AXUR

EBOOK

Ataques a la autenticación multifactor

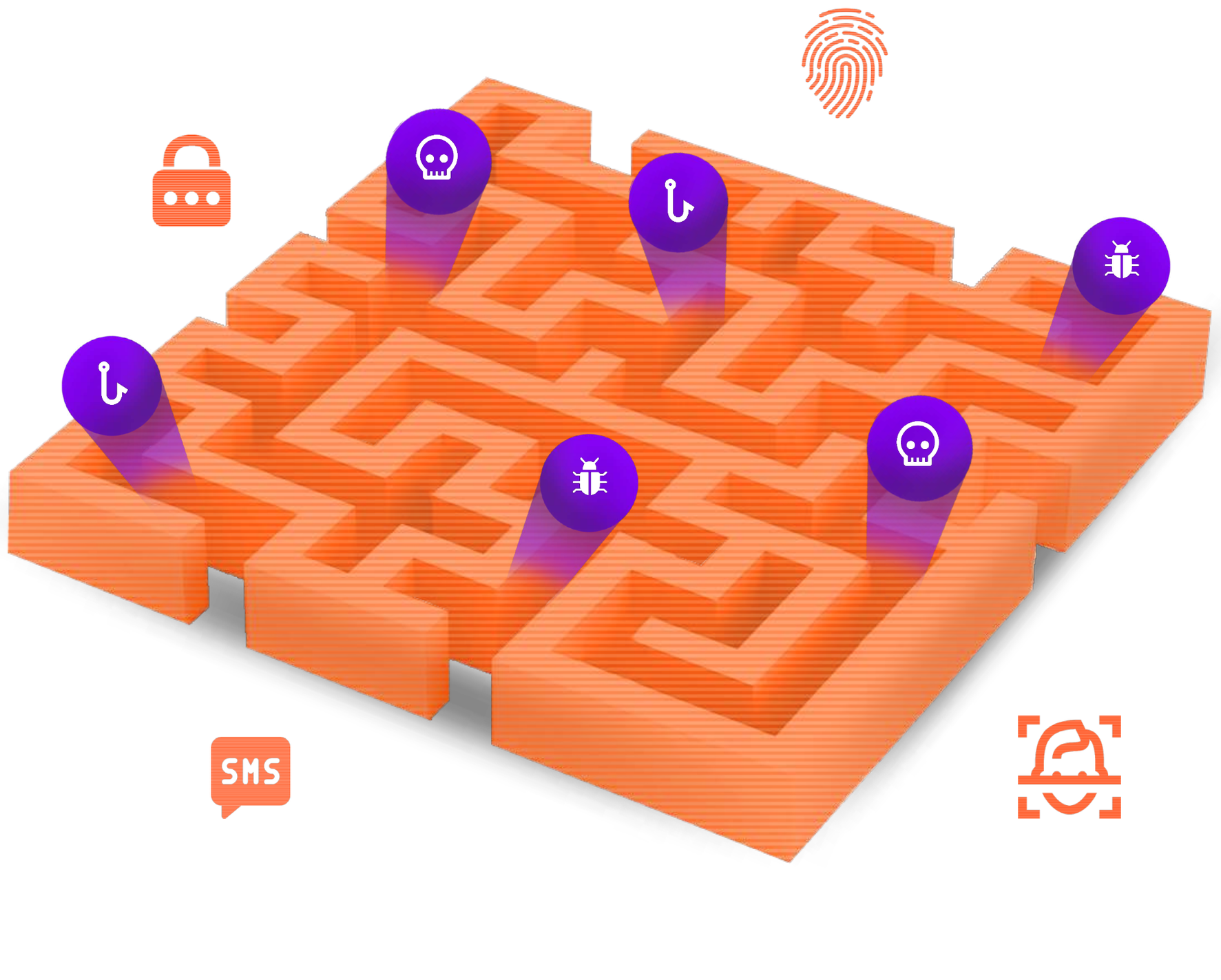
Los ciberdelitos evolucionan en sus tácticas y lanzan nuevos mecanismos que burlan los sistemas de protección. conozca cómo funcionan estos ataques y sepa cómo protegerse de ellos.

Temas desarrollados en éste informe

Definición de MFA

MFA	**Multi-factor authentication:** es **la autenticación multifactor**. Es un **proceso de autenticación** por el cual el acceso al sistema se concede sólo si el usuario presenta más **de un factor o prueba de identidad**. En un intento de preservar las iniciales del término en inglés, algunas definiciones en español lo traducen como "multifactor de autenticación".
2FA	Cuando se exigen sólo dos factores, es común usar la sigla 2FA (two-factor authentication)

Resumen ejecutivo



La administración de identidades constituye uno de los grandes desafíos de la seguridad de la información. Frente a la debilidad del proceso tradicional de autorización con nombre de usuario y contraseña, muchas empresas han migrado sus servicios hacia una autenticación más robusta y con múltiples factores.

Los primeros resultados de la autenticación multifactor han sorprendido, después de bloquear numerosas técnicas de irrupción. Aún hoy, la simple existencia de un segundo factor de autenticación continúa obstaculizando los ataques menos sofisticados.

Por otro lado, no podemos permitir que este éxito aparente se transforme en una trampa que nos impida ver que existen ataques que están venciendo la autenticación multifactor.

Algunos mecanismos de autenticación que antes eran considerados robustos (como el envío de SMS) hoy resultan insuficientes y, según la Agencia de Ciberseguridad e Infraestructura de los Estados Unidos (CISA), ya no integran el "patrón oro" de la autenticación multifactor. Depender exclusivamente de mecanismos más débiles es exponerse a un riesgo mayor al que se imagina.

El phishing fue reinventado para funcionar contra la MFA, y los delincuentes desarrollaron nuevas categorías de malware dedicadas a robar sesiones autorizadas y sacar provecho de las brechas que aparecen al implementar la autenticación. En 2022, dos proveedores de soluciones de MFA sufrieron invasiones, con violaciones a la seguridad de las cuentas, y filtración de las brechas en las redes de telecomunicaciones que entregan códigos de un solo uso.

