[Estado de Internet] / Seguridad

Edición especial para medios, volumen 5

Credential Stuffing: Ataques y mercados

Introducción

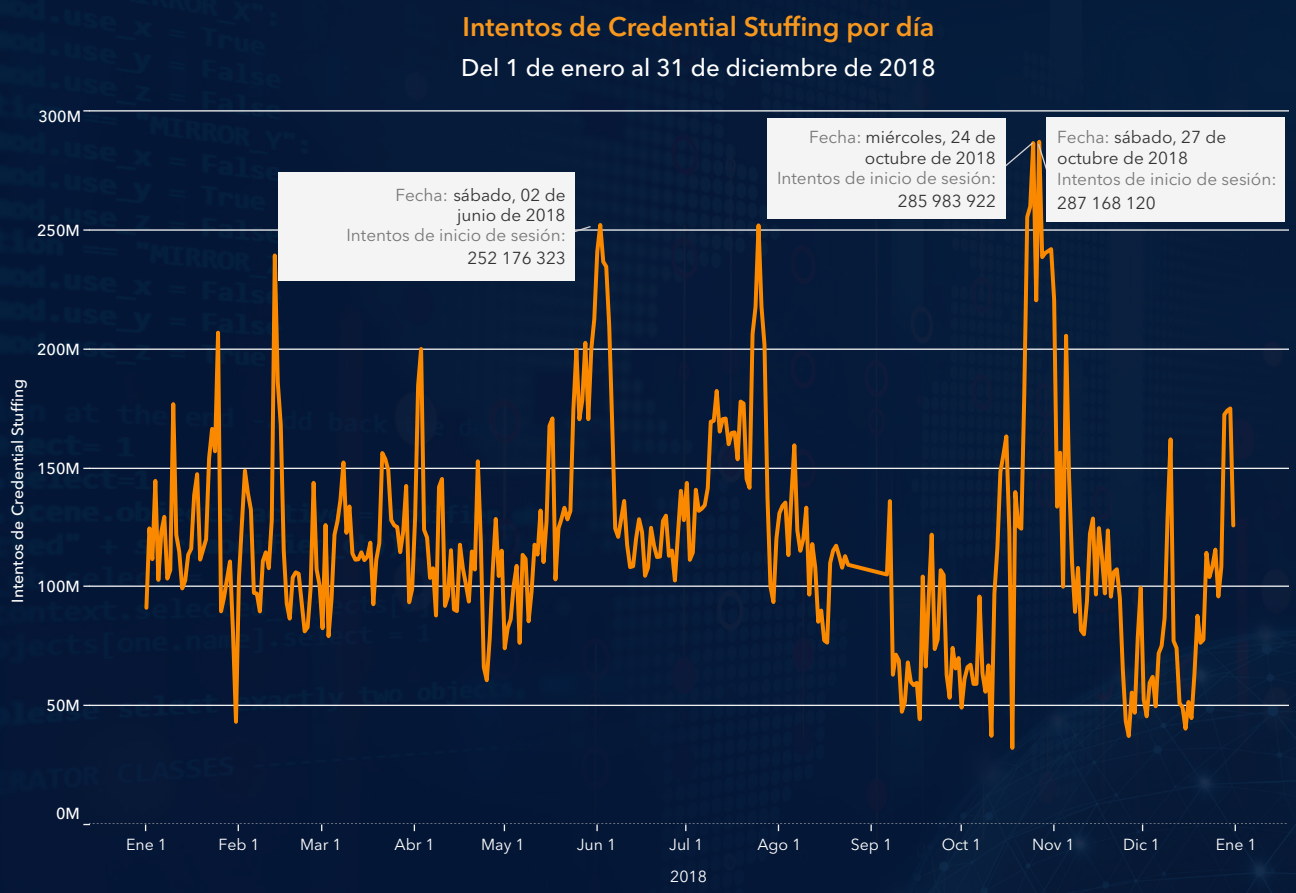
Akamai registró casi 30 000 millones de ataques de Credential Stuffing en 2018. En cada ataque, una persona o un ordenador intentaba iniciar sesión en una cuenta con unas credenciales generadas o robadas. Gran parte de estos ataques pueden atribuirse a botnets o aplicaciones "todo en uno", o All-in-One (AIO).

