ACTUALIDAD

4 AMENAZAS CORPORATIVAS DIFERENTES AL RANSOMWARE

¡PARA RECORDARi

El ransomware es una clase de software maligno que representa un riesgo para su información y su dispositivo. Su nombre no es por casualidad: el término "ransom" refiere a la palabra "rescate" por lo tanto es un software extorsivo que tiene como finalidad impedir el uso hasta que se pague un costo por su rescate. En este boletín presentamos 4 amenazas que afectan a las empresas.

I. FILTRACIÓN O EXPOSICIÓN DE DATOS

Este ransomware filtra la opción robada buscando extorsionar a las víctimas y dañar su reputación, estos datos usualmente se negocian en foros clandestinos en el que algunos interesados buscan aprovechar esta información para llevar a cabo ataques.

¿CÓMO FUNCIONA?	¿DE QUÉ SE APROVECHA?	EJEMPLO
Al encontrar alguna vulnerabilidad o de algún error humano se infiltran diferentes tipos de datos tanto de la empresa, empleado o aliados estratégicos.	De un acceso por parte de los usuario a los sistemas de cualquier organización.	la infiltración que sufrió la plataforma Twich en 2019 en el que se revelaron 125 Gb de datos sensibles de la plataforma de retransmisiones en directo.

Tomado y adaptado de https://www.welivesecurity.com/eset

2. ATAQUES DE FUERZA BRUTA

Un ataque de fuerza bruta se genera cuando un intruso, utiliza diferentes técnicas (Hardware - Software) buscando probar diferentes combinaciones de contraseñas con la finalidad de descubrir las credenciales de sus víctimas y así lograr el acceso a sus cuentas o plataformas.

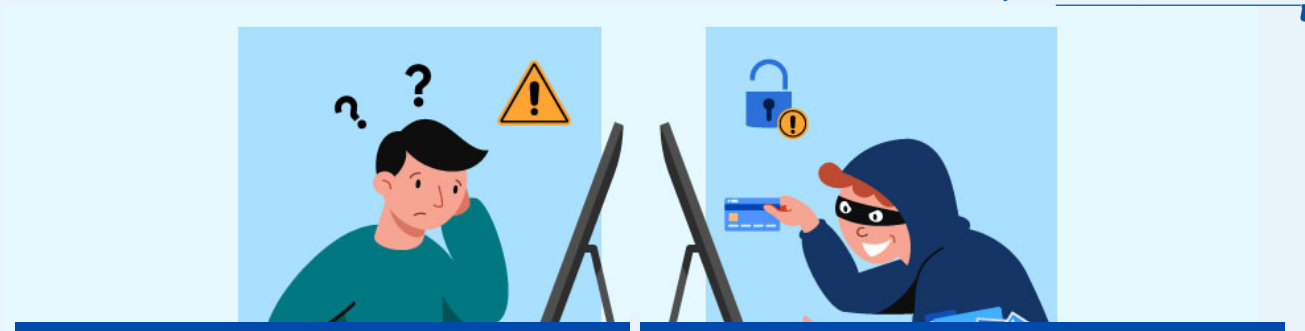
¿CÓMO FUNCIONA?	¿DE QUÉ SE APROVECHA?	EJEMPLO
Uso de software y Hardware automático para descifrar credenciales con contraseñas débiles	Del uso de contraseñas de baja seguridad asignadas por el usuario las cuales son utilizadas en Internet en páginas sitios inseguros.	Ataques a servicios de escritorio remoto durante la pandemia.

3. TROYANOS DE ACCESO REMOTO

Este tipo de malware les brinda herramientas a los atacantes para realizar un gran número de acciones con los equipos infectados. Mediante el uso de comando enviados de manera remota el atacante puede: robar credenciales en navegadores, app de mensajería, keyloggers, capturas de pantallas, interceptar comunicaciones, capturas de pantalla, entre otras.

¿CÓMO FUNCIONA?	¿DE QUÉ SE APROVECHA?	EJEMPLO
Los troyanos de acceso remoto permiten a actores maliciosos realizar a la distancia el envío de comandos, generalmente troyanos que abren la puerta trasera.	De envíos masivos de phishing a los correos electrónicos con enlaces maliciosos o mediante falsas aplicaciones o instaladores de programas.	Espionaje a los equipos utilizando el troyano de acceso remoto Bandook.

Tomado y adaptado de https://www.welivesecurity.com/eset



4. INGENIERÍA SOCIAL

Busca manipular a los usuarios para que invaliden la seguridad de sus dispositivos, hoy encontramos ataques de ingeniería social que utilizan bots de voz para robar códigos de verificación.

¿CÓMO FUNCIONA?

La ingeniera social no requiere de ninguna habilidad técnica por parte del atacante, se valen de estrategias como el spam o el phishing para engañar al usuario.

¿DE QUÉ SE APROVECHA?

De falta de educación de los usuarios en temas relacionadas con la seguridad informática.

EJEMPLO

En el 2021 utilizaron un software basado en inteligencia artificial para imitar la voz de un CEO de una empresa de energía en Alemania, así permitió a los estafadores robar 220.000 euros.

CONCLUSIONES

Las nuevas modalidades de trabajo (remoto e híbrido) hacen un poco más compleja la gestión de la seguridad en una red corporativa, ya que el espectro de control se amplía considerablemente. A razón de la pandemia, los ataques de fuerza bruta fueron unos de los ataques que crecieron significativamente principalmente por actores maliciosos que buscaban desplegar diferentes tipos de programas dañinos buscando la conexión remota del atacante al sistema comprometido.

La gestión de la seguridad informática no solo debe contar con herramientas apropiadas para asegurar la infraestructura, si no también con un componente educativo para lograr un usuario capacitado en materias de seguridad de la información y uso correcto de la gestión de recursos tecnológicos.

Tomado y adaptado de https://www.welivesecurity.com/eset

¡SI PRESENTAS DUDAS O ALGUNA SITUACIÓN SOSPECHOSA CONTÁCTANOSi

Subproceso de Seguridad informática UDES

- En Bucaramanga:
  Correo: seguridadinformatica@udes.edu.co
  Teléfono: (607) 6516500 Ext 1005 - 1001
- En Valledupar
  Correo: lortiz@valledupar.udes.edu.co
  Teléfono: (605) 5730073 Ext 129
- En Cúcuta:
  Correo: wpena@udes.edu.co
  Teléfono: (607) 5748717 Ext 4196