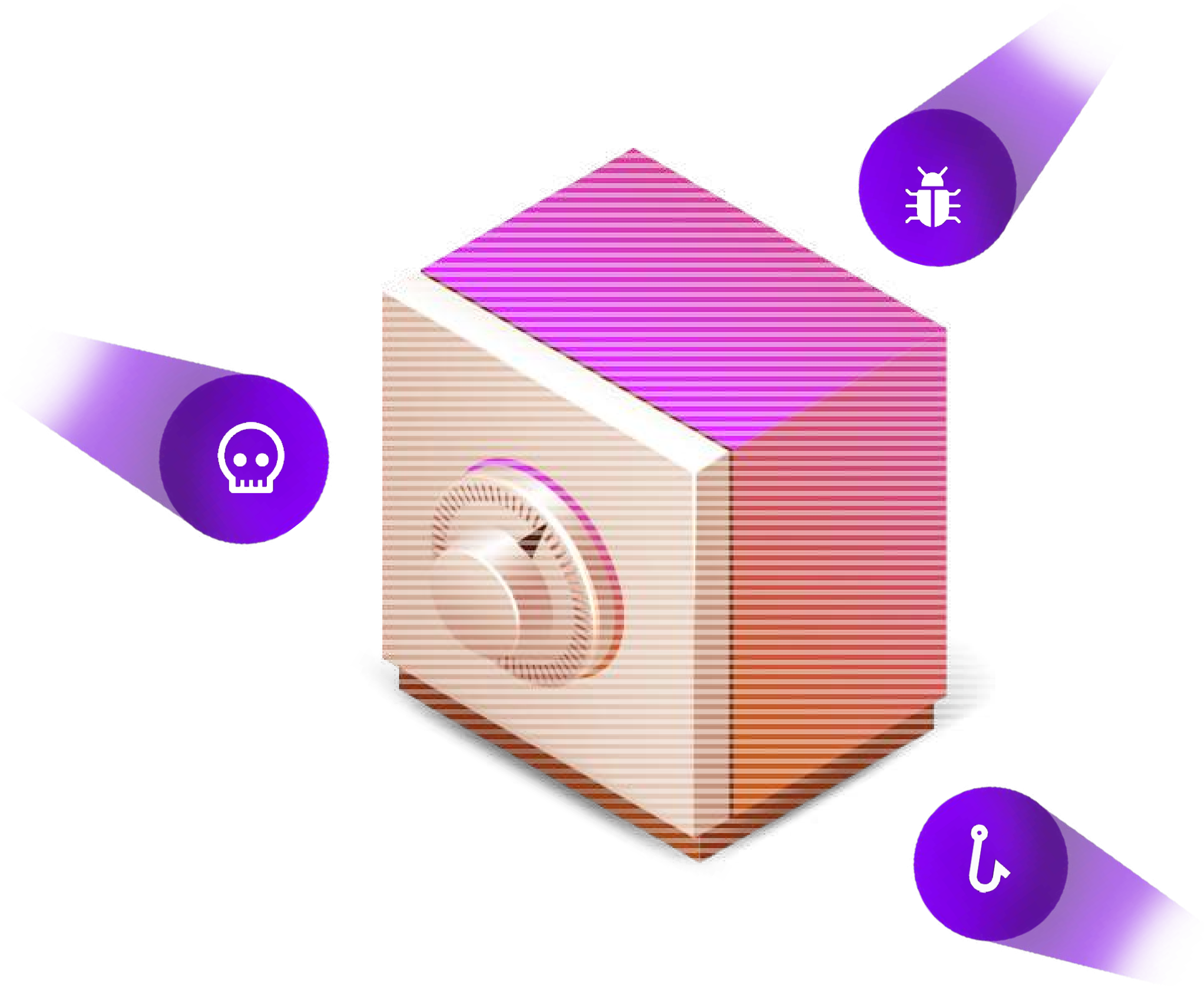
Los prestadores de servicios digitales, que ofrecen la autenticación multifactor a sus usuarios, enfrentan mayores obstáculos aún. No existe visibilidad sobre las prácticas de seguridad del usuario, y no resulta muy efectivo apostar a su concientización. Dejar de ofrecer mecanismos de autenticación cómodos, como el SMS, puede generar que el usuario abandone totalmente la MFA, y esto debilitaría más aún la seguridad de la cuenta.

Este documento muestra el funcionamiento de los ataques, cita ejemplos de usos y sugiere la utilización del monitoreo de credenciales filtradas como un modo simple de mejorar la confiabilidad del proceso de autenticación, cuya integración al ecosistema se ve facilitada al no depender de ningún cambio en el proceso de autenticación ya existente.

Tampoco el monitoreo depende de la visibilidad sobre las prácticas del usuario, lo cual evita contratiempos. Además, el acceso a la información filtrada proporciona medios para que la organización detecte filtraciones y pueda bloquear los accesos indebidos, e incluso proteger las cuentas de e-mail usadas para recuperar información en los sistemas de MFA.

Luego de describir este escenario, se hace evidente que el monitoreo puede ayudar a mitigar las vulnerabilidades de la MFA e interrumpir invasiones que resulten en acciones de ransomware, filtración de datos y pérdidas financieras para la empresa.

La importancia de las credenciales y de la MFA



Antes de abordar las aplicaciones y limitaciones de la autenticación multifactor, haremos referencia a los motivos por los cuales es necesario prestar atención al proceso de autenticación. Sabemos que los agentes maliciosos pueden usar las credenciales para acceder a los sistemas corporativos, pero son dos las cuestiones que vuelven esta amenaza más preocupante: la debilidad de la propia credencial y la relación indirecta y amplia que esta puede tener con la totalidad del ecosistema de la empresa.

En el caso del sistema de nombre de usuario y contraseña tradicional, sin factores adicionales, la protección depende totalmente de la contraseña. Este escenario presenta varios riesgos:

- **La elección de la contraseña depende del usuario.** No siempre la credencial elegida es lo bastante fuerte y, aunque el sistema imponga ciertas reglas en lo que respecta al tamaño de la contraseña y los tipos de caracteres necesarios, los controles son insuficientes. El usuario también puede elegir contraseñas de índole especial (que contengan fechas, nombres de familiares, de mascotas, entre otros), o repetir contraseñas usadas en otros sistemas (inclusive cuentas de servicios personales) que hayan sido previamente atacadas por agentes maliciosos.