Las botnets son grupos de ordenadores que se programan con una serie de comandos. Pueden programarse para encontrar cuentas vulnerables a fin de que otras personas que no sean los titulares puedan acceder; estos ataques reciben el nombre de robos de cuentas (ATO, por sus siglas en inglés). Las aplicaciones AIO permiten automatizar el inicio de sesión o el proceso ATO, y son esenciales para el robo de cuentas y la recopilación de datos.

¿Qué tiene que ver esto con las empresas del sector de medios, videojuegos y entretenimiento? Mucho. Estas empresas constituyen el principal objetivo de los ataques de Credential Stuffing. Las personas que están detrás de estos ataques son conscientes del valor que tiene una cuenta, ya sea de un sitio de streaming, un juego o una cuenta personal en una red social. Y están dispuestos a hacer lo que sea para robarlas.

En este informe, analizaremos los ataques de Credential Stuffing en 2018 contra los sectores que hemos mencionado y examinaremos los riesgos que plantean. También abordaremos algunos de los métodos empleados para perpetrar estos ataques.

Las empresas del sector de medios de comunicación, videojuegos y entretenimiento son los principales objetivos de los ataques de Credential Stuffing.



Ataques por día

En 2018, Akamai observó cientos de millones de ataques de Credential Stuffing día tras día. Estos ataques iban dirigidos a diversos sectores; entre ellos, los de medios de comunicación y entretenimiento, retail y videojuegos. Como puede observarse en la Figura 1, hubo tres días en los que se produjo el mayor número de intentos: más de 250 millones. Los ataques de Credential Stuffing se están convirtiendo en uno de los métodos preferidos por delincuentes de todos los niveles. En los informes anteriores de "Estado de Internet" (SOTI), se analizaba el impacto en el sector retail; sin embargo, en esta ocasión, nos centramos en los sectores multimedia y del entretenimiento.

Los delincuentes ponen el punto de mira en grandes empresas de entretenimiento y vídeos, ya que el acceso a las cuentas verificadas se puede vender o intercambiar en el mercado clandestino. Si alguna vez ha reproducido en streaming y online una canción, una película o un programa de televisión, es probable que ya sepa cuáles son las cuentas preferidas por los delincuentes. La información asociada a estas cuentas también tiene valor.

Figura 1

Se destacan tres de los ataques más importantes observados en 2018, incluidos dos que tuvieron lugar con pocos días de diferencia.

