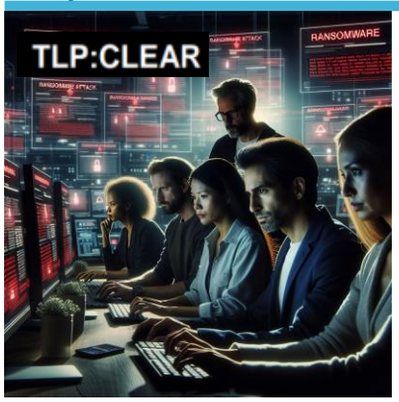
Alerta de Seguridad

Campaña de ransomware - Makop y Crysis en Colombia

COLCERT AL-2810-054



Se ha identificado una nueva campaña de ransomware que afecta a organizaciones en Colombia. Esta campaña involucra **variantes de ransomware conocidas como Makop y Crysis,** así como una herramienta adicional para la recolección de credenciales clasificada como Trojan.Win64.Occamy. Los atacantes emplean técnicas avanzadas de evasión y persistencia, lo que hace que estas amenazas sean particularmente difíciles de detectar y mitigar. Este boletín de advertencia tiene como objetivo alertar a las entidades sobre los riesgos asociados y proporcionar recomendaciones para la protección de sus sistemas y datos.

Descripción de la Amenaza:

Ransomware Makop (mkp_visual.exe)

- **Clasificación:** Ransomware de la familia Makop.
- **Indicadores de Compromiso (IoCs):**
  MD5: 048b493c1e9795a8d28a511d88b86f9e
  SHA256:
  4aace7fd7ba4c0eb24454f9bbf161499363ff34fc5c2eb8
  1b982a25cfc0fdd27

Comportamiento

Modifica claves de registro para asegurar su persistencia.

- Emplea técnicas de evasión de entornos virtuales y sandboxes.
- Realiza comunicaciones con dominios como: slscr.update.microsoft.com para posibles validaciones de certificados.

Impacto: Cifrado de archivos críticos con fines de extorsión, exigiendo el pago de un rescate para restaurar el acceso a los datos.

Ransomware Crysis (5-2NS.exe)

- **Clasificación:** Ransomware de la familia Crysis.
- **Indicadores de Compromiso (IoCs):**
  MD5: 6bffc6c7caa2eb2fa90fac0317f63338
  SHA256:
  92c65b58c4925534c2ce78e54b0e11ecaf45ed8cf034
  4ebff46cdfc4f2fe0d84

Comportamiento

Modifica claves de registro para asegurar su persistencia.

- Detecta entornos de análisis, como sandboxes y depuradores, para evitar la detección.
- Realiza manipulación de registros y utiliza Rundll32 para ejecutar código malicioso.
- Actúa de manera autónoma sin necesidad de comunicación constante con servidores externos.

Impacto: Encripta archivos en sistemas comprometidos, impidiendo el acceso a la información y solicitando un rescate.

Trojan.Win64.Occamy (LostMyPassword.exe)

- **Clasificación:** Herramienta maliciosa de recolección de credenciales.
- **Indicadores de Compromiso (IoCs):**
  MD5: 5f3583d76b81f91d2f63813414cd5b47
  SHA256:
  7da421d00cd50570a79a82803c170d043fa3b22
  53ae2f0697e103072c34d39f1

Comportamiento

- Realiza inyección de código y manipulación de tokens de acceso para obtener credenciales.
- Evade entornos de análisis y captura datos sensibles, como contraseñas y otros credenciales.

Impacto: Facilita el acceso no autorizado a sistemas, posibilitando movimientos laterales dentro de la red antes del despliegue del ransomware.

COLCERT

Alerta de Seguridad

Campaña de ransomware - Makop y Crysis en Colombia

COLCERT AL-2810-054

Makop

Año de aparición: Activo desde 2020.

Método de infección principal:

- Uso de RDP (Protocolo de Escritorio Remoto) con configuraciones débiles para acceder a la red de la víctima.

Cifrado: AES para cifrar archivos, dificultando su recuperación.

Comportamiento:

- Añade extensiones a los archivos cifrados, dejando notas de rescate que indican cómo contactar a los atacantes y realizar pagos, frecuentemente en Bitcoin.

Objetivo: Impactar la operatividad de las empresas, especialmente las redes corporativas.

Crysis/Dharma

Año de aparición: Identificado desde 2016.

Método de infección principal:

- Utiliza RDP débil y campañas de phishing para propagar el ransomware.

Cifrado: AES junto con RSA, asegurando que el descifrado sea difícil.

Comportamiento:

- Personaliza las notas de rescate con correos electrónicos, indicando cómo contactar a los atacantes. Además, agrega múltiples extensiones a los archivos cifrados..

Variante: Ha evolucionado con diferentes versiones, lo que dificulta su detección.

Similitudes y diferencias

Similitud principal: Ambos explotan RDP mal configurado y emplean cifrado robusto (AES + RSA). Representan una amenaza significativa para organizaciones y destacan la necesidad de mejorar la seguridad en accesos remotos.

Diferencia clave: Makop se centra más en redes corporativas, mientras que Crysis/Dharma tiene una mayor versatilidad de métodos de propagación, incluyendo phishing y variantes más frecuentes.