- **La contraseña puede haber sido almacenada en un lugar inseguro**. Así sea una anotación en un papel, un e-mail dejado en una cuenta personal o una foto guardada en el celular, es poco probable asegurar que no haya habido alguna violación a la política de seguridad que debilite la contraseña del usuario.
- **Se puede robar la contraseña a partir del malware, phishing y otros ataques**. Aunque la contraseña sea fuerte y no esté almacenada en un lugar inseguro, el usuario también puede ser atacado directamente.
- **Acceso universal**. La adopción de plataformas de software como servicio y la migración hacia la computación en la nube permiten que el personal de la empresa trabaje desde cualquier lugar. De este mismo modo, las contraseñas filtradas podrán ser usadas por los invasores desde cualquier lugar del mundo. Más allá de dificultar la acción de las autoridades policiales, el acceso universal eleva la importancia de la credencial como mecanismo de acceso, pues hace prescindible la defensa que tradicionalmente ofrece el perímetro físico da empresa.

Así, son diversos los ataques, amenazas y perjuicios para la empresa que pueden materializarse a partir de la filtración de una contraseña, independientemente de la debilidad que esta presente. Algunos ejemplos:

- **Ransomware.** Muchas invasiones que derivan en el secuestro de información y la paralización de actividades de las empresas empiezan por una credencial corporativa: acceso al e-mail, red privada virtual (VPN) y sistemas en la nube. Cada vez que lo necesita, el invasor utiliza técnicas de movimiento lateral para profundizar el acceso inicial obtenido, y con esto aumenta el alcance del ataque.
- **Filtración de datos.** Toda la información accesible para el personal de la empresa cuyas contraseñas hayan estado en riesgo, también estará en riesgo.
- **Perjuicios financieros.** El acceso a los sistemas de gestión financiera, compras y contratos puede ocasionar pérdidas financieras directas para la empresa.
- **Business Email Compromise (BEC)**. Al hacerse pasar por ejecutivos y directores de la empresa utilizando una contraseña filtrada, los delincuentes pueden emitir órdenes de pago y solicitudes de datos falsas.
- **Otros perjuicios y costos**. La filtración de datos, el ransomware y otras acciones de los invasores pueden ocasionar daños a la marca y a la confianza de socios de negocios y clientes, más allá de justificar la aplicación de multas y otras acciones de entidades regulatorias dedicadas a la protección de la privacidad y del consumidor.

En la medida en que los sistemas se interligan al ecosistema de TI de la organización (incluidas las plataformas de software como servicio y otros sistemas de terceros, como reclutamiento, marketing, redes sociales, etc), se hace evidente la necesidad de aumentar la robustez del proceso de autenticación.

Y es a partir de este escenario que surgen conceptos como la autenticación multifactor, la autenticación step-up (también llamada contexto de autenticación o autenticación por etapas), el acceso just-in-time, entre otros, como también la evolución de la noción de privilegio mínimo (como Zero Trust).

De esta manera, el tema de la protección de credenciales está en constante evolución, recibiendo innovaciones y perfeccionándose constantemente. La MFA constituye una de estas evoluciones, pero los riesgos y la complejidad de la temática demuestran que no existe una única solución que sea definitiva para todos los contextos.

En los próximos capítulos, abordaremos las limitaciones mayormente asociadas a la MFA tradicional, en la que el login exige al menos dos factores de autenticación.

Limitaciones de la MFA

Siendo la confidencialidad uno de los pilares de la seguridad de la información, es necesario que haya mecanismos que reconozcan a quienes poseen autorización para acceder a un determinado recurso. La autenticación por medio de contraseña, aun siendo un medio tradicional, es vulnerable a diversos ataques: la contraseña puede ser robada, descifrada o repetida por el usuario, por ejemplo.

En este contexto, uno de los ataques más simples es el phishing. En cualquier caso en el que sea posible enviar una comunicación al usuario (generalmente un e-mail), el invasor puede intentar convencer a la víctima para que revele su contraseña en una pantalla falsa, y así capturar su credencial de acceso.

El objetivo más evidente de la autenticación multifactor es volver inviables los ataques poco sofisticados, como el phishing tradicional, reforzando la autenticación simple con pasos adicionales.

Sin embargo, la suma de pasos adicionales no ocurre sin aumentar la complejidad. En este sentido, la MFA a menudo se implementa sin un panorama adecuado de la superficie de ataque y de la función que debe desempeñar. A raíz de esto es que aparecen algunas dificultades y contratiempos:

- **La amenaza de malware está fuera del alcance de la MFA**. Aunque muchos códigos maliciosos sean creados para robar credenciales, la MFA no proporciona una protección eficaz contra la acción de estos malwares. Cuando el malware actúa directamente a partir del endpoint del usuario (es decir, el invasor controla el dispositivo durante el acceso del usuario), el invasor aprovecha la sesión autenticada que está en marcha. Y salvo que la MFA haya sido pensada para acciones específicas, no actuará en este escenario.
- **La autorización en sí misma puede ser atacada**. La MFA mejora el proceso para obtener la autorización, pero no refuerza el mecanismo de autorización en sí. En las implementaciones más simples de MFA, no se tiene en cuenta este punto y la autenticación resulta idéntica a la de una cuenta de factor único.
- **La MFA puede exigir un nuevo proceso de recuperación de cuenta**. Si la recuperación de una cuenta protegida con MFA sucede de la misma forma que la de una cuenta sin MFA, el eslabón más débil de la cadena se traslada de la credencial al proceso de recuperación. No obstante, aun teniendo una correcta implementación de la recuperación de cuenta no se eliminan los ataques contra este proceso.

- **Los factores adicionales de MFA también pueden ser atacados**. De forma aislada, cada factor es vulnerable a ataques específicos. Como la contraseña es un objetivo antiguo y común, con frecuencia los ataques llevados a cabo contra los demás factores pasan inadvertidos.