Los mayores ataques

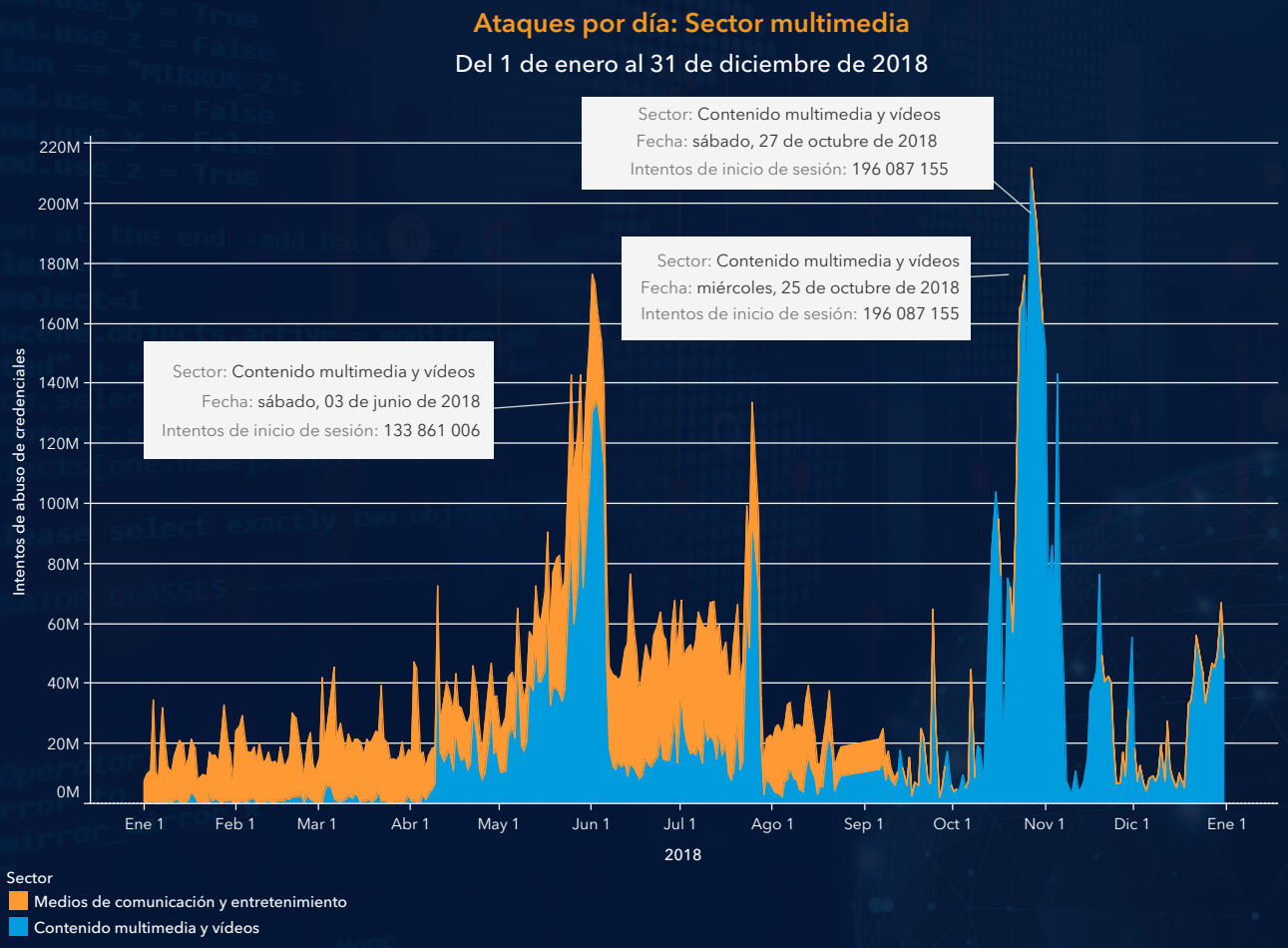
Solo en el sector dedicado a los vídeos, tres de los mayores ataques de Credential Stuffing que se produjeron en 2018 hicieron que la cifra de intentos ascendiera de 133 millones a cerca de 200 millones. Es un dato que tener en cuenta, ya que las fechas de los ataques coinciden con unas filtraciones de datos conocidas. Es probable que los responsables estuvieran probando las credenciales antes de venderlas. A principios de febrero de 2019, unos 620 millones de nombres de usuario, contraseñas y otros registros (procedentes de 16 organizaciones que comunicaron haber sido víctimas de filtraciones de datos) se pusieron a la venta en la Dark Net.

Credential Stuffing

Es probable que, a principios de 2019, haya oído la noticia de alguien anónimo que divulgó un conjunto de direcciones de correo electrónico y contraseñas para Credential Stuffing, un conjunto dividido en cinco lotes.

Figura 2

Tres de los mayores ataques de Credential Stuffing contra el sector de contenido multimedia y vídeos durante 2018 supusieron un aumento de los 133 millones a casi 200 millones de intentos.



