Ransomware Dharma/Crysis

Bogotá, 8 de mayo de 2018

Apreciado,

Nuestro equipo de especialistas ha detectado casos de ataque de Ransomware, infectando estaciones y servidores mediante vectores de ataque asociados a servicios RDP (protocolo de escritorio remoto) incorrectamente gestionados. El ransomware desplegado en este tipo de ataques ha sido identificado como Dharma\Crysis.

Las muestras identificadas son detectadas por Kaspersky Endpoint Security desde 21.02.2017 como HEUR:Trojan.Win32.Generic y específicamente desde 19.04.2017 como TrojanRansom.Win32.Crusis.to. Además, confirman que varios de nuestros registros basados en heurística son capaces de detectarlo desde antes de 21.02.2017.

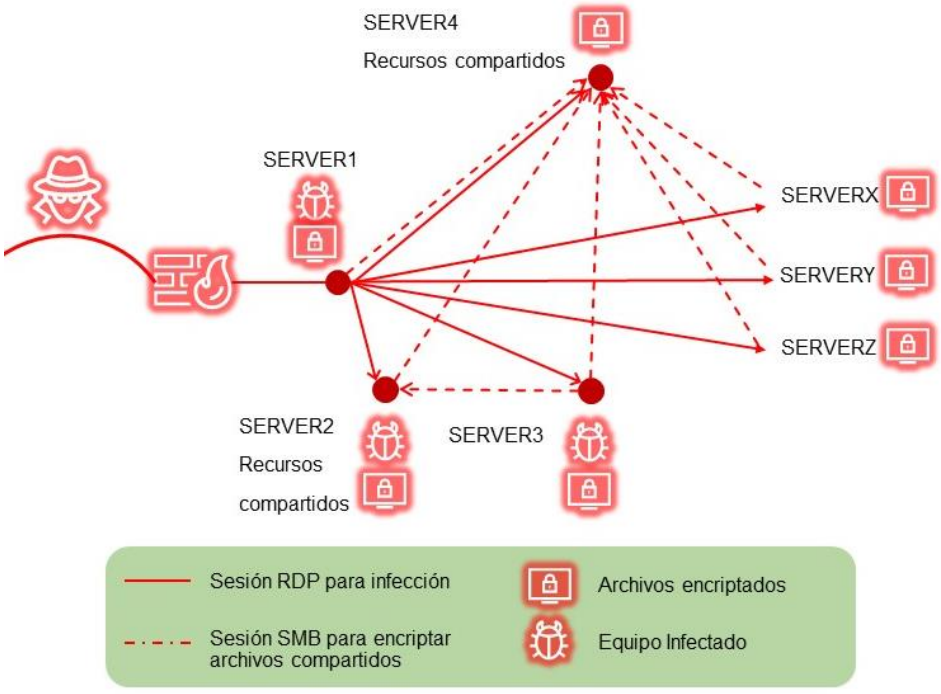
¿Cómo se difunde el Ransomware?

Uno de los principales vectores implementados por los atacantes ha sido mediante acceso RDP expuesto en Internet, pero también se han identificado ataques utilizando spam de correo electrónico, archivos adjuntos maliciosos, exploits, actualizaciones falsas y componentes de programas legítimos suplantando productos de Microsoft, Adobe, entre otros.

Para los casos de RDP, el atacante se conecta a los servidores o estaciones de trabajo mediante sesiones de escritorio remoto expuestas en Internet e incluso mediante sesiones de VPN donde se han comprometido los activos de otras compañías. Si el servicio de escritorio remoto permite las sesiones de usuarios privilegiados (Administradores del sistema o del dominio) y el atacante se apodera de credenciales privilegiadas en el servidor o el dominio, tiene la capacidad de desinstalar/desactivar las soluciones de seguridad y generar cualquier tipo de compromiso en el sistema y otros sistemas a su alcance.

¿Qué hace el ransomware?

El ransomware cifra todos los archivos del sistema y se difunde hacia recursos compartidos, encriptando la totalidad de la información. El atacante continúa desplegando el ransomware en la red haciendo uso del servicio RDP, identificando otros servidores a su alcance y conectándose a estos con las mismas credenciales obtenidas, para acceder e instalar el ransomware, ampliando el despliegue del malware y el impacto a las organizaciones.



Indicadores de compromiso:

El malware se copia en las siguientes rutas del sistema:

- C:\Users\<nombre usuario>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\
- C:\Windows\System32\
- C:/ProgramData/Microsoft/Windows/Start Menu/Programs/StartUp/

Mecanismos de persistencia:

- Registro de windows, llave autorun: "\\REGISTRY\\ MACHINE\\ SOFTWARE\\ Microsoft\\ Windows\\ CurrentVersion\\ Run\\ $selfname.exe"
- StartUp: *"$user\\$appdata\\Microsoft\\Windows\\Start Menu\\ Programs\\ Startup\\ $selfname.exe"*

Recomendaciones:

- Deshabilitar el servicio RDP en la red de la organización. En caso de ser requerido, habilitarlo únicamente mediante acceso vía VPN a usuarios autorizados y haciendo uso de la política del menor privilegio, imposibilitando el acceso a usuarios privilegiados mediante sesiones remotas.
- Si es indispensable el uso de estas herramientas se debe programar una tarea para cerrar los puertos de conexión (TCP 3389), en horarios de inactividad.
- Usar contraseñas robustas para el acceso a los sistemas: 12 caracteres, mayúsculas, minúsculas y caracteres especiales, así como habilitar políticas que no permitan más de tres intentos de acceso.
- Habilitar la contraseña del producto Kaspersky Endpoint Security 10x o de los productos de seguridad de Kaspersky evitando que puedan ser desactivados por usuarios privilegiados en el sistema, implementando contraseñas robustas y diferentes de las usadas por los administradores o usuarios de red. Seguir las recomendaciones registradas en el portal https://help.kaspersky.com/KESWin/10SP2/es-ES/123303.htm
- Ejecute una robusta suite anti-malware con protección antivirus incorporada como System Watcher de Kaspersky Enterprise Security for Business
- Asegúrese de actualizar Microsoft Windows y todos los programas de terceros.
- Garantizar que los productos de seguridad se encuentren debidamente actualizados y activos en todos los sistemas de la red.
- No ejecute archivos adjuntos abiertos desde fuentes no confiables.
- Copia de seguridad de los datos confidenciales en el almacenamiento externo y manténgalos fuera de línea.
- Implementar una DMZ para los servicios disponibles en Internet y separar la red interna de los recursos disponibles a través de Internet. Esto asegura que, si un servicio público es comprometido, solo ese servidor o máxime los equipos en la DMZ se verán afectados y no se afectará la totalidad de la red.

Acerca de Kaspersky Lab

Kaspersky Lab es una compañía mundial de seguridad cibernética que celebra más de 20 años de trayectoria en el mercado. La amplia experiencia de Kaspersky Lab en inteligencia de amenazas y seguridad se transforma constantemente en soluciones de seguridad y servicios de vanguardia para proteger a empresas, infraestructura crítica, gobiernos y consumidores de todo el mundo. La amplia cartera de seguridad de la compañía incluye una destacada protección de terminales y numerosas soluciones de seguridad y servicios especializados para combatir las amenazas digitales más avanzadas y en evolución. Más de 400 millones de usuarios están protegidos por las tecnologías de Kaspersky Lab y ayudamos a 270,000 clientes corporativos a proteger lo que más valoran.

Obtenga más información en http://latam.kaspersky.com