A continuación, veremos cómo estas limitaciones y dificultades se manifiestan en las implementaciones prácticas de MFA en el mundo real.

¿MFA o 2FA?

El concepto de MFA abarca cualquier situación en la cual los usuarios de una aplicación necesiten combinar más de un tipo de verificación o autorización para obtener su acceso al entorno. La implementación correcta de este método exige que los "factores" usados sean de diferente naturaleza: algo que se "sabe" (una contraseña), algo que se "es" (biometría) o algo que se posee (clave, tarjeta, celular, entre otros).

Más recientemente, la ubicación del usuario también se ha evidenciado como un factor viable. En Brasil, este factor ya aparece como complemento en sistemas que controlan los turnos de trabajo, y condiciona la autorización de inicio de las tareas a una ubicación predeterminada.

Aunque en teoría no esté limitada a implementaciones específicas, el uso de la MFA presenta algunas complejidades. De hecho, es bastante extraño que el proceso de autenticación exija más de dos factores y, por esta razón, la MFA es más conocida por el nombre de 2FA, o "verificación en dos pasos".

Si bien en ocasiones las lenguas latinas presentan inconsistencias al momento de traducir terminología que se origina en el idioma inglés, el presente es una variación del témino "2FA" que aparece en las opciones de seguridad de las aplicaciones. En WhatsApp, por ejemplo, se denomina "verificación en dos pasos".

En el ambiente corporativo, agregar más de un factor puede resultar más difícil, ya sea por la necesidad de brindar un soporte para más de un producto o plataforma como por los costos que surgen de la adquisición de hardware especializado o servicios de asistencia.

En resumen, aunque la MFA contemple más de dos factores de autenticación, usar tres o más factores no es una práctica común. Un tercer factor de autenticación generalmente no aporta un avance de seguridad proporcional al aumento de la complejidad y la incomodidad para los usuarios. Por esta razón, los factores adicionales habitualmente quedan restringidos a aplicaciones y sistemas de alto riesgo.

Si bien es importante observar que el invasor deberá burlar dos factores de autenticación (y no tres o cuatro), podemos decir que algunos ataques contra la MFA continuarían obteniendo buenos resultados aun si se agregaran más factores de autenticación. Esto sucede porque, como ya hemos observado, la seguridad no siempre es proporcional al número de factores.

Como el término "MFA" incluye 2FA y muchos ataques poseen potencial suficiente como para funcionar en ambos, generalmente no se establece una separación o diferenciación entre ellos. Vale decir, un ataque contra 2FA es un ataque contra MFA y viceversa.

Los factores de autenticación

Los mecanismos de autenticación se dividen en tres factores: algo que se sabe, algo que se posee y algo que se es (características inherentes al usuario). Cada factor es una categoría; un sistema que exige dos contraseñas de hecho no utiliza dos factores, pues las dos solicitudes se encuadran en el mismo factor.

Cuando un proceso de autenticación exige una contraseña generada en tiempo real en una aplicación del celular, el objetivo del código de un solo uso es comprobar que el usuario está en posesión del dispositivo (celular o clave capaz de generar la contraseña), contemplando el factor "algo que el usuario posee".

Aunque el código de un solo uso (one-time password), generado por una aplicación o recibido por SMS, sea una "contraseña", no debe ser confundido con una contraseña en sí, ya que esta última verifica algo que el usuario sabe y está incluida en otro factor.

No existe un único mecanismo para cada factor, lo que lleva a una gran variación en las formas y tipos de MFA existentes en el mercado. Como no es raro que la misma persona tenga contacto con varias formas de MFA, la sobrecarga de factores de autenticación facilita las cosas a los invasores, ya que los usuarios fácilmente pueden confundir un método con otro.

Mecanismos usados como factores de autenticación

Factor	Mecanismos
Concimientoel usuario "sabe"	Contraseña PIN Dibujo de patrón
Posesiónel usuario "posee"	**Smartphone** Clave generadora de contraseña temporal (OTP) Linea telefónica (SMS) Acceso previo (notificación PUSH, aplicación autenticada) **Dispositivos en general** Clave privada guardada en el dispositivo **Otros** E-mail Llave criptográfica USB (U2F/FIDO) Smartcard (PKI) Token generador de contraseñas
Natural/Propioel usuario "es"	Voz Iris Rostro Huellas dactilares

El uso de múltiples factores de autenticación causa inconvenientes al usuario y, por esta razón, no resulta extraño que el mecanismo se flexibilice. En este escenario, el usuario elige si prefiere utilizar un código generado por una aplicación, una autorización en el celular o una llave criptográfica USB. Aunque todos funcionan, sólo uno es obligatorio para cumplir la exigencia del factor. Para el usuario, la redundancia puede ser útil en el caso de que surja algún problema en los mecanismos configurados (falla en el celular, ausencia de señal para recibir SMS, entre otros).

Desafortunadamente, esta práctica conduce a la reducción de la seguridad del usuario, ya que el invasor necesita poner en riesgo sólo un mecanismo para acceder a la cuenta. Por ejemplo: si un usuario usa códigos recibidos por SMS o de una aplicación, el invasor puede acceder a la cuenta por medio de la red móvil, el chip, el aparato celular o la clave. Si retiramos la opción del SMS, el invasor se ve obligado a recurrir a las dos últimas opciones, pues el servicio de telecomunicación deja de estar incluido.

Por esta razón, es necesario ser conscientes de que el uso de más de un mecanismo de autenticación dentro del mismo factor beneficia la conveniencia y la disponibilidad de la cuenta, pero no la confidencialidad.

Los ataques contra la MFA

Este capítulo abordará los ataques concretos capaces de burlar la autenticación multifactor. Los ataques pueden dividirse en dos grandes categorías: los que funcionan independientemente del mecanismo adoptado, y los que son dirigidos hacia mecanismos específicos.

Ataques contra cualquier mecanismo

Malware

- **En 2022, Axur extrajo 435,98 millones de credenciales robadas a partir del análisis de 7,4 TB de archivos generados por credential stealers y compartidos en el submundo del delito.**

El uso de factores adicionales en la autenticación no tiene efecto sobre la actuación de un malware. Un código malicioso instalado en el dispositivo de la víctima puede llegar a permitir el control remoto del sistema, dando al invasor el mismo nivel de acceso que al usuario luego del login.