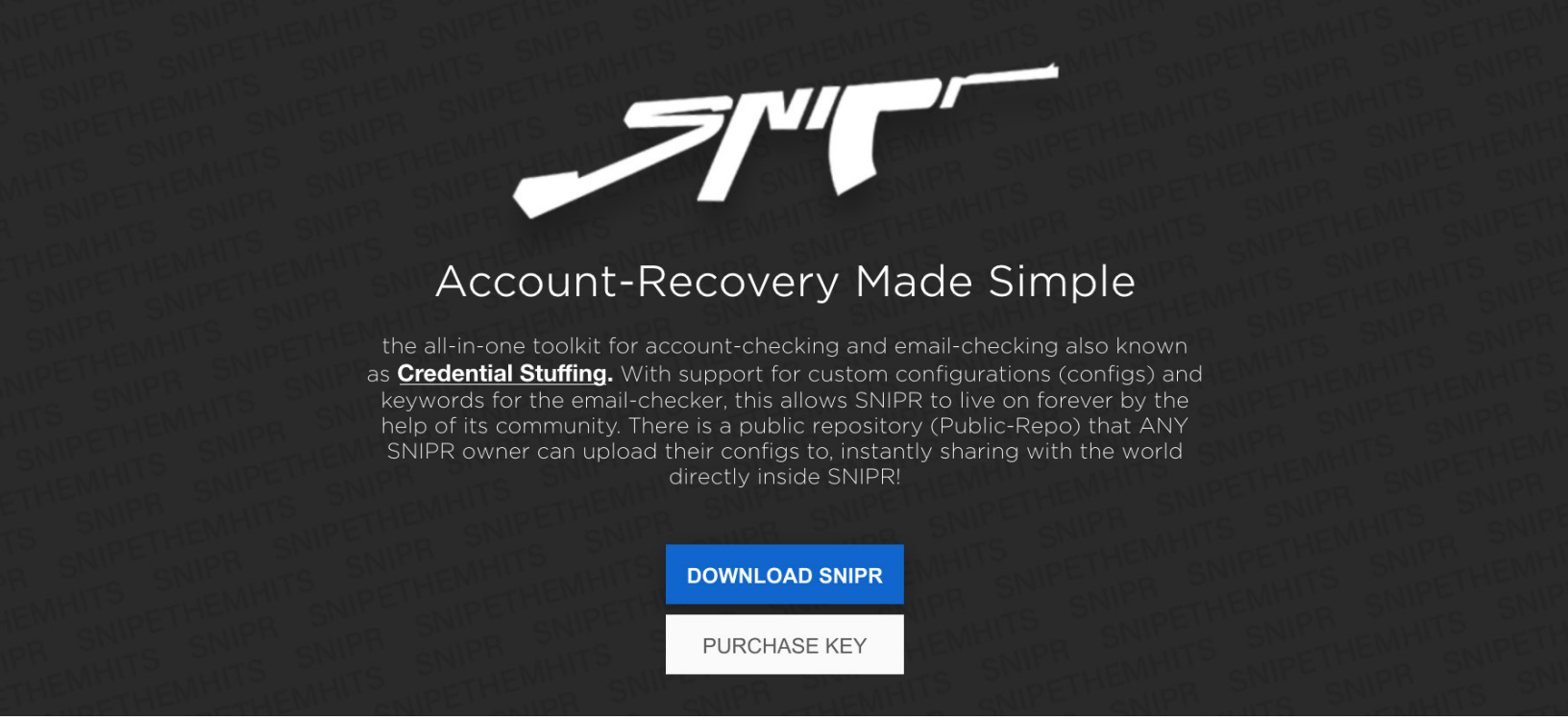


Figura 3

SNIPR es una aplicación AIO de bajo coste para ataques de Credential Stuffing que se vende a un precio de 20 USD.

Con estas cinco colecciones, esta persona anónima publicó aproximadamente 1 TB de información, un total de más de 25 000 millones de combinaciones de correo electrónico y contraseña. Tras eliminar duplicados y registros no válidos, la cifra seguía siendo de miles de millones de combinaciones que, en el momento de publicación de este informe, estaban disponibles en varios sitios online.

Los lotes del 1 al 5 son colecciones básicas de nombres de usuario y contraseñas; sin embargo, representan la colección más grande que se haya divulgado jamás en un solo caso. Esta enorme colección es una excepción, es decir, no suele ser lo habitual. No obstante, pueden crearse colecciones como esta mezclando listas de combinación obtenidas en otras filtraciones de datos, entre las que se incluyen algunas especialmente notables.

Los ataques de Credential Stuffing constituyen un riesgo importante para los negocios online, por lo tanto, disponer de más de mil millones de combinaciones con las que probar allana considerablemente el camino para cualquier delincuente en potencia que quiera sacar tajada económica con el método de Credential Stuffing. Sin embargo, las listas como esta no son la única forma que tienen los delincuentes de recopilar los datos que necesitan para realizar ataques de Credential Stuffing.

