- ¿Qué tipo de amenaza es?
- ¿Cómo comienza y cómo se propaga esta amenaza?
- ¿Hay más de una amenaza aplicada ?

LECTURA 1

- ¿Qué tipo de amenaza es?
    - Es una vulnerabilidad encontrada en sistema de microsoft exchange para simular autenticación de usuarios con permisos desde otras terminales similar al Exploit
- ¿Cómo comienza y cómo se propaga esta amenaza?
    - Fue hallada por un grupo de hacker desde china hacia los servidores de microsfot Exchange y las personas que utilizan el servicio estaban en peligro
- ¿Hay más de una amenaza aplicada ?
    - Fallos de actualización y brechas de seguridad
    - troyano (backdoor)

LECTURA 2

- ¿Qué tipo de amenaza es?
    - Troyano
- ¿Cómo comienza y cómo se propaga esta amenaza?
    - A través de un archivo adjunto en un email, simulando ser un documento bancario como un extracto
- ¿Hay más de una amenaza aplicada ?
    - phishing o suplantación de identidad
    - troyano para activar phishing

LECTURA 3

- ¿Qué tipo de amenaza es?
    - Malware
- ¿Cómo comienza y cómo se propaga esta amenaza?
    - Un email con un archivo adjunto, que al ejecutar despliega una serie de rutinas de consola para descargar programas e instalarse, a cierto modo es un docker de malware ya que permite contener cualquier archivo

malicioso e instalarlo en el computador de la víctima, estos archivos se encuentran alojados en Discord a través de sus cdns.

- ¿Hay más de una amenaza aplicada ?
    - phishing
    - malware

LECTURA 4

- ¿Qué tipo de amenaza es?
  adWare : Crea varios anuncios publicitarios
- ¿Cómo comienza y cómo se propaga esta amenaza?
  Se distribuyeron como aplicaciones legítimas, pero luego se actualizaron para mostrar anuncios maliciosos en pantalla completa a sus usuarios.
- ¿Hay más de una amenaza aplicada ?
  No, pero comprometío la funcionalidad de varias apps

LECTURA 5

- ¿Qué tipo de amenaza es?
  Tekia: Da click en anuncios publicitarios sin que el usuario se de cuenta
- ¿Cómo comienza y cómo se propaga esta amenaza?
  Empieza en aplicaciones para niños
- ¿Hay más de una amenaza aplicada ?
  Generaba ingresos ilegales por medio de los clics dados sin previo conocimiento del ususario

LECTURA 6

- ¿Qué tipo de amenaza es?
  Es una variante del malware publicitario Pirrit
- ¿Cómo comienza y cómo se propaga esta amenaza?
  Comienza ejecutándose en chips Intel x86 para intentar llegar al M1 de Apple
- ¿Hay más de una amenaza aplicada ?

LECTURA 7

- ¿Qué tipo de amenaza es?

Es una vulnerabilidad en el sistema de validacion de URL que causa la ejecucion de archivos maliciosos

- ¿Cómo comienza y cómo se propaga esta amenaza?

Comienza al usar aplicaciones con dicha vulnerabilidad.

- ¿Hay más de una amenaza aplicada ?

  No

LECTURA 8

¿Qué tipo de amenaza es?

Ramsonware

- ¿Cómo comienza y cómo se propaga esta amenaza?

  Se altero una computadora de la empresa y se instalo el ramsonware

- ¿Hay más de una amenaza aplicada ?

No

Lectura 9

- ¿Qué tipo de amenaza es?

  Spyware

- ¿Cómo comienza y cómo se propaga esta amenaza?

  Ataca computadoras conectadas al servicio de seguridad preventivo de Palestina.

- ¿Hay más de una amenaza aplicada ?

  Si, un malware para robar informacion con el motivo de hacer ingenieria social

LECTURA 10

- ¿Qué tipo de amenaza es?

Spyware que permite acceso a la información de cuentas de correo electrónico, también tiene acceso a las pestañas del navegador y a los datos del usuario de todos los sitios web, viene equipada con funciones para buscar, leer y eliminar mensajes e incluso reenviar y enviar correos electrónicos desde la cuenta de Gmail comprometida.

- ¿Cómo comienza y cómo se propaga esta amenaza?

Por una extensión de navegador de mozilla firefox, que permite al acceso a las cuentas de gmail de los usuarios. Esta se propaga por medio de correos electrónicos con un link de youtube que los redirecciona a la extensión y esta toma los datos.

- ¿Hay más de una amenaza aplicada ?

Scanbox es un marco de reconocimiento que permite a los atacantes rastrear a los visitantes a sitios web comprometidos, capturar pulsaciones de teclas y recopilar datos

que podrían usarse para permitir compromisos posteriores. También se informó que se modificó para entregar malware de segunda etapa en hosts específicos.

LECTURA 11

- ¿Qué tipo de amenaza es?

Malware ToxicEye en telegram. Troyano multifuncional de acceso remoto (RAT).

- ¿Cómo comienza y cómo se propaga esta amenaza?
- ¿Hay más de una amenaza aplicada ?