Nro. Alerta:	AL-2024-026	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	30-oct-2024	**IOCs Ransomware Makop y Crysis**	Pág.: **1** of **7**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de incidente: Ransomware
Nivel de riesgo: Alto

II. ALERTA

Se ha identificado una nueva campaña de ransomware que afecta a organizaciones en países de Latinoamérica especialmente 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.

***Figura 1**: Mensaje de Ransomware*

III. INTRODUCCIÓN

Los ransomware Makop y Crysis/Dharma utilizan diversas técnicas de ingeniería social para engañar a las víctimas y facilitar su infección. Estas técnicas se centran en manipular la confianza y aprovechar la vulnerabilidad de las personas.

Utiliza el phishing y spear Phishing en sus ataques que contienen archivos adjuntos maliciosos o enlaces a sitios comprometidos. También se distribuye mediante el acceso no autorizado a servidores a través del Protocolo de Escritorio Remoto (RDP) con credenciales débiles.

Estos grupos de ransomware se consideran peligrosos debido a sus características que aumentan su efectividad y el impacto en las víctimas; tales como:

- Modelo Ransomware-as-a-Service (RaaS): Operan bajo un modelo RaaS, lo que permite a los ciberdelincuentes alquilar el ransomware y personalizarlo para sus propios ataques.

- Cifrado Efectivo: El ransomware Makop utiliza el cifrado AES utilizando la extensión «.makop»; cifrado robusto que dificulta la recuperación de datos sin la clave de descifrado, puede cifrar hasta el 100% de los archivos en un sistema infectado, lo que maximiza el daño. Por otro lado, Crysis cifra una amplia gama de archivos en sistemas Windows, utilizando combinaciones de algoritmos de cifrado RSA y AES. Los archivos cifrados reciben la extensión .crysis o variantes similares, lo que dificulta su acceso.

- Tácticas de Doble Extorsión: Makop no solo cifra los archivos, sino que también puede robar datos sensibles antes de cifrarlos. Si la víctima no paga el rescate, los atacantes amenazan con publicar estos datos robados.

- Uso de Herramientas Personalizadas: Emplea herramientas personalizadas y estándar para llevar a cabo sus ataques, lo que le permite adaptarse y evadir detecciones por parte de software de seguridad.

- Métodos de Distribución Variados: Se distribuye a través de técnicas como phishing, campañas de spam y acceso no autorizado a través de RDP (Remote Desktop Protocol). Esto le permite infiltrarse en redes corporativas sin ser detectado inicialmente.

- Persistencia: Crysis crea entradas en el registro de Windows para asegurarse de que se ejecute cada vez que el sistema se inicie, lo que complica su eliminación.

- Personalización del Rescate: Las demandas de rescate pueden variar según la información recopilada sobre la víctima, lo que significa que empresas más grandes pueden ser objeto de demandas más altas.

- Nota de Rescate Específica: Al finalizar el proceso de cifrado, Makop deja una nota de rescate con instrucciones claras sobre cómo contactar a los atacantes y pagar el rescate, lo que facilita la comunicación entre las víctimas y los delincuentes; en cambio Crysis deja un archivo de nota de rescate en el escritorio, personaliza las notas de rescate con correos electrónicos, indicando cómo contactar a los atacantes. Además, agrega múltiples extensiones a los archivos cifrados y también puede cambiar el fondo del escritorio para incluir información sobre cómo pagar el rescate.

IV. FUNCIONAMIENTO

RANSOMWARE	COMPORTAMIENTO	IMPACTO
Ransomware Makop	– 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.	Cifrado de archivos críticos con fines de extorsión, exigiendo el pago de un rescate para restaurar el acceso a los datos
Ransomware Crysis **Existe desde 2016**	– 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	Encripta archivos en sistemas comprometidos, impidiendo el acceso a la información y solicitando un rescate

RANSOMWARE	COMPORTAMIENTO	IMPACTO
	constante con servidores externos	
Trojan.Win64.Occamy	– 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	Facilita el acceso no autorizado a sistemas, posibilitando movimientos laterales dentro de la red antes del despliegue del ransomware.

V. INDICADORES DE COMPROMISO:

A continuación los hashes de archivos maliciosos detectados:

RAMSONWARE	INDICADORES DE COMPROMISO
Ransomware Makop (mkp_visual.exe)	MD5: 48b493c1e9795a8d28a511d88b86f9e SHA256: 4aace7fd7ba4c0eb24454f9bbf161499363ff34fc5c2eb81b982a25cfc0fdd27
Ransomware Crysis (5-2NS.exe)	MD5: 6bffc6c7caa2eb2fa90fac0317f63338 SHA256: 92c65b58c4925534c2ce78e54b0e11ecaf45ed8cf0344ebff46cdfc4f2fe0d84
Trojan.Win64.Occamy (LostMyPassword.exe)	MD5: 5f3583d76b81f91d2f63813414cd5b47 SHA256: 7da421d00cd50570a79a82803c170d043fa3b2253ae2f0697e103072c34d39f1