En un vídeo de YouTube que vieron los investigadores de Akamai, un individuo ofrecía a los espectadores un tutorial detallado sobre cómo crear listas de combinación para usarlas en un popular videojuego: battle royale.

El tutorial empezaba explicando en qué consistía el concepto "Google Dorking", que utiliza los operadores del motor de búsqueda de Google para localizar sitios web potencialmente vulnerables a la inyección SQL. Una vez que se localizan los sitios web, el tutorial pasa a explicar a los espectadores los métodos para atacar estos dominios vulnerables con una herramienta de inyección SQL corriente. A continuación, esta herramienta descarga direcciones de correo electrónico y contraseñas, descifra contraseñas si es necesario, genera una lista de combinaciones válidas y efectúa un seguimiento con un programa de verificación con proxies para comprobar la validez de la lista generada.

Estos programas de verificación, o aplicaciones AIO, permiten al atacante validar credenciales generadas o robadas. Según el tipo, las aplicaciones AIO pueden apuntar directamente a formularios de inicio de sesión, API o ambos, si la situación lo requiere.

Una vez que se validan las cuentas, pueden venderse, intercambiarse o analizarse para extraer información personal. Dependiendo de la situación, no es nada raro que se lleven a cabo todas las opciones posibles.

Hay decenas de aplicaciones AIO online. Algunas se venden abiertamente, y otras están disponibles en la clandestinidad. Una de estas aplicaciones, SNIPR, es muy apreciada entre aquellos que quieren realizar ataques en juegos, redes sociales y servicios de contenido multimedia en streaming debido a su sencillez.

Otra aplicación AIO, denominada STORM, utiliza parámetros de configuración detallada que se venden o comercializan por separado. En el momento de redactar este informe, un vendedor ofrecía en la Dark Net configuraciones de STORM para usarlas contra una de las plataformas de streaming online más importantes, a un precio de 52 USD.

Esa misma persona vendía también códigos de tarjetas regalo para la plataforma en cuestión por un precio inferior al original, por ejemplo, una tarjeta de 30 USD a tan solo 7,80 USD. Normalmente, se trata de códigos generados, aunque con bastante frecuencia son códigos adquiridos con tarjetas de crédito robadas, por lo que todo son ganancias para el delincuente.

Los negocios de esta persona no terminan ahí: también vende listas de combinaciones para ataques de Credential Stuffing. Una de las ofertas consiste en un lote de 5000 millones de direcciones de correo electrónico y contraseñas aleatorias por 5,20 USD. Otra de las ofertas es una lista personalizada de 50 000 direcciones de correo electrónico y contraseñas por el mismo precio. La opción personalizada permite al comprador elegir el formato (correo electrónico:contraseña o usuario:contraseña), el proveedor, la ubicación, etc.

Vídeos instructivos sobre SNIPR en YouTube

Mientras buscaban datos e información para este informe, los investigadores de Akamai encontraron varios vídeos en YouTube sobre Credential Stuffing y ataques relacionados. Según pudimos constatar, al menos 89 000 personas habían visto los vídeos de demostración y los tutoriales sobre la aplicación AIO conocida como SNIPR.

Hay multitud de vídeos que tratan sobre diferentes versiones de SNIPR y explican el uso de la aplicación, así como la manera de sacar el máximo partido a la inversión en recursos. SNIPR es una herramienta básica, y los tutoriales suelen estar dirigidos a sus usuarios; son los desarrolladores u otros usuarios los encargados de crear estos materiales.

Un mercado en auge

El mercado de las cuentas robadas de servicios de entretenimiento y contenido multimedia está en auge.

Los sectores de medios, videojuegos y entretenimiento son objetivos muy apreciados por delincuentes que quieren hacer negocio con credenciales de acceso e información robada. Las cuentas se venden en grandes lotes, y el objetivo de los delincuentes es dar salida a la mercancía en grandes volúmenes, en lugar de vender las cuentas una a una.

