectados de forma individual con los detalles.

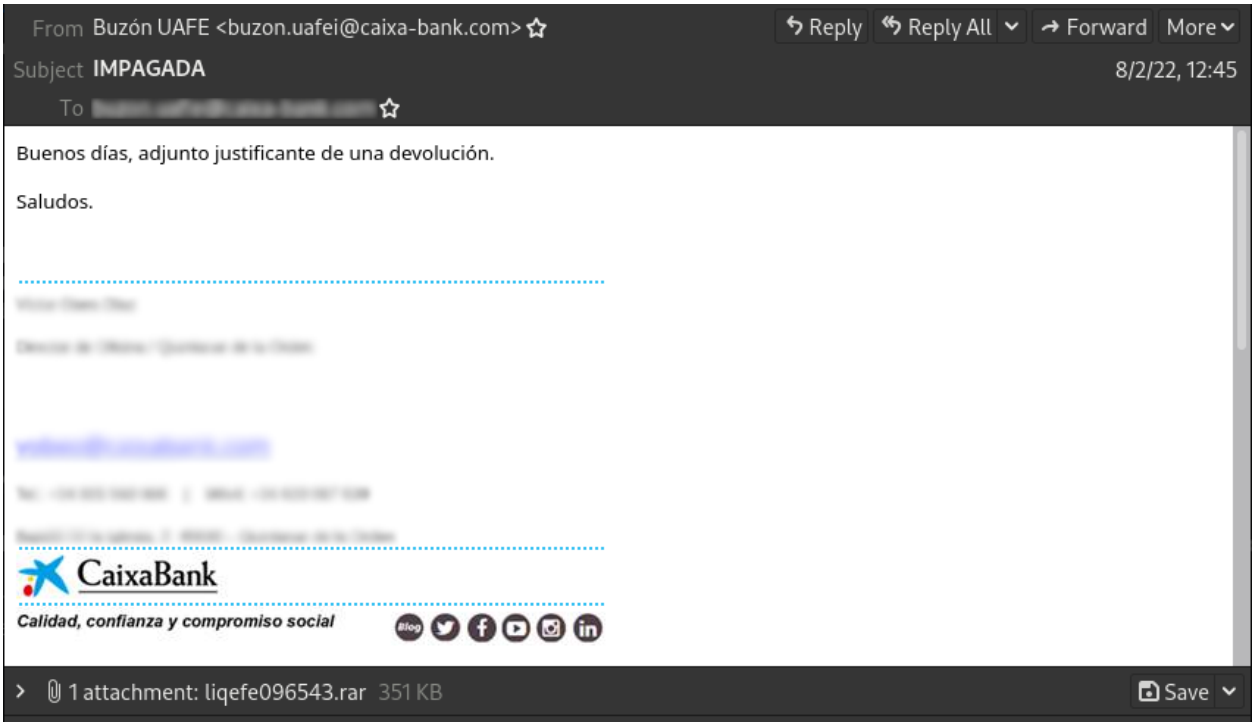
Actualmente este caso continúa bajo investigación y se publicaran los nuevos hallazgos aquí.

CAIXABANK

A inicio del mes de agosto, el equipo de Avast Threat Labs advirtió sobre una campaña de correo electrónico malicioso (malspam) en España, dirigida específicamente a usuarios de CaixaBank. Desde julio de 2022, el equipo de Avast ha bloqueado más de 7.000 intentos de ataque.