El malware también puede servir de accesorio para otras modalidades de ataque a la MFA, como el robo de cookies de sesión, spear phishing y MFA fatigue.

Una de las principales ventajas de las que se vale el malware es la posibilidad de esparcirse usando carnadas sin conexión directa con el sistema de autenticación. La víctima puede instalar un malware mientras busca bajar un programa común y, sin sospecharlo, su información será robada luego de conceder los permisos indebidos al malware que supuestamente era un programa de confianza.

Este escenario es bastante común, inclusive para las personas que no demuestran comportamientos inseguros en su navegación. Los estafadores usan perfiles en las redes sociales, anuncios on-line y otros mecanismos para divulgar links que llevan a descargas de softwares adulterados. La prevalencia del malware en los anuncios llevó al FBI a recomendar el uso de un bloqueador de anuncios en la web como medida de prevención.

El malware también puede actuar en los dispositivos personales de los empleados de la empresa, robando las credenciales por una ruta con visibilidad reducida para los sectores de seguridad y de tecnología.

Aunque la solución tradicional contra la actividad del malware sea utilizar un antivirus, esta medida por sí sola no ha demostrado mayor eficacia. Los malwares de tipo credential stealer pueden ser reconfigurados, adaptados y reciclados constantemente, y es posible que la actualización del antivirus llegue después de haberse producido el robo de las credenciales.

Phishing, spear phishing y vishing

- **En 2022, Axur detectó 34 mil páginas de phishing**

Si bien la autenticación multifactor es muy citada como una medida de prevención contra las consecuencias del phishing, este ataque puede adaptarse para funcionar en un contexto con MFA. El spear phishing (mensaje redactado para un destinatario específico) tiene la capacidad de ser especialmente eficaz para los casos en que el invasor ya cuenta con información sobre la víctima.

Entre las posibilidades se encuentran:

- **Robo de códigos de recuperación**. La mayoría de los sistemas de MFA permiten el uso de códigos de recuperación generados previamente. El objetivo es garantizar que el usuario conserve el acceso a la cuenta en situaciones imprevistas, como la pérdida del celular, la llave USB o la línea telefónica. En vez de robar la contraseña, el phishing será utilizado para robar el código de recuperación que, por ser fijo, estará disponible para un uso posterior.
- **Etapa inicial de otros ataques**. El mensaje de phishing puede contener links usados para diseminar malware, robar cookies o realizar ataques de interceptación.

A comienzos de 2023, la red social Reddit anunció que un empleado fue víctima de un spear-phishing que clonó la vista del interior de la empresa para engañar al usuario.

En el caso del vishing (voice phishing, o phishing por llamada telefónica), el estafador intenta llamar a la víctima y confundirla al solicitar el código recibido por SMS o la confirmación de otro mecanismo para una finalidad diferente (una promoción o chequeo de seguridad, por ejemplo). Luego de que la víctima realiza la acción solicitada o informa el código, el invasor cuenta con toda la información necesaria para llevar a cabo el acceso exactamente en ese instante.

En 2022, el proveedor de equipos de red Cisco fue objetivo de vishing. Según el informe de la empresa, el invasor derrotó la MFA de la cuenta Google de un empleado que había almacenado y sincronizado la contraseña de la red corporativa en su navegador Chrome, y, así, el atacante pudo obtener las contraseñas sincronizadas luego de acceder a la cuenta Google de la víctima.

Estos ataques suelen ser más efectivos después de que la credencial básica (usuario y contraseña) fue obtenida por otro medio (malware, por ejemplo). Las contraseñas repetidas también constituyen un riesgo, pues muchos sistemas de login validan la contraseña (que puede haberse filtrado de otro servicio) antes de solicitar el segundo factor.

Después de validar la contraseña, el atacante puede iniciar los intentos de phishing del segundo factor, con la seguridad de que tiene la contraseña correcta para derrotar al primer factor.

Robo de sesión y cookies (pass-the-cookie)

La MFA requiere varias pruebas para conceder la autorización de login. Sin embargo, la autorización en sí generalmente se almacena en una cookie en el navegador web o en la aplicación. A cada visita del usuario, se realiza una comprobación de los parámetros de esa cookie y, si se constata la existencia de una autorización válida, el usuario continúa navegando o usando la aplicación.

Si se obtiene ese código de autorización, el mismo se puede utilizar para entrar directamente en la cuenta, sin pasar por el proceso de login. Algunos servicios y plataformas incorporan chequeos a fin de impedir que la cookie que se envía a un navegador funcione en otro, pero la efectividad de esta protección puede variar de un caso a otro. Este tipo de ataque se denomina pass-the-cookie.

Los malwares credential stealers habitualmente incluyen las cookies de sesiones autorizadas en el paquete de información robada de las computadoras infectadas. El conjunto de datos se vende a otros interesados en el submundo del delito, y ellos evalúan la mejor forma de utilizar la sesión capturada.

La ingeniería social aliada al phishing también puede emplearse para robar la sesión. En este caso, se convence al usuario para que pegue un código en su navegador web a fin de robar las cookies que le interesen al atacante.

El riesgo es aún mayor en los servicios de criptografía. En este caso, cualquier agente malicioso de la misma red puede realizar el robo de sesión. En 2010, una aplicación llamada Firesheep demostró cómo este ataque podría realizarse fácilmente en redes Wi-Fi públicas, por ejemplo.

Hoy en día, la mayoría de las grandes plataformas y aplicaciones utilizan criptografía, como TLS (Transport Layer Security). Sin embargo, las aplicaciones corporativas que hacen uso de la MFA necesitan utilizar criptografía adecuada para evitar que sus sesiones sean robadas en redes compartidas.

Interceptación e intermediación (AiTM)

EL ataque "hombre en el medio", hoy llamado "adversario en el medio", se caracteriza por un escenario en que el agente malicioso logra posicionarse "entre” el usuario y el servicio al que se está accediendo.