Muchas cuentas afectadas por ataques de Credential Stuffing se venderán por tan solo 3,25 USD. Estas cuentas incluyen una garantía: si las credenciales no funcionan después de la compra, pueden cambiarse sin coste alguno, un servicio que los vendedores ofrecen para que los clientes vuelvan a comprar. El motivo por el que se ofrece este servicio es que las empresas son capaces de detectar cada vez con más rapidez las cuentas afectadas para desactivarlas.

Entonces, ¿cómo es posible el robo de cuentas tras ataques de Credential Stuffing para venderlas en el mercado clandestino? La respuesta es muy simple: el uso compartido de contraseñas.

Los intentos de Credential Stuffing pueden acabar en robo de cuentas porque la gente suele usar la misma contraseña en diferentes sitios web, o bien porque las contraseñas empleadas son muy fáciles de adivinar y se han podido generar las credenciales.

Principales orígenes de los ataques

PAÍS DE ORIGEN	INTENTOS DE INICIO DE SESIÓN
Estados Unidos	4 016 181 582
Rusia	2 509 810 095
Canadá	1 498 554 065
Vietnam	626 028 826
India	625 476 485
Brasil	585 805 408
Malasia	369 345 043
Indonesia	367 090 420
Alemania	354 489 922
China	308 827 351

Figura 4

Principales orígenes de los ataques, ordenados por país; Estados Unidos sigue siendo el origen principal de los ataques de Credential Stuffing.

Principales objetivos de los ataques

PAÍS OBJETIVO	INTENTOS DE INICIO DE SESIÓN
Estados Unidos	12 522 943 520
India	1 208 749 669
Canadá	1 025 445 535
Alemania	760 722 969
Australia	104 655 154
Corea	37 112 529
China	26 173 541
Gibraltar	6 559 360
Países Bajos	4 991 790
Japón	3 424 334
Italia	2 601 632
Francia	1 864 733
Hong Kong	1 305 262

Figura 5

Principales objetivos de los ataques, ordenados por país; Estados Unidos sigue siendo el principal objetivo de los ataques de Credential Stuffing.

Por tanto, la filtración de datos de un solo sitio web o la publicación masiva de combinaciones de nombres de usuario y contraseñas (como las colecciones mencionadas anteriormente) pueden dejar expuesta toda la vida digital de una persona. Cuando sucede esto, es posible crear un kit con toda la información relacionada con dicha persona para venderla.

Como era de esperar, Estados Unidos encabezó la lista de países de origen de ataques de Credential Stuffing. El motivo es que la mayoría de las herramientas de Credential Stuffing se desarrollan allí. Rusia ocupa el segundo puesto, y Canadá, el tercero. Asimismo, Estados Unidos es el país al que van dirigidos la mayoría de los ataques, ya que los objetivos más populares tienen su sede allí.

India y Canadá le siguen con muy poca diferencia entre sí, pero la ventaja de Estados Unidos con respecto a estos países es abismal.

> *Estados Unidos es el principal objetivo de los ataques".*

Una mirada hacia el futuro

El impacto que pueden tener los delincuentes que perpetran ataques de Credential Stuffing en los negocios es muy amplio; las listas de combinación, como las publicadas de manera anónima a principios de año, son solo la punta del iceberg. Cuando un ataque de Credential Stuffing logra su objetivo, la empresa sufre un duro golpe en su reputación (aunque no se le pueda atribuir la culpa) y debe enfrentarse a unos costes operativos mayores en concepto de gastos de respuesta al incidente, personal, comunicación de la crisis y otros gastos asociados.

> *Cuando un ataque de Credential Stuffing logra su objetivo, la empresa sufre un duro golpe en su reputación (aunque no se le pueda atribuir la culpa)...".*

En febrero de 2019, un famoso servicio online para cumplimentación de declaraciones de impuestos envió avisos sobre filtraciones de datos a algunos clientes. El aviso explicaba claramente que se trataba de un ataque de Credential Stuffing, ya que todas las cuentas afectadas usaban contraseñas expuestas en filtraciones de datos en otros sitios. El servicio de declaración de impuestos restableció las contraseñas para evitar el acceso y avisó a los clientes. Aunque el propio servicio no tuvo nada que ver con el incidente, los clientes no tuvieron la misma percepción, y la reacción pública ante la noticia fue un tanto negativa.

