ALERTA: RANSOMWARE HELLO KITTY (02/NOVIEMBRE/2021)

Investigadores alertan de equipos comprometidos con ransomware HELLO KITTY.

Introducción

El 01 de noviembre del 2021, el Centro de Respuesta a Incidentes Informáticos de la ARCOTEL – EcuCERT, recibió de su red de confianza internacional la notificación de afectación a empresas de la contaminación del ransomware HelloKitty (también conocida como FiveHands)y el cambio en sus métodos ha agregado ataques distribuidos de denegación de servicio (DDoS) a su arsenal de tácticas de extorsión, por lo que a fin de que se tomen las respectivas medidas preventivas y correctivas emite esta alerta con información técnica para su mitigación.

Información de HELLO KITTY

HelloKity es una operación de ransomware operada por humanos activa desde noviembre de 2020

HelloKitty se dirige a empresas provee notas de rescate personalizadas, una de las víctimas conocidas es CD Project, el desarrollador de los juegos Cyberpunk 2077, Witcher 3, Gwent; donde robaron el código fuente de sus juegos y los subieron a su sitio de filtración. Otras variantes de este ransomware también han atacado servidores ESXI en el pasado, utilizando un cifrador de Linux para cifrar datos.

HelloKitty también es conocido por robar documentos confidenciales de los servidores comprometidos de las víctimas antes de cifrarlos. Los archivos exfiltrados se utilizan más tarde como palanca para presionar a las víctimas a

pagar el rescate bajo la amenaza de filtrar los datos robados en línea en un sitio de filtración de datos.

Este ransomware cambia el nombre de los archivos encriptados. Agrega la extensión "**.crypted**" a sus nombres de archivo. Por ejemplo, cambia el nombre de "**1.jpg**" a "**1.jpg.crypted**", "**2.jpg**" a **"2.jpg.crypted**", y así sucesivamente. HelloKitty también crea el archivo "**read_me_unlock.txt**" (nota de rescate).

El grupo de ransomware ha indicado que derribaría los sitios web oficiales de sus víctimas en ataques DDoS si no cumplían con las demandas de rescate.

El ransomware HelloKitty o sus variantes también se han utilizado con otros nombres, incluidos DeathRansom y Fivehands

Vector de ataque:

El ransomware se propaga a través de spam, troyanos, herramientas de actualización de software falsas, herramientas de "craqueo" y canales cuestionables para descargar software y archivos. La mayoría de los correos electrónicos de spam contienen archivos adjuntos o enlaces de descarga para archivos maliciosos como Microsoft Office, documentos PDF, archivos ejecutables como .exe, archivos de almacenamiento como ZIP, RAR y JavaScript.

Ejemplo de correo solicitando el pago:

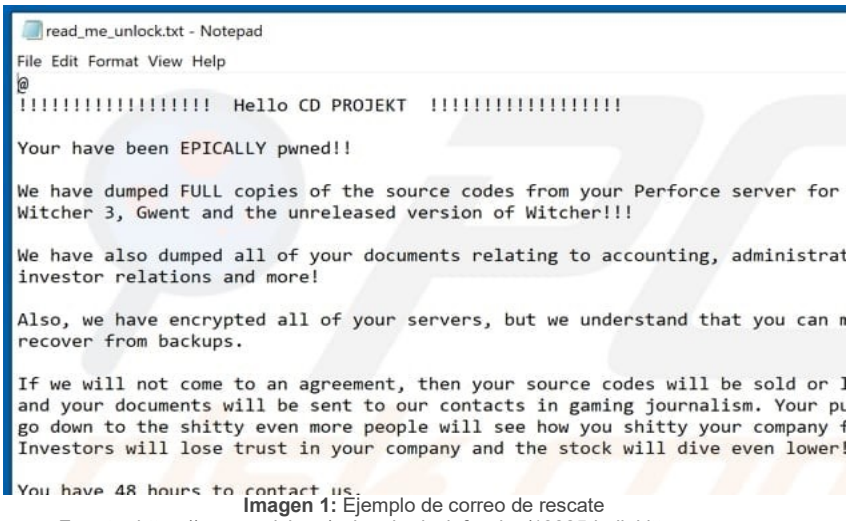

Imagen 1: Ejemplo de correo de rescate
Fuente: https://www.pcrisk.es/guias-de-desinfeccion/10385-hellokitty-ransomware

