Atención, periodistas: Cibercriminales roban contraseñas y estas son las 5 formas más comunes

Por: Clases de periodismo. 11/11/2022

Debido a que la contraseña es, a menudo, lo único que se interpone entre un ciberdelincuente y los datos personales y financieros, los delincuentes apuntan a robar o descifrar estos inicios de sesión. Una persona promedio tiene 100 credenciales de inicio de sesión para recordar, y este ha ido en aumento en los últimos años. Por lo tanto, no es de extrañar que se elija acortar caminos y, como resultado, la seguridad sufra las consecuencias.

ESET, compañía líder en detección proactiva de amenazas, advierte sobre las 5 formas más comunes en que los cibercriminales roban contraseñas, para estar mejor preparado para minimizar los riesgos de convertirse en víctima y proteger así las cuentas en línea.

Las contraseñas son las llaves virtuales del mundo digital, ya que proporcionan acceso a servicios de banca en línea, correo electrónico y redes sociales, cuentas como Netflix o Uber, así como a todos los datos alojados en el almacenamiento en la nube. Al obtener los inicios de sesión, un cibercriminal podría: · **Robar información de identidad personal y venderla a otros delincuentes en foros.**

- ·Vender el acceso a la cuenta en sí. Los sitios criminales de la dark web comercializan rápidamente estos inicios de sesión. Los compradores podrían utilizar el acceso para obtener desde traslados en taxi gratuitos y streaming de video, hasta viajes con descuento desde cuentas con millas aéreas comprometidas.
- ·Utilizar las contraseñas para desbloquear otras cuentas en las que use la misma clave.

ESET advierte cuáles son las 5 técnicas que más utilizan los ciberdelincuentes para robar contraseñas:

1. Phishing e ingeniería social: La ingeniería social, es un truco psicológico diseñado para convencer a alguien de hacer algo que no debería, y el phishing es la forma de ingeniería social más conocida. Mediante este tipo de ataques los cibercriminales se hacen pasar por entidades legítimas como amigos, familiares, organizaciones públicas y empresas conocidas, etc. El correo electrónico o texto que se reciba se verá auténtico, pero incluirá un enlace malicioso o un archivo adjunto que, en caso de hacer clic en él, descargará malware o llevará a una página que solicitará que ingreses datos personales. Afortunadamente, hay muchas maneras de detectar las señales de advertencia de un ataque de phishing. Los estafadores incluso utilizan llamadas telefónicas para obtener directamente inicios de sesión y otra información personal de sus víctimas, a menudo fingiendo ser ingenieros de soporte técnico. Esto se conoce como vishing (phishing basado en voz).

2. **Malware**: Otra forma popular de obtener contraseñas es a través de malware. Los correos electrónicos de phishing son el vector principal para este tipo de ataque, aunque también se puede ser víctima de malware al hacer clic en un anuncio malicio (publicidad maliciosa o malvertising) o incluso al visitar un sitio web previamente comprometido (drive-by-download). Como ha demostrado muchas veces el investigador de ESET, Lukas Stefanko, el malware podría incluso ocultarse en una aplicación móvil de apariencia legítima, que a menudo se encuentra en tiendas de aplicaciones de terceros.

Existen múltiples variedades de malware que roban información, pero algunos de los más comunes están diseñados para registrar las pulsaciones de teclas o tomar capturas de pantalla de un dispositivo y enviarlas a los atacantes. Entre ellos, los keyloggers.

3. Ataques de fuerza bruta: El número promedio de contraseñas que una persona tiene que administrar aumentó en un estimado del 25% interanual en 2020. Esto trae como consecuencia que la mayoría de las personas se incline por utilizar contraseñas fáciles de recordar (y de adivinar), y que cometa el error de utilizar las

mismas contraseñas para acceder a múltiples sitios y servicios. Sin embargo, lo que muchas veces no se tiene en cuenta es que las contraseñas débiles pueden abrir la puerta a las denominadas técnicas de fuerza bruta para descubrir contraseñas.