Este escenario se construye fácilmente a través de un link enviado en un phishing. En algunas situaciones más específicas, existe la posibilidad de redireccionar el acceso del usuario hacia una página falsa. Este redireccionamiento puede pasar inadvertido si la víctima no presta atención a la barra de direcciones y a otras indicaciones del navegador.

A diferencia del phishing tradicional, en el cual la página falsa sólo captura la credencial que se ingresó, este ataque hace uso de la intermediación (o "proxy") de acceso: toda la información y las interacciones realizadas por el usuario se envían a la página verdadera. Si se digita la contraseña incorrecta, el usuario verá un error; si existe más de un factor de autenticación, será perfectamente replicado.

Las diferencias comienzan cuando el usuario finaliza el proceso de login. En este momento, en vez de enviarse al navegador del usuario la cookie de sesión y otros tipos de información de autorización, los datos se remiten al atacante a fin de que pueda acceder a la cuenta.

El ataque se concreta a través del empleo de una táctica de pass-the-cookie o por la automatización de las acciones maliciosas que el invasor pretende realizar.

Aunque parezca sofisticado, este ataque se puede organizar fácilmente con herramientas listas para usar y gratuitas como Evilginx2, Modlishka y Muraena. El atacante sólo necesita configurar un dominio y un servidor web para crear el sitio falso con una de estas soluciones.

Microsoft ha registrado ataques de este tipo contra varios de sus clientes. En julio de 2022, la empresa reveló que más de 10 mil organizaciones que usan la nube Azure o Microsoft 365 fueron el objetivo de los atacantes.

Autorización de aplicaciones (OAuth)

Una ventaja de muchas plataformas de software como servicio (SaaS) es la posibilidad de integrar aplicaciones externas. Para que las aplicaciones sean compatibles con la MFA es necesario que se las vincule al acceso del usuario mediante una clave de autenticación (OAuth) con canal de API (application programming interface).

En síntesis, se trata de un canal de acceso dedicado a las aplicaciones conectadas, lo que genera pros y contras para el invasor. El acceso puede ser más limitado que el login real, pero al invasor se le facilitará automatizar la recolección de datos usando la API. De todos modos, el acceso no pasará por la MFA luego de ser concedido por el dueño de la cuenta.

Como las capacidades de este canal de acceso y su funcionamiento no siempre están claros para todos los usuarios, los invasores aprovechan esto para intentar convencer a las víctimas de que autoricen las aplicaciones en sus cuentas. Otra posibilidad es utilizar aplicaciones autorizadas por OAuth con la finalidad de construir un acceso persistente luego de un login exitoso.

Otra variación de este concepto puede incluir tokens de single sign-on (SSO), aunque esto generalmente depende de la implementación o de las vulnerabilidades técnicas en el servicio de login.

De cualquier manera, la obtención de un token OAuth autorizado permite burlar el proceso de autenticación.

Una vez concedido el permiso, este suele separarse de las sesiones de usuario. Es decir, el acceso no se remueve cuando el usuario cierra todas las sesiones abiertas. Si el token de la API o OAuth no puede ser fácilmente anulado, es posible que permanezca válido inclusive luego del cambio de contraseña de la cuenta.

El riesgo que representan estas autorizaciones indebidas provocó que muchos servicios restrinjan el uso de sus APIs. En el caso de los sistemas corporativos y OAuth, puede ser necesario comprobar los permisos y configuraciones de entorno para verificar si los usuarios pueden o no delegar este acceso a terceros.

Ataques a mecanismos específicos

MFA Fatigue

- **Mecanismo atacado:** notificación push / acceso previo

También llamado "push bombing", la MFA Fatigue se usa para burlar sistemas de MFA por notificación push. Este es el mecanismo de MFA en que el usuario recibe un aviso en el smartphone solicitando la confirmación de un acceso iniciado en otro dispositivo.

Además de las aplicaciones preparadas para recibir las notificaciones push a fin de obtener esta confirmación, otro abordaje similar prevé el uso de un dispositivo previamente autorizado para confirmar el acceso de una nueva sesión.

Para llevar a cabo este ataque, el invasor hace varios intentos de login usando la credencial de la víctima. Con esto genera diferentes solicitudes de confirmación de acceso, una por cada intento. A partir de esta situación, la víctima puede terminar confirmando el acceso del invasor ya sea por cansancio ante los reiterados mensajes de aviso, o por un clic accidental en la pantalla, o por haber confundido un intento de acceso propio con el intento del invasor.

En septiembre de 2022, Uber reveló que el grupo de ciberdelincuentes Lapsus$ logró burlar su autenticación multifactor usando MFA Fatigue.

SIM Swap, Spoofing Y SS7

- **Mecanismo atacado**: código por SMS

Un atacante puede interferir en el envío de códigos por SMS de dos maneras: alterando el chip que recibirá el código ("SIM swap") o interfiriendo en el protocolo de comunicación entre las operadoras de telefonía, el Signalling System 7 (SS7).

Los ataques al SS7 son más escasos y resultan más efectivos cuando existen vulnerabilidades o errores en la implementación. Aun así, la operadora de telefonía O2, de Alemania, confirmó en 2017 el robo de cuentas a clientes bancarios porque los delincuentes lograron redireccionar SMSs de confirmación de transferencias hacia números telefónicos controlados por ellos.

Vale recordar que los invasores también lograron utilizar el servicio de buzón de voz de los celulares para grabar códigos de autorización recibidos a través de una llamada telefónica. Con todo, estos ataques no sucedieron por interferencia directa en el protocolo SS7, sino que los invasores se valieron del Caller ID spoofing (falsificación de origen de la llamada), ofrecido por proveedores de VoIP, para acceder a los buzones de voz de forma irregular.

Con todo, los más comunes son los ataques de SIM Swap, que ocurren cuando los invasores logran transferir la titularidad de una línea móvil a otro chip, muchas veces gracias a la acción de cómplices que integran la banda delictiva dentro de las empresas de telecomunicaciones.

