ALERTA: AFECTACIÓN POR MALWARE AZORULT (05/JULIO/2021)

Investigadores alertan de equipos comprometidos con malware AZORULT en equipos de redes del Ecuador.

Introducción

En junio 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 ciudadanos de la contaminación del malware AZORULT, 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 del Malware AZORULT

El malware AZORULT se descubrió por primera vez en 2016 como un ladrón de información que roba el historial de navegación, cookies, ID / contraseñas, información de criptomonedas y más. También puede actuar como descargador de otro malware. Se vendió en foros clandestinos rusos para recopilar varios tipos de información confidencial de una computadora infectada. Una variante de este malware pudo crear una nueva cuenta de administrador oculta en la máquina para establecer una clave de registro para establecer una conexión de Protocolo de escritorio remoto (RDP).

Los kits de explotación como Fallout Exploit Kit (EK) y los correos de phishing con técnica de ingeniería social son ahora los principales vectores de infección del malware AZORult. Otras familias de malware como Ramnit y Emotet también descargan AZORult. Los correos electrónicos actuales de malspam y phishing utilizan solicitudes de pedidos de productos, documentos de facturas y solicitudes de información de pago falsas. Este troyano-spyware se conecta a los servidores de comando y control (C&C) del atacante para enviar y recibir información.

Comportamientos

- Roba datos de la computadora, como los programas instalados, el identificador único global (GUID) de la máquina, la arquitectura del sistema, el idioma del sistema, el nombre de usuario, el nombre de la computadora y la versión del sistema operativo (SO)

- Roba la información de la cuenta almacenada utilizada en diferentes clientes de Protocolo de transferencia de archivos (FTP) o software de administración de archivos instalados
- Roba las credenciales de correo electrónico almacenadas de diferentes clientes de correo
- Roba nombres de usuario, contraseñas y nombres de host de diferentes navegadores
- Roba carteras de bitcoin - Monero y uCoin
- Roba credenciales de Steam y telegram
- Roba el historial y los mensajes de chat de Skype
- Ejecuta comandos de puerta trasera de un usuario malintencionado remoto para recopilar información del protocolo de Internet (IP) del host, descargar / ejecutar / eliminar archivos

Capacidades

- Robo de información
- Comandos de puerta trasera
- Exploits
- Descargar rutina

Impacto

- Comprometer la seguridad del sistema: con capacidades de puerta trasera que pueden ejecutar comandos maliciosos, descargar e instalar malwares adicionales.
- Violación de la privacidad del usuario: recopila y roba las credenciales de usuario de varias aplicaciones

Ejemplo de correo no deseado: correo no deseado de consultas de envío

From : ctnprincipal@inscape.co.za Date Time : 9/4/2019 10:05:07 PM

To : [redacted]

Cc :

Bcc :

Subject : Re: As Agreed

Attachments : attachedFile.rtf Attachment_747547567546754675090978236327345634 34.img

[EXTERNAL EMAIL] Verify sender before clicking on links or attachments

Good day,

Kindly find the below documents as you requested, Please Sign on the last 3 pages where your initials and Banking informations are then we can proceed with payment.

Your soonest response will be highly appreciated.

Best Regards
Njisuh Zebedee
Assistant Manager
1 Forssman Close, Barbeque Downs 16185
Fax: 0822748278

Detalles técnicos de instalación

TAMAÑO DEL ARCHIVO: 965,120 bytes
TIPO DE ARCHIVO: EXE
RESIDENTE DE LA MEMORIA: Sí
FECHA DE RECEPCIÓN DE LAS MUESTRAS INICIALES: 12 de mayo de 2020

Detalles de llegada

Este troyano llega a un sistema como un archivo arrojado por otro malware o como un archivo descargado sin saberlo por los usuarios cuando visitan sitios maliciosos.

Instalación

Este troyano agrega los siguientes procesos:

- "% Windows% \\ Microsoft.NET \\ Framework \\ v4.0.30319 \\ InstallUtil.exewT \ xc3 \ xa2A"

(Nota: *% Windows%* es la carpeta de Windows, donde suele ser C: \ Windows en todas las versiones del sistema operativo Windows).

Crea las siguientes carpetas:

- % Raíz del sistema% \ {computername}
- % Raíz del sistema% \ {nombre de equipo} \ XofKna

(Nota: *% System Root%* es la carpeta raíz de Windows, donde suele ser C: \ en todas las versiones del sistema operativo Windows).