VI. RECOMENDACIONES:

Ante un ataque de ransomware, es fundamental actuar con rapidez y seguir un conjunto de pasos específicos para minimizar el daño y aumentar las posibilidades de recuperación. Algunos pasos a seguir son:

1. **Aislar el Sistema o Red:** Si se detecta actividad de ransomware en una computadora o en la red, aislar inmediatamente el sistema afectado desconectándolo de la red informática. Esto ayudará a evitar que el ransomware se propague a otros sistemas. **Recuerde** no apagar el equipo para no perder información que se almacena temporalmente en la memoria volátil, necesaria para la investigación; la cual se borra cuando se reinicia o apaga el equipo.
2. **Confirmar el Ataque:** Asegurarse de que se trata de un ataque de ransomware. Los ataques de ransomware suelen mostrar una nota de rescate en la pantalla de la víctima. Tomar capturas de pantalla o fotografías de la pantalla para documentar la nota de rescate.
3. **No Pagar el Rescate:** No pagar el rescate exigido por los atacantes. No hay garantía de que se obtendrá la clave de descifrado después de realizar el pago, y pagar solo alienta a los ciberdelincuentes.
4. **Informar del Ataque:** Notificar de inmediato al equipo de seguridad de la organización o a las autoridades. Cuanto antes se informe, mejor será la respuesta y la posibilidad de rastrear a los atacantes.
5. **Restauración desde una Copia de Seguridad:** Si se cuenta con copias de seguridad actualizadas y seguras, utilizar estas copias para restaurar los datos y sistemas afectados. Asegurarse de que las copias de seguridad sean de confianza y no estén comprometidas.
6. **No Borrar Evidencia:** No apagar los equipos afectados, no borrar ningún archivo o evidencia del ataque, hasta que se haya evaluado completamente la situación y se haya informado a las autoridades. La evidencia es necesaria para iniciar la investigación.
7. **Contactar con la autoridad:** De ser víctima, contacte a las Autoridades competentes para denunciar el ciberdelito con base a la Normativa Legal Vigente.

8. **Recopilar Información:** Documentar todos los detalles del ataque, incluyendo la nota de rescate, la dirección de Bitcoin utilizada para el rescate (si está disponible), y cualquier información sobre cómo se propagó el ransomware.

9. **Buscar información sobre el ransomware:** En el caso de que la organización se vea afectada por un ransomware, se puede visitar páginas especializadas en tratamiento de ese ransomware y en el mejor de los casos encontrar el descifrador (ej. www.nomoreransom.org).
10. **Escanear y Limpiar el Sistema:** Escanear el sistema afectado en busca de malware residual y limpia cualquier instancia del ransomware. Utilizar herramientas de seguridad confiables y actualizadas.

11. **Control de Ejecución:** Restringir el acceso a las conexiones RDP especialmente el 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.

Post ataque es importante tomar medidas preventivas para minimizar nuevos ataques, a continuación algunas acciones:

1. **Mejorar la Seguridad:** Identificar las vulnerabilidades o puntos débiles que permitieron que el ransomware infectara el sistema y tomar medidas para mejorar la seguridad, como parchear software, fortalecer contraseñas, educar a los usuarios sobre la seguridad cibernética, implementar sistemas de detección de intrusos (IDS) y sistemas de prevención de intrusos (IPS) para identificar y bloquear actividades sospechosas.
2. **Mejorar el Plan de Respuesta a Incidentes:** Desarrollar y revisar un plan de respuesta a incidentes que incluya los pasos específicos a seguir en caso de futuros ataques de ransomware.
3. **Monitoreo Continuo:** Implementar un monitoreo de seguridad continuo para detectar actividades inusuales en la red y sistemas que podrían indicar un ataque en curso o intentos de infiltración futuros.
4. **Concienciación de Usuarios:** Educar a los usuarios sobre cómo identificar el ransomware y los peligros del phishing, ya que la mayoría de los ataques de ransomware comienzan con correos electrónicos maliciosos.
5. **Establecer perfiles de usuarios** en equipos y sistemas en los cuales se otorgue derechos de administrador y acceso solo cuando sea necesario.

6. **Añadir varias capas extras de seguridad** con por ejemplo la autenticación multifactor (MFA) especialmente en los servicios críticos.
7. **Realizar periódicamente una evaluación de riesgos y análisis de brechas** para identificar y mitigar oportunamente posibles vulnerabilidades.

VII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VIII. REFERENCIAS:

- https://www.colcert.gov.co/800/w3-propertyvalue-412601.html, COLCERT AL-2810-054
- https://www.fortinet.com/blog/threat-research/ransomware-roundup-playing-whack-a-mole-with-new-crysis-dharma-variants
- https://www.malwarebytes.com/blog/detections/ransom-crysis