En los Estados Unidos, las autoridades acusaron a varios individuos de cometer delitos que involucraban el SIM Swap, especialmente para robar criptoactivos. Algunos de ellos eran ex empleados de operadoras de telefonía, como AT&T y Verizon. Esto motivó la creación de nuevos procedimientos de seguridad para dificultar la transferencia de la línea hacia otro chip.

De cualquier manera, todos los mecanismos basados en el SMS dependen de la seguridad del proveedor de servicios de telecomunicaciones.

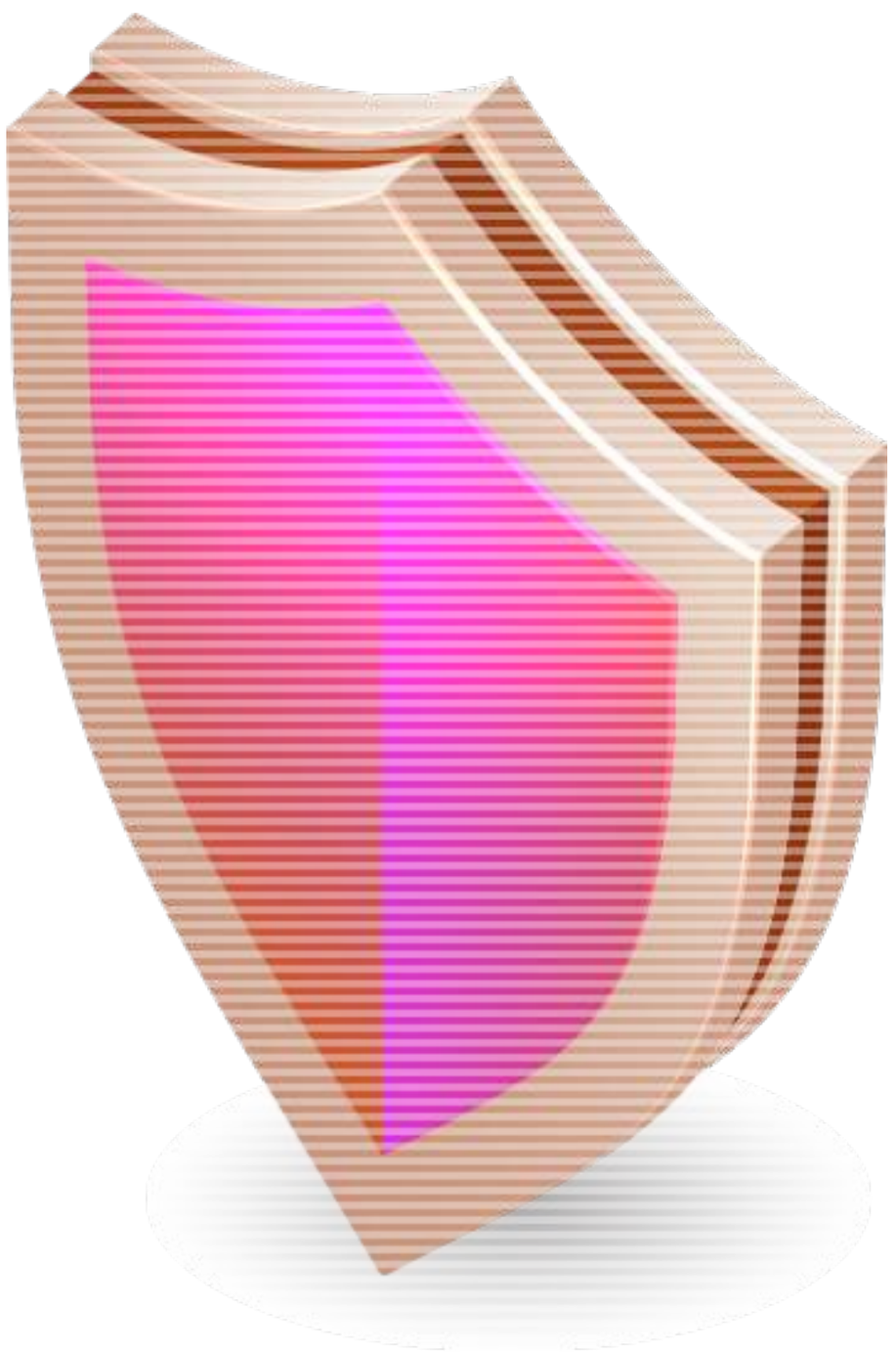
Extravío

- **Mecanismo atacado**: código por SMS, OTP, llave USB, llave incorporada en el dispositivo

Como la MFA utiliza como factor de autenticación "algo que el usuario posee", el invasor tiene la posibilidad de robar el dispositivo. La efectividad del robo puede variar entre caso y caso: por ejemplo, las tarjetas SIM con chip y celulares bloqueados tal vez no sean útiles para el invasor. En cambio, otros mecanismos, como las llaves USB, no utilizan ninguna autenticación adicional para liberar las claves almacenadas.

Para mitigar las consecuencias, es importante que la víctima informe rápidamente del extravío, lo cual no sucederá siempre. La existencia de mecanismos adicionales de autenticación permite que el usuario siga entrando a su cuenta a través de otras rutas de acceso. Además, existe la posibilidad de que la víctima confunda el robo con algo menos grave (una simple pérdida u olvido), lo que también puede demorar la denuncia del extravío.

Cómo evolucionar en la seguridad de los accesos



Muchas de las técnicas viables para violar la autenticación multifactor sólo se pueden utilizar después de la obtención de la credencial de la víctima (usuario y contraseña) por parte del atacante. Por esta razón, existe la oportunidad de mejorar la seguridad del proceso protegiendo la propia credencial.

Los datos sobre las credenciales filtradas, combinados con un proceso robusto de respuesta a incidentes, contribuyen a detectar y mitigar los incidentes de seguridad, al indicar cuáles son las credenciales que están en riesgo para que la empresa pueda bloquearlas.

Del mismo modo, la información sobre la actuación de los atacantes, procedente de Cyber Threat Intelligence (CTI), permite identificar la filtración de tokens de autenticación o cookies que cayeron en las manos de los delincuentes.