Uno de los tipos de fuerza bruta más comunes es el credential stuffing. En este caso, los atacantes vuelcan grandes volúmenes de combinaciones de nombre de usuario/contraseñas previamente comprometidas en un software automatizado. Luego, la herramienta prueba las credenciales en un gran número de sitios con la esperanza de encontrar una coincidencia. De esta manera, los cibercriminales podrían desbloquear varias cuentas con una sola contraseña. El año pasado hubo aproximadamente 193 billones de intentos de este tipo en todo el mundo, según una estimación. Recientemente, el gobierno canadiense ha sido una víctima de este ataque. Otra técnica de fuerza bruta es el password spraying. En este caso, los criminales utilizan software automatizado para probar una lista de contraseñas de uso común contra una cuenta.

4. Por deducción: Aunque los cibercriminales cuentan con herramientas automatizadas para realizar los ataques de fuerza bruta y descubrir contraseñas, a veces ni siquiera las necesitan: incluso las conjeturas simples, a diferencia del enfoque más sistemático utilizado en los ataques de fuerza bruta, pueden servir para hacer el trabajo. La contraseña más común de 2021 fue “123456”, seguida de “123456789”. Y si se recicla la misma contraseña o se usa un derivado cercano para acceder a varias cuentas, entonces se le facilita la tarea a los atacantes, sumando un riesgo adicional de robo de identidad y fraude.

5. Mirar por encima del hombro (Shoulder surfing): Vale la pena recordar algunas de las técnicas para escuchar de manera oculta también representan un riesgo. Esta no es la única razón por la que las miradas indiscretas por encima del hombro de los usuarios sigue siendo un riesgo. Una versión más de alta tecnología, conocida como un ataque “man-in-the-middle” (hombre en el medio) involucra escuchas de Wi-Fi, y puede permitir a los criminales informáticos dentro de conexiones Wi-Fi públicas espiar la contraseña mientras se la ingresa si está conectado a la misma red.

Hay muchas maneras de bloquear estas técnicas, ya sea agregando una segunda forma de autenticación, administrando las contraseñas de manera más efectiva o tomando medidas para detener el robo en primer lugar. ESET acerca los siguientes consejos para proteger las credenciales de inicio de sesión:

- Activar la autenticación de doble factor (2FA) en todas las cuentas
- Utilizar solo contraseñas o frases de contraseña, seguras y únicas en todas las cuentas en línea, especialmente en cuentas bancarias, de correo electrónico y de redes sociales
- Evitar reutilizar tus credenciales de inicio de sesión en varias cuentas y cometer otro de los errores comunes de contraseña · Utilizar un gestor de contraseñas, que almacena contraseñas seguras y únicas para cada sitio y cuenta, haciendo que los inicios de sesión sean simples y seguros · Cambiar la contraseña inmediatamente si un proveedor advierte que los datos pueden haber sido comprometidos
- Usar solo sitios HTTPS para iniciar sesión
- No hacer clic en enlaces ni abrir archivos adjuntos en correos electrónicos no solicitados.
- Solo descargar aplicaciones de tiendas de aplicaciones oficiales.
- Invertir en un software de seguridad de un proveedor de buena reputación para todos los dispositivos
- Asegurarse de que todos los sistemas operativos y aplicaciones están actualizados en su última versión
- Tener cuidado con las miradas indiscretas por encima del hombro en espacios públicos
- Nunca iniciar sesión en una cuenta si se está conectado a una red Wi-Fi pública. En caso que se deba usar una red de este tipo, se recomienda utilizar una VPN

“La extinción de la contraseña ha sido predicha durante más de una década. Sin embargo, las alternativas a menudo tienen dificultades para reemplazar la contraseña en sí, lo cual implica que los usuarios deberán tomar el asunto en sus propias manos. Mantenerse alerta y cuida la seguridad de las credenciales de inicio de sesión es el primer paso para proteger la información personal”, comenta Camilo Gutierrez Amaya, Jefe del Laboratorio de Investigación de ESET Latinoamérica.

Para conocer más sobre seguridad informática ingrese al portal de noticias de

ESET: https://www.welivesecurity.com/la-es/2022/01/11/formas-cibercriminales-roban-contrasenas/

ESET invita a conocer Conexión Segura, su podcast para saber qué está ocurriendo en el mundo de la seguridad informática. Para escucharlo ingrese a: https://open.spotify.com/show/0Q32tisjNy7eCYwUNHphcw

LEER EL ARTÍCULO ORIGINAL PULSANDO AQUÍ

Fotografía: Clases de periodismo

Fecha de creación
2022/11/11