Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

RORSCHACH: UN NUEVO RANSOMWARE SOFISTICADO Y RÁPIDO.

05 /Abril /2023

CONTENIDO.

INTRODUCCIÓN.

Mientras respondía a un caso de ransomware contra una empresa con sede en los EE. UU., el CPIRT se encontró recientemente con una cepa de ransomware única implementada utilizando un componente firmado de un producto de seguridad comercial. A diferencia de otros casos de ransomware, el autor de la amenaza no se escondió detrás de ningún alias y parece no estar afiliado a ninguno de los grupos de ransomware conocidos. Esos dos hechos, rarezas en el ecosistema de ransomware, despertaron el interés de CPR y nos impulsaron a analizar a fondo el malware recién descubierto.

RORSCHACH: UN NUEVO RANSOMWARE SOFISTICADO Y RÁPIDO.

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2023_04_05_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	05/04/2023
Es día cero (0 day):	No

RESUMEN

El nuevo ransomware exhibió características únicas. Un análisis de comportamiento del nuevo ransomware sugiere que es parcialmente autónomo y se propaga automáticamente cuando se ejecuta en un controlador de dominio (DC), mientras borra los registros de eventos de las máquinas afectadas.

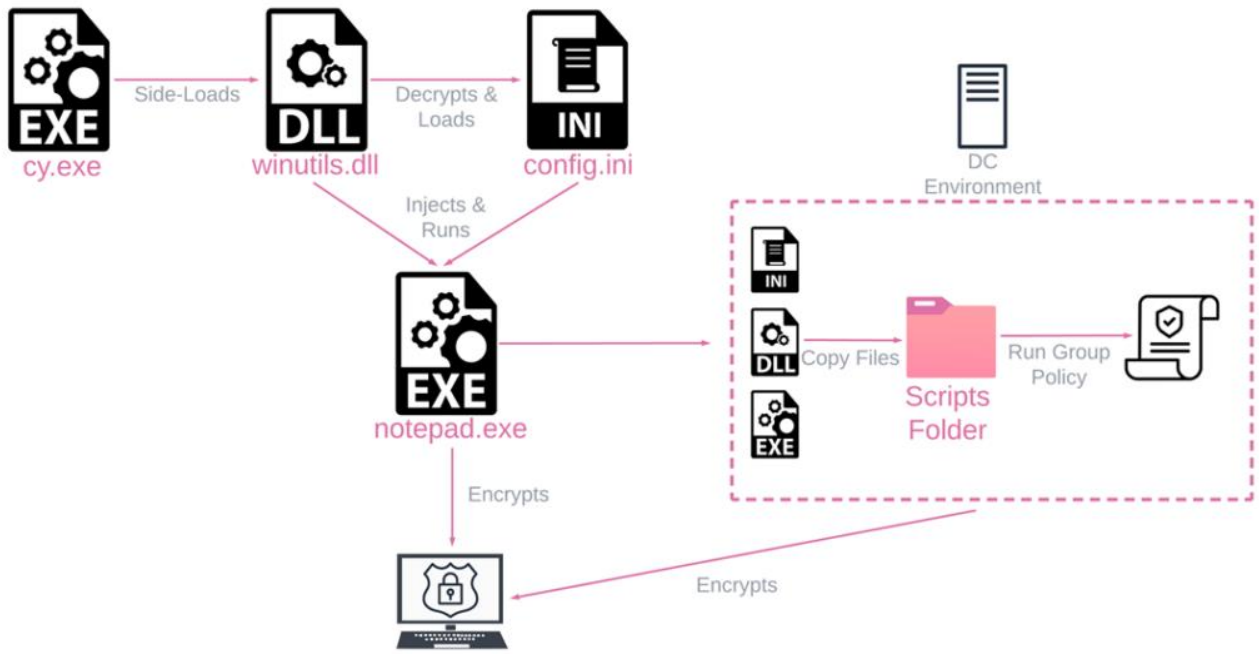
Además, es extremadamente flexible, operando no solo en base a una configuración incorporada, sino también a numerosos argumentos opcionales que le permiten cambiar su comportamiento de acuerdo con las necesidades del operador. Si bien parece haberse inspirado en algunas de las familias de ransomware más infames, también contiene funcionalidades únicas, que rara vez se ven entre los ransomware, como el uso de llamadas al sistema directas.