Estos datos se obtienen a través del **monitoreo de credenciales de Axur** por medio del seguimiento de los movimientos de los agentes maliciosos y la identificación de la información filtrada en la Web (tanto en la Surface, como en la Dark o Deep Web).

Al recibir una alerta sobre una credencial que ha sido obtenida por los delincuentes, la empresa puede dar inicio al proceso de respuesta a incidentes e impedir que esta credencial se use en ataques. La posibilidad de **automatización** de este proceso aumenta más aún las chances de mitigar y hasta evitar un incidente.

Visión fuera del perímetro

Una de las ventajas del monitoreo de Axur es el acceso a los datos que han sido obtenidos por malwares de tipo credential stealer. La información capturada por estos malwares se distribuye en archivos de “log” en el submundo del delito digital. Los archivos “log” contienen datos del sistema, contraseñas, cookies y otros datos especificados por los operadores del código malicioso.

De esta manera, el monitoreo tiene la capacidad de visibilizar las credenciales robadas en cualquier dispositivo, inclusive en los sistemas del personal de la empresa remoto, clientes o terceros, **agregando una capa de protección tanto a la red corporativa como a los servicios digitales prestados a clientes y socios.**

Para clientes y socios

Para los proveedores de servicios digitales que exigen credenciales de acceso de cada cliente o socio, no es posible depender de la seguridad del dispositivo del usuario. Desafortunadamente, cualquier violación a la seguridad que suceda derivada de un ataque de phishing o malware al usuario generará trastornos también para el proveedor, tanto por la actividad indebida en la cuenta como por el costo del soporte que deberá ofrecerse al usuario para recuperar el acceso.

El monitoreo de credenciales puede examinar servicios o dominios y detectar todas las credenciales filtradas para un servicio específico. El prestador de servicios alerta a los usuarios sobre la necesidad de cambiar la contraseña o deshacer los cambios en la cuenta que fueron ocasionados por la invasión.

Para el personal de la empresa

Con el trabajo híbrido en home office o a través de políticas de Bring Your Own Device (BYOD), muchas empresas permitieron el uso de dispositivos personales. La seguridad de estos dispositivos es un desafío para el equipo de seguridad, pues no siempre es posible registrar toda la actividad que en ellos se desarrolla. En otras palabras, existe una falta de visibilidad.

Además de esto, la actividad personal de los empleados puede acarrear riesgos adicionales difíciles de calcular. Aunque la política de seguridad de la organización prohíba un tipo de uso del dispositivo, el usuario puede no respetar las disposiciones o las políticas de uso del dispositivo que recibió para su trabajo.

Como el monitoreo puede visualizar las credenciales filtradas independientemente de su origen, una actividad de malware o phishing en el dispositivo personal del usuario también será detectada. Esta es una visibilidad que la empresa difícilmente tendría de otra forma.

Beneflcio para los usuarios y para la empresa

Aun teniendo la MFA a disposición, no todos los usuarios optan por su utilización. También hay casos en los que la empresa depende de sistemas que no ofrecen MFA o que no pueden ser migrados hacia una plataforma de single sign-on.

El monitoreo actúa en cualquiera de estos casos. Como podemos ver en el cuadro a continuación, el alcance de las detecciones del monitoreo asegura beneficios para los usuarios con o sin MFA, puede alertarlos sobre la información expuesta a posibles intentos de spear phishing y, además, puede colaborar con la investigación de las violaciones a la política de seguridad.

El monitoreo detecta:

- **Contraseñas robadas:** para usuarios o sistemas sin MFA, proteger sus contraseñas significa resguardar la seguridad del proceso de autenticación. Para usuarios con MFA, una contraseña robada puede ser el antecedente de un ataque de phishing contra los códigos de recuperación, una estafa telefónica o un intento de MFA fatigue.
- **Cookies robadas:** las cookies de autenticación pueden usarse para acceder a cuentas con o sin MFA. Detectando e invalidando las cookies que cayeron en las manos de delincuentes, todos los usuarios se benefician.
- **Datos que pueden ser usados por spear phishing:** el spear phishing se caracteriza por ser un mensaje extremadamente personalizado, y el atacante puede utilizar la información personal de la víctima para volver el mensaje más confiable. Con el monitoreo, los usuarios de alto privilegio pueden recibir alertas sobre la información personal que se filtró y que es probable que sea usada en este tipo de ataque.

- **Datos que pueden violar los sistemas de recuperación:** la MFA exige que las organizaciones y los prestadores de servicios adopten mecanismos de recuperación para los casos en que el segundo factor no está disponible. Las credenciales robadas pueden dar acceso a sistemas de e-mail u otros datos relacionados con este proceso, debilitando la MFA.
- **Violaciones a la política de seguridad:** los logs de los credential stealers casi siempre contienen información sobre el sistema del usuario. Esta información puede ayudar a la empresa a determinar si se accedió a una cuenta corporativa a partir de dispositivos personales o si fue el usuario quien registró su e-mail corporativo en otros servicios.

¿Desea comprobar su seguridad?

Agende una demostración gratuita de la plataforma Axur y descubra cómo el monitoreo de amenazas puede ayudar a su empresa para estar protegida en toda su superficie externa.

Sobre a Axur

Axur permite la escalabilidad y la automatización de la gestión de las ciberamenazas para apoyar a los equipos de seguridad de la información y ofrecer experiencias digitales más seguras. Nuestra plataforma de Cyber Threat Intelligence posee el tiempo de reacción más rápido del mercado, solicitando Takedowns automáticos 24×7.

Esto es posible porque la plataforma Axur trabaja en cuatro capas: además de la detección, las tecnologías de inspección, automatización y eliminación reducen en gran medida el tiempo medio de contención (MTTC) para los equipos de seguridad. Además, nuestros expertos en Ciber Inteligencia amplían la investigación tanto en la Surface como en la Deep & Dark Web, convirtiendo a Axur en la empresa líder en Cyber Threat Intelligence de Latinoamérica.

Detecte y remueva amenazas con la plataforma All-in-one nº 1 del mercado

AGENDE UNA DEMO

HÁGANOS SUS CONSULTAS

Contacto para prensa:
Letícia Peres
press@axur.com
+55 (11) 9 3209.7588