Recomendaciones de Seguridad:

Para mitigar el riesgo de ser víctima de esta campaña de ransomware, se recomienda a las organizaciones implementar las siguientes medidas de seguridad:

Control de Ejecución:

- Restringir el acceso a las conexiones RDP - puerto 3389, y habilitar acceso a través de VPN.
- Limitar la ejecución de archivos desconocidos mediante la aplicación de políticas estrictas de seguridad en el sistema operativo.
- Utilizar listas blancas para permitir la ejecución solo de software autorizado.

Detección y Respuesta Proactiva:

- Implementar soluciones de seguridad que detecten comportamientos anómalos, como el cifrado masivo de archivos, manipulación del registro y cambios inusuales en el sistema.
- Realizar auditorías regulares de los registros de eventos para identificar cualquier actividad sospechosa.

Monitoreo de Red:

- Monitorear la actividad de red y analizar el tráfico para detectar conexiones inusuales con dominios o direcciones IP no autorizadas, especialmente aquellas relacionadas con el ransomware.
- Implementar sistemas de detección de intrusos (IDS) y sistemas de prevención de intrusos (IPS) para identificar y bloquear actividades sospechosas.

Respaldo de Información Crítica:

- Realizar copias de seguridad periódicas de datos críticos y almacenarlas en ubicaciones seguras y desconectadas de la red principal.
- Verificar que los respaldos sean funcionales y que se puedan restaurar rápidamente en caso de un incidente.

COLCERT

Alerta de Seguridad

Campaña de ransomware - Makop y Crysis en Colombia

COLCERT AL-2810-054

Concientización de Usuarios:

- Capacitar a los empleados sobre el reconocimiento de correos electrónicos de phishing y la importancia de no abrir archivos adjuntos o enlaces de remitentes desconocidos.
- Promover el uso de contraseñas seguras y la autenticación multifactor (MFA) para todas las cuentas de usuario.

Recomendaciones para el Equipo de TI

Para enfrentar una campaña de ransomware como la detectada (familias Makop y Crysis), es esencial que el equipo de TI implemente medidas de prevención, detección y respuesta. A continuación, se proporcionan recomendaciones detalladas para fortalecer la postura de seguridad y minimizar el riesgo de infección y propagación del ransomware:

Fortalecimiento de la Seguridad Perimetral:

- Implementar filtros avanzados de correo electrónico para bloquear phishing y escanear archivos adjuntos antes de su entrega.
- Mantener actualizados el sistema operativo, software y parches de seguridad para mitigar vulnerabilidades

Protección Interna:

- Realizar respaldos regulares de datos críticos y almacenarlos de forma segura fuera de la red principal.
- Segmentar la red para limitar la propagación del malware y restringir el acceso entre diferentes partes de la red.

Detección y Respuesta Temprana:

- Utilizar herramientas de EDR y SIEM para monitorear actividades sospechosas y correlacionar eventos en tiempo real.
- Implementar sistemas IDS/IPS para detectar señales de comunicaciones de comando y control (C2) del ransomware.

Control de Acceso y Seguridad:

- Activar la autenticación multifactor (MFA) para todas las cuentas críticas, reduciendo el riesgo de accesos no autorizados.
- Aplicar el principio de menor privilegio, revisando y ajustando los permisos de acceso para limitar el uso de cuentas con privilegios elevados.

Concientización del Personal:

- Capacitar a los empleados sobre los riesgos del ransomware y las buenas prácticas de ciberseguridad.
- Realizar simulaciones de phishing para evaluar y mejorar la preparación de los usuarios.

Planes de Respuesta y Recuperación:

- Desarrollar un plan de respuesta a incidentes que incluya la contención de la infección y la notificación a las partes implicadas.
- Preparar al equipo para la restauración de sistemas y datos a partir de respaldos, manteniendo canales de comunicación de emergencia.

Makop y Crysis/Dharma son dos tipos de ransomware que atacan principalmente a través de RDP mal configurados y vulnerabilidades en sistemas expuestos a Internet. Ambos cifran archivos con algoritmos robustos (AES y RSA) y exigen rescates, usualmente en Bitcoin

COLCERT

Alerta de Seguridad

Campaña de ransomware - Makop y Crysis en Colombia

Conclusión

Esta campaña de ransomware representa una amenaza significativa para las organizaciones debido a la capacidad de los atacantes para cifrar datos críticos y extraer credenciales antes del despliegue del ransomware. La implementación de las recomendaciones aquí descritas es fundamental para proteger los sistemas y datos de posibles ataques. El COLCERT continuará monitoreando la situación y proporcionará actualizaciones a medida que se disponga de nueva información sobre la campaña.

La protección contra el ransomware requiere una combinación de prevención, detección avanzada y una respuesta eficaz ante incidentes. La implementación de estas recomendaciones permitirá al equipo de TI minimizar el impacto de posibles ataques y garantizar la continuidad de las operaciones de la organización. La preparación continua y la formación son claves para mantener una defensa sólida frente a amenazas de ransomware

NIVEL DE RIESGO

ALTO

FUENTES:

- Plataforma Detectic - COLCERT (Sandbox) - https://detectic.colcert.gov.co/external-user/upload-sample
- BleepingComputer - https://www.bleepingcomputer.com
- Kaspersky Threat Intelligence Portal - https://opentip.kaspersky.com
- Recorded Future - https://www.recordedfuture.com
- Reddit - r/Malware - https://www.reddit.com/r/Malware/
- Malware Traffic Analysis - https://www.malware-traffic-analysis.net