FLUJO DE EJECUCIÓN.

La ejecución de Rorschach utiliza estos tres archivos:

- **cy.exe** – Cortex XDR Dump Service Tool versión 7.3.0.16740, abusado para carga **lateralwinutils.dll**
- **winutils.dll** : cargador e inyector de Rorschach empaquetado, que se utiliza para descifrar e inyectar el ransomware.
- **config.ini** : ransomware Rorschach cifrado que contiene toda la lógica y la configuración.

Tras la ejecución de **cy.exe**, debido a la carga lateral de DLL, el cargador/inyector **winutils.dll** se carga en la memoria y se ejecuta en el contexto de **cy.exe**. La carga útil principal de Rorschach **config.ini** también se carga posteriormente en la memoria, se descifra y se inyecta en notepad.exe, donde comienza la lógica del ransomware.



PROPAGACIÓN.

Cuando se ejecuta en un controlador de dominio (DC) de Windows, el ransomware crea automáticamente una política de grupo y se propaga a otras máquinas dentro del dominio. En el pasado, se vinculó una funcionalidad similar a LockBit 2.0 , aunque la implementación del GPO de Rorschach Ransomware se lleva a cabo de manera diferente, como se describe a continuación:

1. Rorschach copia sus archivos en la carpeta de scripts del DC y los elimina de la ubicación original.
2. Luego, Rorschach crea una política de grupo (consulte el Apéndice C) que se copia a sí misma en la **%Public%** carpeta de todas las estaciones de trabajo del dominio.
3. El ransomware crea otra política de grupo en un intento de eliminar una lista de procesos predefinidos. Esto se hace creando una tarea programada invocando **taskkill.exe**.

4. Finalmente, Rorschach crea otra política de grupo que registra una tarea programada que se ejecuta inmediatamente y al iniciar sesión el usuario, para ejecutar el ejecutable principal de Rorschach con los argumentos relevantes.

ANÁLISIS DE RANSOMWARE.

Además del comportamiento poco común del ransomware descrito anteriormente, el binario de Rorschach en sí mismo contiene características interesantes adicionales, que lo diferencian aún más de otros ransomware.

Protección binaria y antianálisis.

La muestra real está cuidadosamente protegida y requiere bastante trabajo para acceder. Primero, el cargador/inyector inicial winutils.dllestá protegido con empaque estilo UPX. Sin embargo, esto se modifica de tal manera que no se desempaqueta fácilmente con soluciones estándar y requiere un desempaquetado manual. Después de desempaquetar, la muestra se carga y descifra config.ini, que contiene la lógica del ransomware.

Después de inyectar Rorschach en notepad.exe, aún está protegido por VMProtect. Esto da como resultado que una parte crucial del código se virtualice además de carecer de una tabla IAT. Solo después de derrotar estas dos medidas de seguridad es posible analizar adecuadamente la lógica del ransomware.

Evasión de soluciones de seguridad.

Aunque Rorschach se usa únicamente para encriptar un entorno, incorpora una técnica inusual para evadir los mecanismos de defensa. Hace llamadas directas al sistema usando la instrucción “syscall”. Si bien se observó anteriormente en otras variedades de malware, es bastante sorprendente ver esto en el ransomware.

El procedimiento implica utilizar la instrucción en sí, y es el siguiente:

1. El ransomware encuentra los números de llamada al sistema relevantes para las API de NT, principalmente relacionados con la manipulación de archivos.
2. Rorschach luego almacena los números en una tabla para uso futuro.
3. Cuando es necesario, llama a una rutina auxiliar que usa el número directamente con la instrucción syscall en lugar de usar la API de NT.

CONSLUSIÓN.