Técnica de inicio automático

Este troyano agrega las siguientes entradas de registro para permitir su ejecución automática en cada inicio del sistema:

```
HKEY_CURRENT_USER \ Software \ Microsoft \
Windows \ CurrentVersion \ Run
XofKn = "% raíz del sistema% \ {nombre de equipo} \ XofKna \
XofKnalKR.vbs"
```

Archivos instalados

Este troyano suelta los siguientes archivos:

- % Raíz del sistema% \ {nombre de equipo} \ XofKna \ XofKnalKR.vbs
- % Raíz del sistema% \ {nombre de equipo} \ XofKna \ XofKn.exe

(Nota: *% System Root%* es la carpeta raíz de Windows, donde suele ser C: \ en todas las versiones del sistema operativo Windows).

En consideración al alto riesgo contra la confidencialidad de los sistemas de información en los cuales se encuentren infectados con el Malware Azorult, el EcuCERT recomienda a su comunidad objetivo, tomar en consideración las siguientes recomendaciones:

Paso 1

Antes de realizar cualquier escaneo, los usuarios de Windows 7, Windows 8, Windows 8.1 y Windows 10 deben deshabilitar *Restaurar sistema* para permitir el escaneo completo de sus computadoras.

Paso 2

Reiniciar en modo seguro:

El modo seguro es un modo de software o sistema operativo donde se realizan la mayoría de las correcciones. Es un modo de diagnóstico. Algunos programas maliciosos deben eliminarse en este modo.

Para los sistemas operativos Windows, puede seguir estos pasos según el sistema operativo instalado en su computadora:

• En Windows 7 y Windows Server 2008 (R2)

- Reinicia tu computadora.
- Presione *F8* después de que *finalice* la rutina de autoprueba de encendido (POST). Si no aparece el menú *Opciones de arranque avanzadas* , intente reiniciar y luego presione *F8* varias veces después de que se muestre la pantalla POST.
- En el menú *Opciones de arranque avanzadas* , use las teclas de flecha para seleccionar la opción *Modo seguro* y luego presione *Entrar* .

• En Windows 8, Windows 8.1 y Windows Server 2012 (R2)

- Acceda a la *barra de* accesos moviendo el puntero del mouse a la esquina superior derecha de la pantalla.
- Mueva el puntero del mouse hacia abajo y haga clic en *Configuración> Cambiar la configuración de su PC* .
- En el panel de la izquierda, haz clic en General.

- En el panel derecho, desplácese hacia abajo hasta la parte inferior para encontrar la sección *Inicio avanzado* , luego haga clic en el botón *Reiniciar ahora* y espere a que el sistema se reinicie.
- En el menú *Inicio avanzado* , haga clic en *Solucionar problemas> Opciones avanzadas> Configuración de inicio> Reiniciar* y espere a que el sistema se reinicie.
- En el menú *Configuración de inicio* , presione *4* para habilitar el modo seguro.

• En Windows 10

- Presione la *tecla del logotipo de Windows + I* en su teclado para abrir Configuración. Si eso no funciona, seleccione el botón *Inicio* , luego seleccione *Configuración* .
- Seleccione *Actualización y seguridad* > *Recuperación* .
- En *Inicio avanzado* , seleccione *Reiniciar ahora* .
- Después de que su PC se reinicie en la pantalla *Elija una opción* , seleccione *Solucionar problemas* > *Opciones avanzadas* > *Configuración de inicio* > *Reiniciar* .
- Después de que su PC se reinicie, verá una lista de opciones. Seleccione *4* o presione *F4* para iniciar su PC en Modo seguro.

Paso 3

Identificar y eliminar archivos detectados como Trojan.MSIL.AZORULT.USMANR

- Es posible que el Administrador de tareas de Windows no muestre todos los procesos en ejecución.
- Si el archivo detectado se muestra en el Administrador de tareas de Windows o en el Explorador de procesos pero no puede eliminarlo, reinicie su computadora en modo seguro.

- Si el archivo detectado no se muestra en el Administrador de tareas de Windows o en el Explorador de procesos, continúe con los siguientes pasos.

Paso 4

Eliminar este valor de registro:

Importante: la edición incorrecta del *Registro de Windows* puede provocar un mal funcionamiento irreversible del sistema. Realice este paso solo si sabe cómo hacerlo o puede solicitar ayuda al administrador del sistema. De lo contrario, consulte este artículo de Microsoft antes de modificar el registro de su computadora.

- En *HKEY_CURRENT_USER* \ *Software* \ *Microsoft* \ *Windows* \ *CurrentVersion* \ *Run*
  - **XofKn = "% raíz del sistema% \ {nombre de equipo} \ XofKna \ XofKnalKR.vbs"**

Para eliminar el valor de registro que creó este malware / grayware:

1. Abra el Editor del registro.

   »Para usuarios de Windows 7 y Windows Server 2008 (R2), haga clic en el botón *Inicio* , escriba **regedit** en el campo de entrada de *búsqueda* y presione *Entrar* .
   »Para usuarios de Windows 8, Windows 8.1, Windows 10 y Windows Server 2012 (R2), haga clic con el botón derecho en la *esquina inferior izquierda de la pantalla* , haga clic en *Ejecutar* , escriba **regedit** en el cuadro de texto proporcionado y luego presione *Entrar* .