Trabajar con un proveedor de soluciones sólidas, capaces de detectar y bloquear los ataques de Credential Stuffing, es vital para evitar este tipo de situaciones. No obstante, abordar la amenaza que plantea el Credential Stuffing no es una cuestión sencilla. Cualquier organización debe contar con una solución de protección a medida, ya que los delincuentes ajustan sus ataques para poder evadir configuraciones y medidas de protección básicas estándar.

Además, no basta con acudir a un proveedor o recurrir a un conjunto de productos para solucionar el problema. Los usuarios deben recibir formación sobre los ataques de Credential Stuffing, phishing y otros riesgos que ponen en peligro la información de sus cuentas. Las empresas deberían hacer especial hincapié en el uso de contraseñas únicas y administradores de contraseñas, así como resaltar el valor de la autenticación multifactorial. En lo que respecta a ATO y scripts AIO, los delincuentes suelen verse en problemas cuando se usa la autenticación multifactorial, un método especialmente eficaz para impedir la mayoría de los ataques.

El refuerzo constante de estas soluciones, administradas del mismo modo que cualquier programa de sensibilización, ha sido una solución eficaz para organizaciones de los sectores financiero y de los videojuegos.

Metodologías

A efectos de este informe, se consideran intentos de Credential Stuffing los intentos fallidos de inicio de sesión en cuentas usando una dirección de correo electrónico como nombre de usuario. Para diferenciarlos de los usuarios reales, que sí pueden escribir, los intentos de uso indebido se identifican mediante dos algoritmos distintos. El primero consiste en una regla volumétrica sencilla que cuenta el número de errores de inicio de sesión en una dirección concreta. La capacidad de detección de Akamai es mucho mayor que la de una sola organización, ya que compara datos de cientos de organizaciones.

El segundo algoritmo utiliza datos de nuestros servicios de detección de bots para identificar Credential Stuffing de botnets y herramientas conocidas. Una botnet bien configurada puede evitar la detección volumétrica repartiendo su tráfico entre varios objetivos, usando un gran número de sistemas en su análisis o repartiendo el tráfico a lo largo del tiempo, entre otras opciones.

La investigación sobre herramientas y tácticas de las botnets de Credential Stuffing se llevó a cabo a mano, con un gran número de búsquedas en Internet y con inteligencia humana.

Créditos

Colaboradores de Estado de Internet / Seguridad

Shane Keats, director de Marketing Global del Sector, Contenido Multimedia y Entretenimiento (investigación en YouTube)

Steve Ragan, investigador y redactor técnico sénior (investigación en el mercado de la Dark Net)

Martin McKeay, director editorial (análisis y datos de ataques de Credential Stuffing)

Personal editorial

Martin McKeay, director editorial

Amanda Fakhreddine, redactora técnica sénior y editora jefe

Steve Ragan, redactor técnico sénior, editor

Gestión del programa

Georgina Morales Hampe, directora creativa del proyecto

Murali Venukumar, director de marketing del programa

Akamai garantiza experiencias digitales seguras a las empresas más importantes del mundo. La plataforma perimetral inteligente de Akamai llega a todas partes, desde la empresa a la nube, lo que permite a nuestros clientes y a sus negocios ser rápidos, inteligentes y seguros. Las mejores marcas del mundo confían en Akamai para lograr su ventaja competitiva gracias a soluciones ágiles que permiten destapar todo el potencial de sus arquitecturas multinube. En Akamai mantenemos las decisiones, las aplicaciones y las experiencias más cerca de los usuarios que nadie; y los ataques y las amenazas, a raya. La cartera de soluciones de seguridad perimetral, rendimiento web y móvil, acceso empresarial y distribución de vídeo de Akamai está respaldada por un servicio de atención al cliente, análisis y una supervisión ininterrumpida durante todo el año sin precedentes. Para descubrir por qué las marcas más importantes del mundo confían en Akamai, visite www.akamai.com, blogs.akamai.com, o siga a @Akamai en Twitter. Puede encontrar los datos de contacto de todas nuestras oficinas en www.akamai.com/locations. Publicado en abril de 2019.