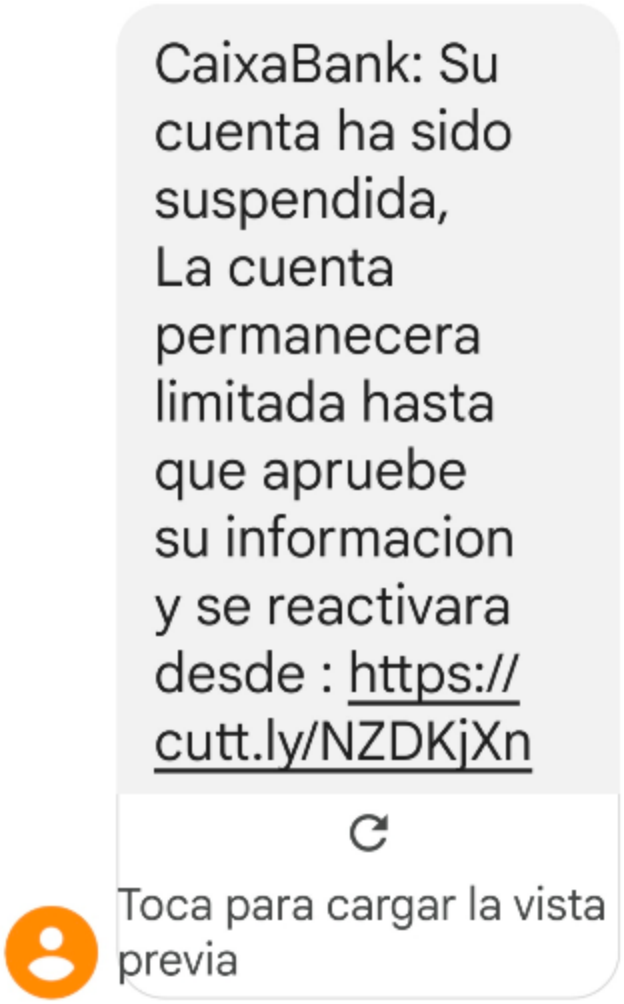
Estos correos malspam se envían desde las siguientes direcciones de correo electrónico: Buzón UAFE <buzon.uafei@caixa-bank.com>, y Buzón UAFE <buzon.uafe@ caixa-bank. com>, bajo la línea de asunto "IMPAGADA" e incluyen un archivo adjunto llamado liqefe096543.rar, que ejecuta un archivo llamado liqefe096543.ex, el cual es un malware llamado Guloader. Este malware descarga el software espía AgentTesla, que tiene la capacidad de robar contraseñas, tomar capturas de pantalla, robar información de la computadora de la víctima y descargar más malware.

La siguiente captura de pantalla, es un claro ejemplo de esta campaña de malspam donde podemos ver el remitente y asunto mencionado anteriormente, así como un archivo adjunto incluído en el correo electrónico. En este caso, podemos ver que los atacantes se hacen pasar por CaixaBank utilizando el logo y una dirección de correo electrónico que hacen que parezca real, sin embargo, no lo es.



Tras publicar este caso en las diferentes redes sociales de Avast, así como diversos medios digitales en España para advertir a los usuarios de CaixaBank, se nota creciente preocupación de los españoles por la privacidad y seguridad de sus datos bancarios. Incluso, un usuario hizo llegar una captura de pantalla y ha permitido compartirla para ayudar a difundir esta estafa.

A continuación, podemos ver una estafa smishing (phishing vía sms o mensaje de texto) donde supuestamente se advierte que la cuenta del usuario de CaixaBank ha sido suspendida y es necesario ingresar sus datos para reactivarla a través de un enlace:



RECOMENDACIONES

- Realizar capacitaciones de forma continua a su personal sobre detección y reporte de Phishing.
- Asegúrese que ningún usuario cuente con permiso para instalar software en su endpoint asignado, todo debe ser monitoreado y aprobado por el departamento de IT.
- Valide que su Anti-Spam cuente con integraciones a fuentes externas con actualización constante que le permitan mejorar la detección de Spam y Phishing.
- Si su empresa no utiliza servicios de mensajería de texto para enviar notificaciones o códigos a su personal, hágales saber que todo mensaje de este tipo es un intento de estafa y debe ser reportado.
- Recomendar a su personal que en redes sociales no tengan publica su información laboral (Por ejemplo, la empresa en la que laboran y su puesto).

Noticia Completa

https://devel.group/multiples-ataques-de-smishing-a-grandes-organizaciones/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757
El Salvador: +(503) 2249 4252
Honduras: +(504) 2283 5904
República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente