ALERTA: AFECTACIÓN POR RANSOMWARE (19/JULIO/2021)

Investigadores alertan de equipos comprometidos con RANSOMWARE de la familia RANSOMEXX en redes del Ecuador.

Introducción

El Centro de Respuesta a Incidentes Informáticos de la ARCOTEL – EcuCERT, dentro de su gestión y como parte del apoyo recibió de su red de confianza nacional la notificación de posibles afectaciones a organizaciones en el país, por la contaminación con el ransomware de la familia RANSOMEXX, por lo que a fin de que se tomen las respectivas medidas preventivas y correctivas emite esta alerta, con información técnica para su mitigación.

Este ransomware inició con el nombre de Defray en 2018, pero se volvió más peligroso en junio de 2020 cuando cambió su nombre a RansomEXX (Ransom X, AKA Defray777, Ransom.exx o RansomExx) y comenzó a apuntar a grandes entidades corporativas,.

RansomEXX ingresa a una red a través de credenciales comprometidas por ataques previos tipo phishing, ataques de fuerza bruta a conexiones de escritorio remoto RDP y/o mediante la utilización de exploits hacia sistemas no parchados.

Una vez que obtienen el acceso, se propaga silenciosamente por toda la red, mientras roba archivos no cifrados para usarlos en intentos de extorsión posteriores.

Finalmente, luego de obtener acceso a una contraseña de administrador, implementa el ransomware en la red y cifran todos sus dispositivos.

Como se está volviendo común entre las operaciones de ransomware, RansomEXX creó una versión de Linux para garantizar que puedan apuntar a todos los servidores y máquinas virtuales críticos; como el nuevo troyano de

cifrado de archivos construido como un ejecutable ELF y destinado a cifrar datos en máquinas controladas por sistemas operativos basados en Linux.

RansomEXX es un troyano muy específico. Cada muestra del malware contiene un nombre codificado de la organización víctima. Además, tanto la extensión del archivo cifrado como la dirección de correo electrónico para contactar con los extorsionadores hacen uso del nombre de la víctima.

Descripción técnica

Cuando se ejecuta RansomEXX, este interrumpe una variedad de procesos de seguridad, herramientas de administración remota y servidores de bases de datos. Luego, toma más medidas para obstruir los intentos de recuperación, incluido el borrado de los registros de eventos de Windows, la eliminación de diarios NTFS, la desactivación de Restaurar sistema y el Entorno de recuperación de Windows, la eliminación de catálogos de copia de seguridad de Windows y la limpieza del espacio libre en el almacenamiento local.

Cuando RansomEXX cifra los datos, agrega una extensión personalizada asociada con la víctima a los nombres de archivo afectados. Una nota de rescate llamada *! [Extensión] _READ_ME! .Txt* se guarda en cada directorio cifrado. Esta nota incluye el nombre de la organización de la víctima, una dirección de correo electrónico para contactar e instrucciones sobre cómo pagar el rescate. Mientras se ejecuta, RansomEXX muestra una consola en pantalla con información sobre el proceso de cifrado.

La muestra hash MD5 encontrada aa1ddf0c8312349be614ff43e80a262f , es un ejecutable ELF de 64 bits, que implementa su esquema criptográfico utilizando funciones de la biblioteca de código abierto mbedtls.

Cuando se inicia, el troyano genera una clave de 256 bits y la utiliza para cifrar todos los archivos que pertenecen a la víctima a los que puede acceder, utilizando el cifrado de bloque AES en modo ECB; la clave AES está encriptada por una clave pública RSA-4096 incrustada en el cuerpo del troyano y adjunta a cada archivo encriptado. El malware lanza un hilo que regenera y vuelve a cifrar la clave AES cada 0,18 segundos; sin embargo, según un análisis de la implementación, las claves en realidad solo difieren cada segundo.

Además de cifrar los archivos y dejar notas de rescate, la muestra no tiene ninguna de las funciones adicionales que otros actores de amenazas tienden a usar en sus troyanos: sin comunicación C&C, sin terminación de procesos en ejecución, sin trucos anti-análisis, etc.

```
if ( a1 )
{
  v10 = strlen(s) + 277;
  v2 = alloca(16 * ((v10 + 23LL) / 0x10uLL));
  dest = (16 * ((&s + 7) >> 4));
  if ( dest )
  {
    strcpy(dest, s);
    strcat(dest, ".[redacted]");
    v3 = rand();
    sprintf(src, "-%08x", v3);
    strcat(dest, src);
    if ( fsize(dest) == -1 )
    {
      stream = fopen64(s, "r+");
      if ( stream )
      {
        v9 = fsize(s);
        if ( v9 )
        {
          if ( v9 > 15 )
          {
            mbedtls_aes_init(aes_ctx);
            pthread_mutex_lock(&csPreData);
            qmemcpy(ptr, &g_RansomHeader, 0x200uLL);
            mbedtls_aes_setkey_enc(aes_ctx, &g_KeyAES, 256LL);
            pthread_mutex_unlock(&csPreData);
            if ( !fseek(stream, 0LL, SEEK_END)
              && fwrite(ptr, 1uLL, 0x200uLL, stream)
              && !fseek(stream, -512 - v9, 1)
              && ProcessFileHandleWithLogic(stream, aes_ctx, a2, v9, CryptOneBlock) )
            {
              v13 = 1;
            }
```

Fragmento del pseudocódigo del procedimiento de cifrado de archivos; Los nombres de variables y funciones se guardan en la información de depuración y deben coincidir con el código fuente original.

El binario ELF contiene información de depuración, incluidos nombres de funciones, variables globales y archivos de código fuente utilizados por los desarrolladores de malware.

Nombres originales de los archivos fuente incrustados en el cuerpo del troyano

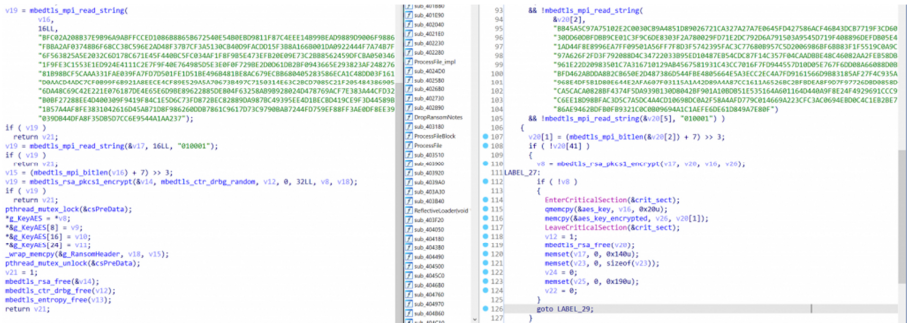
Registro de ejecución del troyano en Linux Sandbox

Similitudes con las compilaciones de Windows de RansomEXX

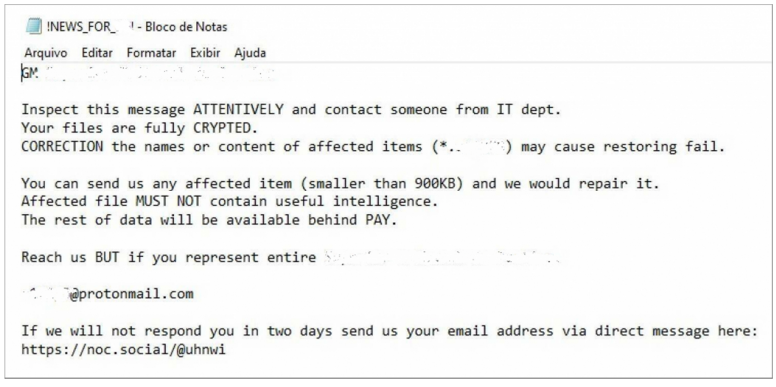
A pesar del hecho de que las compilaciones PE de RansomEXX previamente descubiertas usan WinAPI (funciones específicas del sistema operativo Windows), la organización del código del troyano y el método de uso de funciones específicas de la biblioteca mbedtls sugieren que tanto ELF como PE pueden derivarse de la misma fuente código.

En la captura de pantalla a continuación, vemos una comparación de los procedimientos que cifran la clave AES. A la izquierda está la muestra de ELF aa1ddf0c8312349be614ff43e80a262f; a la derecha está la muestra de PE fcd21c6fca3b9378961aa1865bee7ecb utilizada en el ataque TxDOT.

A pesar de estar construido por diferentes compiladores con diferentes opciones de optimización y para diferentes plataformas, la similitud es bastante obvia.



También observamos semejanzas en el procedimiento que cifra el contenido del archivo y en el diseño general del código. El texto de la nota de rescate también es prácticamente el mismo, con el nombre de la víctima en el título y una redacción equivalente. A continuación la nota de rescate de la muestra aa1ddf0c8312349be614ff43e80a262f



!NEWS_FOR_ [redacted] - Bloco de Notas

Arquivo Editar Formatar Exibir Ajuda

GM [redacted]

Inspect this message ATTENTIVELY and contact someone from IT dept.
Your files are fully CRYPTED.
CORRECTION the names or content of affected items (*.. [redacted]) may cause restoring fail.

You can send us any affected item (smaller than 900KB) and we would repair it.
Affected file MUST NOT contain useful intelligence.
The rest of data will be available behind PAY.

Reach us BUT if you represent entire [redacted]

[redacted]@protonmail.com

If we will not respond you in two days send us your email address via direct message here:
https://noc.social/@uhnwi

Nota de rescate de la publicación de Bleeping Computer sobre el ataque más reciente en Brasil

Segmentación de VMWare ESXi

Recientemente se ha observado que el actor de amenazas que controla RansomEXX explota vulnerabilidades en VMWare ESXi para apagar máquinas virtuales y cifrar dispositivos de almacenamiento virtual directamente en el hipervisor. Una vez que se ha obtenido el acceso inicial a una red, se envían mensajes maliciosos del Protocolo de ubicación de servicio (SLP) para tomar el control del dispositivo ESXi.

Los administradores de VMWare ESXi deben asegurarse de que se hayan aplicado todas las actualizaciones de seguridad recientes. El Protocolo de ubicación del servicio (SLP) también puede desactivarse para ayudar a prevenir un ataque exitoso, si no es necesario.

Comportamiento del atacante

El monitoreo realizado permite identificar que el atacante utiliza los puertos 445, 423 y 427 inicialmente, tiene un comportamiento polimórfico que se evidencia al realizar el monitoreo en el que se identifica el uso de los puertos 2000 y 8329 con tráfico UDP y TCP.

Consejos de remediación

Si un dispositivo de su red se infecta con ransomware, comenzará a cifrar archivos, que también pueden incluir archivos remotos en ubicaciones de red. La única forma garantizada de recuperarse de una infección de ransomware es restaurar todos los archivos afectados desde su copia de seguridad más reciente. Para limitar el impacto de una infección de ransomware, el Centro de Respuesta a Incidentes Informáticos – EcuCert recomienda:

- Guardar los datos críticos en copias de seguridad en ubicaciones diversas.
- Mantener al menos una copia de seguridad fuera de línea, disponible en cualquier momento (separada de los sistemas activos).
- Probar las copias de seguridad y los planes de recuperación de incidentes, para garantizar que los datos se puedan restaurar cuando sea necesario.
- Revisar periódicamente los permisos de la cuenta de usuario para modificar datos y limitarlos al mínimo posible.
- Desconectar de la red y se apagar los sistemas infectados, tan pronto como sea posible.
- Restablecer en un dispositivo limpio cualquier credencial de cuenta de usuario que pueda haber sido comprometida.
- Desconectar la infraestructura infectada de las redes nacionales, para limitar la propagación, cuando los sistemas infectados no se pueden poner en cuarentena o con el nivel de confianza adecuado.

Además, para prevenir y detectar una infección, se sugiere:

- Las configuraciones seguras se aplican a todos los dispositivos.
- Las actualizaciones de seguridad se aplican lo antes posible.
- La configuración de protección contra manipulaciones en los productos de seguridad está habilitada cuando está disponible.
- Las plataformas obsoletas están segregadas del resto de la red.
- Las políticas de uso de TI se refuerzan con capacitación periódica para garantizar que todos los usuarios sepan que no deben abrir vínculos o archivos adjuntos no solicitados.
- La autenticación multifactor (MFA) y las políticas de bloqueo se utilizan cuando es posible, especialmente para las cuentas administrativas.
- Las cuentas administrativas solo se utilizan para los fines necesarios.
- Los servicios de administración remota utilizan protocolos fuertemente encriptados y solo aceptan conexiones de usuarios o ubicaciones autorizados.
- Los sistemas se monitorean continuamente y se investiga la actividad inusual, de modo que se pueda detectar un compromiso de la red lo antes posible.
- Tomar en cuenta las guías de seguridad para configurar de forma segura dispositivos de usuario final (EUD).

Indicadores de compromiso

Versión reciente de Linux: aa1ddf0c8312349be614ff43e80a262f
Versión anterior de Windows: fcd21c6fca3b9378961aa1865bee7ecb

Indicadores de Host

Hashes MD5

- 4bb2f87100fca40bfbb102e48ef43e65
- 80cfb7904e934182d512daa4fe0abbfb

Hashes SHA1

- 3bf79cc3ed82edd6bfe1950b7612a20853e28b0
- 9df15f471083698b818575c381e49c914dee69de

Referencias

NHS Digital (03-jul-2020 actualizado el 05-feb-2021). Recuperado el 18 de julio del 2021. Disponible en https://digital.nhs.uk/cyber-alerts/2020/cc-3532

Sinistsyn. F, Kuskov. V, El troyano RansomEXX ataca los sistemas Linux (06-nov-2020). Recuperado el 18 de julio del 2021. Disponible en: https://securelist.com/ransomexx-trojan-attacks-linux-systems/99279/