2. En el panel izquierdo, haga doble clic en lo siguiente: HKEY_CURRENT_USER> Software> Microsoft> Windows> CurrentVersion> Ejecutar

3. En el panel derecho, busque y elimine la entrada: **XofKn = "% System Root% \ {computername} \ XofKna \ XofKnalKR.vbs"**
4. Cierre el Editor del registro.

Paso 5

Busque y elimine estos componentes

Es posible que algunos componentes estén ocultos. Asegúrese de marcar la casilla de verificación *Buscar archivos y carpetas ocultos* en la opción "Opciones más avanzadas" para incluir todos los archivos y carpetas ocultos en el resultado de la búsqueda.

- % Raíz del sistema% \ {nombre de equipo} \ XofKna \ XofKnalKR.vbs
- % Raíz del sistema% \ {nombre de equipo} \ XofKna \ XofKn.exe

Para eliminar manualmente un archivo de malware / grayware de un sistema afectado:

• Para Windows 7, Windows Server 2008 (R2), Windows 8, Windows 8.1, Windows 10 y Windows Server 2012 (R2):

- Abra una ventana del Explorador de Windows.
  - *Para usuarios de Windows 7 y Server 2008 (R2),* haga clic en *Inicio> Equipo* .
  - *Para los usuarios de Windows 8, 8.1, 10 y Server 2012 (R2),* haga clic con el botón derecho en la *esquina inferior izquierda de la pantalla* y luego haga clic en *Explorador de archivos* .
- En el cuadro de entrada *Buscar equipo / Este equipo* , escriba:

  - % Raíz del sistema% \ {nombre de equipo} \ XofKna \ XofKnalKR.vbs

- % Raíz del sistema% \ {nombre de equipo} \ XofKna \ XofKn.exe
- Una vez localizado, seleccione el archivo y luego presione *MAYÚS + SUPR* para eliminarlo.
  *** Nota:** Lea la siguiente página de Microsoft si estos pasos no funcionan en Windows 7 y Windows Server 2008 (R2).

Paso 6

Busque y elimine estas carpetas

Asegúrese de marcar la casilla de verificación *Buscar archivos y carpetas ocultos* en la opción Opciones más avanzadas para incluir todas las carpetas ocultas en el resultado de la búsqueda.

- % Raíz del sistema% \ {computername}
- % Raíz del sistema% \ {nombre de equipo} \ XofKna

Para eliminar carpetas de malware / grayware / spyware:

Para Windows 7, Windows Server 2008 (R2), Windows 8, Windows 8.1, Windows 10 y Windows Server 2012 (R2):

- Abra una ventana del Explorador de Windows.
  - *Para usuarios de Windows 7 y Server 2008 (R2),* haga clic en *Inicio> Equipo* .
  - *Para los usuarios de Windows 8, 8.1, 10 y Server 2012 (R2),* haga clic con el botón derecho en la *esquina inferior izquierda de la pantalla* y luego haga clic en *Explorador de archivos* .
- En el cuadro de entrada *Buscar equipo / Este equipo* , escriba:

  - % Raíz del sistema% \ {computername}
  - % Raíz del sistema% \ {nombre de equipo} \ XofKna
- Una vez localizado, seleccione el archivo y luego presione *MAYÚS + SUPR* para eliminar permanentemente la carpeta.

- Repita los pasos 2-3 para las carpetas restantes:
  - % Raíz del sistema% \ {computername}
  - % Raíz del sistema% \ {nombre de equipo} \ XofKna

  *** Nota:** Lea la siguiente página de Microsoft si estos pasos no funcionan en Windows 7 y Server 2008 (R2).

Paso 7

Reinicie en modo normal y escanee su computadora con su aplicación de antivirus.

Referencias

TrendMicro - Azorult Malware information (20-dic-2019). Recuperado el 30 de mayo del 2021. Disponible en https://success.trendmicro.com/solution/000146108-AZORULT-Malware-Information

TrendMicro - Trojan. MSIL.AZORULT.USMANR (12-may-2020). Recuperado el 30 de mayo de 2021. Disponible en: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/trojan.msil.azorult.usmanr/

Trendmicro - Modo Seguro. Recuperado el 30 de mayo de 2021. Disponible en: https://www.trendmicro.com/vinfo/us/security/definition/safe-mode