El análisis de Rorschach revela la aparición de una nueva variedad de ransomware en el panorama del crimeware. Sus desarrolladores implementaron nuevas técnicas de evasión de defensa y antianálisis para evitar la detección y dificultar que el software de seguridad y los investigadores analicen y mitiguen sus efectos. Además, Rorschach parece haber tomado algunas de las “mejores” funciones de algunos de los principales ransomwares filtrados en línea y las integró todas juntas. Además de las capacidades de autopropagación de Rorschach, esto eleva el nivel de los ataques de rescate. Los operadores y desarrolladores del ransomware Rorschach siguen siendo desconocidos. No usan marcas, lo cual es relativamente raro en las operaciones de ransomware.

Los hallazgos subrayan la importancia de mantener fuertes medidas de ciberseguridad para prevenir ataques de ransomware, así como la necesidad de monitoreo y análisis continuos de nuevas muestras de ransomware para adelantarse a las amenazas en evolución. A medida que estos ataques continúan creciendo en frecuencia y sofisticación, es esencial que las organizaciones se mantengan vigilantes y proactivas

RECOMENDACIONES.

- Generar una regla personalizada para bloqueos de IOC’s en perfiles entrantes perimetrales.
- Desconfía de los correos alarmantes. Si un mensaje le indica o incentiva a tomar decisiones apresuradas o en un tiempo limitado, probablemente se trata de phishing.
- Disponer de sistemas antispam para correos electrónicos, de esta manera se reducen las posibilidades de infección a través de campañas masivas de malspam por correo electrónico.
- Proteger el protocolo RDP:
  – Deshabilita los servicios RDP, si no es necesario.
  – La desactivación de servicios no utilizados e innecesarios ayuda a reducir su exposición a las vulnerabilidades de seguridad, y es una buena práctica de seguridad.
  – Si no es posible cerrarlos, límita las direcciones de origen que pueden acceder a los puertos.
  – Proteger el acceso a los sistemas RDP, bloqueando el sistema local en lugar del sistema remoto.
  – Incluso si el primero no tiene valor, la sesión RDP solo estará protegida limitando el acceso al sistema cliente.
  – Desconectar sesiones RDP en lugar de bloquearlas, esto invalida la sesión actual, lo que impide una reconexión automática de la sesión RDP sin credenciales.
  – Bloquear bidireccionalmente el puerto TCP 3389 utilizando un firewall o hacerlo accesible sólo a través de una VPN privada.
- Habilitar la autenticación de nivel de red (NLA).
- Tener políticas de respaldo periódico que se almacenen fuera de la red organizacional.
  Escanear todos los archivos adjuntos, antes de abrirlos, con un antivirus que detecte comportamientos para combatir los ransomwares.
- Mantener una buena estrategia de respaldo de información: sistemas de copias de seguridad que deben estar aisladas de la red; y políticas de seguridad. Lo anterior permitirá neutralizar el ataque, restaurar las operaciones y evitar el pago del rescate.
- Actualizar los equipos con Windows a las últimas versiones.
- Nunca seguir la instrucción de deshabilitar las funciones de seguridad, si un correo electrónico o documento lo solicita.

- Establecer políticas de seguridad en el sistema para impedir la ejecución de ficheros desde directorios comúnmente utilizados por Ransomware (App Data, Local App Data, etc.)
- Mantener listas de control de acceso para las unidades mapeadas en red restringiendo los privilegios de escritura.
  Con esto podrás identificar el impacto generado por el cifrado de archivos, entendiendo que el secuestro de información se producirá en todas las unidades de red mapeadas en el equipo víctima.
- Seguir las normativas internacionales tales como ISO 27001:2013 en su control A.7.2.2 "Concienciación con educación y capacitación en seguridad de la información" o NIST PR.AT-1: "Todos los usuarios se encuentran entrenados e informados", a fin de tener bases para divulgar campañas educativas orientadas a nivel de usuarios respecto al correcto uso de las herramientas tecnológicas, haciendo énfasis en cómo proceder al recibir correos de orígenes desconocidos, objeto prevenir que los usuarios sean víctimas de entes maliciosos.

INDICADORES DE COMPROMISO

INDICADORES DE COMPROMISO.

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:
Guatemala: +(502) 2307 5757
El Salvador: +(503) 2249 4252
Honduras: +(504) 2283 5904
República Dominicana: +1 829 734 2040
WhatsApp: +(502) 5124 9536
Sitio Web: https://www.devel.group/reporta-un-incidente