Captura de imagen de archivos encriptados:

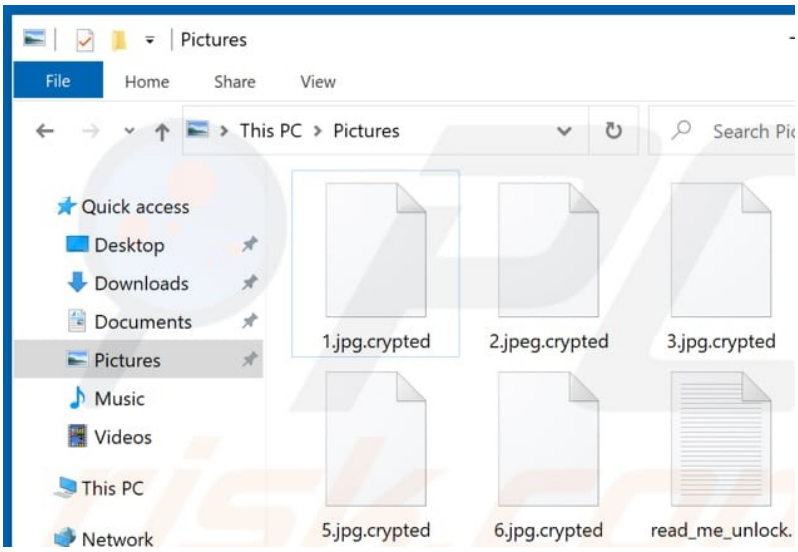

Imagen 2: Caputura de pantalla de archivos encriptados
Fuente: https://www.pcrisk.es/guias-de-desinfeccion/10385-hellokitty-ransomware

Nombres de detección:

- Avast (FileRepMalware),
- BitDefender (Gen:Variant.Razy.801167),
- ESET-NOD32 (A Variant Of Win32/Filecoder.DeathRansom.D),
- Kaspersky (HEUR:Trojan-Ransom.Win32.Generic),
- Microsoft (Ransom:Win32/KittyCrypt.CM!MTB),
- Lista Completa de Detecciones (VirusTotal)

En consideración al alto riesgo contra la confidencialidad de los sistemas de información al ser afectados por un ransomware, el EcuCERT recomienda a su comunidad objetivo, tomar en consideración lo siguiente ante la materialización de un ataque:

Paso 1: Aislar el equipo infectado de la red y notificar a las autoridades.

Paso 2: Identificar el ransomware que produce la infección.

Paso 3: Búsqueda de herramientas de desencriptado de ransomware.

Paso 4: Restaurar archivos con herramienta de recuperación de datos.

Paso 5: Crear copias de seguridad de datos.

Se recomiendan las siguientes medidas preventivas:

- No abra archivos adjuntos de correo electrónico con enlaces que se reciben de remitentes desconocidos y sospechosos.
- Descargue archivos y software de páginas web oficiales confiables y mediante enlaces directos.
- No utilice instaladores de terceros.
- Activar o actualizar el software de su equipo utilizando funciones o herramientas implementadas por los desarrolladores oficiales.
- Utilice software con licencia de uso habilitada por el desarrollador o fabricante.
- Realice un escaneo del sistema operativo con aplicativos especializados en busca de malware y otras amenazas con regularidad.
- Utilice antivirus o anti-spyware en su equipo, verifique que este siempre actualizado.

Referencias

Sergiu Gatlan(01-nov-2021). FBI: el ransomware HelloKitty agrega ataques DDoS a las tácticas de extorsión. Recuperado el 01 de noviembre de 2021. Disponible en https://www.bleepingcomputer.com/news/security/fbi-hellokitty-ransomware-adds-ddos-attacks-to-extortion-tactics/

Tomas Meskauskas(2-mar-2021). Instrucciones de eliminación del ransomware HelloKitty. Recuperado el 01 de noviembre de 2021. Disponible en https://www.pcrisk.es/guias-de-desinfeccion/10385-hellokitty-ransomware

(11-03-2021). ¿Qué es el HelloKitty Ransomware?. Recuperado el 01 de noviembre de 2021. Disponible en https://purelysandy.com/what-is-the-hellokitty-ransomware.