BOLETIN DE CIBERSEGURIDAD

El Domingo 06-09-2020 fue confirmado en el Banco Estado de Chile la materialización de un Ransomware (Malware que secuestra la información) en su infraestructura, la cual ha afectado servicios de cara a clientes, dado ese escenario Banco Estado levantó y está ejecutando el proceso de contención y recuperación de infraestructura.

Ese mismo día el Banco coordinó una reunión de contingencia para entender el alcance del incidente en Banco Estado en chile y las medidas que se deben tomar todas las entidades.

Resumen de alcance del Incidente Banco Estado en chile.

1.- El incidente aún no está contenido y aún no se identifica el vector de ataque.

2.- Se confirma que tienen mas de14.000 estaciones de trabajo y cerca de 4.000 servidores infectados (Toda la plataforma Windows)

3.- Hay impacto operacional el cual se está evaluando alcance.

3.- El Malware utilizó una cuenta de dominio para propagarse y utiliza una vulnerabilidad reportada en 2018 de fácil explotación, CVE-2018-8453, para ingresar a la infraestructura del banco.

5.- Además mediante una tarea programada baja el servicio de antivirus, lo que le permite propagarse con más facilidad.

VECTOR DE ATAQUE

El vector de infección inicial utilizado por el actor de la amenaza es un correo electrónico de phishing que contiene un enlace malicioso. Cuando se presiona, el enlace descarga un archivo zip supuestamente legítimo que en realidad es malicioso.

El Banco se vio comprometido por el Ransomware Sodinokibi, el cual es un programa distribuido con un modelo de negocio Ransomware-as-a-Service, detectado por primera vez en una campaña en 2019. “Sodinokibi” explota una vulnerabilidad de Oracle WebLogic para obtener acceso a la máquina del objetivo. Una vez que está dentro, el malware intenta implementarse con derechos legales de usuario elevados para acceder a todos los archivos, así como a los recursos del sistema sin restricciones.

Este ransomware utiliza AES y también el algoritmo Salsa20 para encriptar los datos individuales, AES se utiliza para encriptar los secretos de la sesión y también los datos que se envían al servidor de control, Sodinokibi utiliza un algoritmo de intercambio crucial Diffie-Hellman de curva elíptica para crear y también proliferar claves de cifrado.

Al comienzo del proceso de ejecución, Sodinokibi intenta obtener privilegios explotando algunas vulnerabilidades, después de esta etapa el malware recopila datos básicos del sistema y del usuario, para luego generar el cifrado de datos.

Algunos métodos de propagación son a través de campañas de phishing que contengan archivos adjuntos maliciosos, tratando de engañar a los usuarios para que abran los archivos adjuntos. Estos archivos suelen ser documentos Microsoft Office, archivos como ZIP, RAR, JavaScript, ficheros PDF, ejecutables (.exe), entre otros. Una vez abiertos, descargan otros tipos de malware tipo troyano para propagarse por la red atacada y generar infecciones en cadena.

Microsoft ha observado ataques de fuerza bruta en servidores de escritorio remoto (RDP) y dispositivos de red vulnerables. Luego de la intrusión inicial es seguida por el uso de herramientas básicas para el robo de credenciales y generar los movimientos laterales antes de inyectar la carga útil del ransomware.

RECOMENDACIONES

- Aumentar el monitoreo de tráfico no usual
- Mantener los equipos actualizados, tanto sistemas operativos como otro software instalados.
- No abrir documentos de fuentes desconocidas.
- Tener precaución en abrir documentos y seleccionar enlaces de correos electrónicos.

- Verificar y controlar los servicios de escritorio remoto (RDP).
- Bloqueo de script o servicios remotos no permitidos en la instrucción.
- Monitorear servicios SMB de forma horizontal en la red.
- Mantener actualizados las protecciones perimetrales de las instituciones
- Aumentar los niveles de protección en los equipos que cumplan las funciones de Anti-spam, WebFilter y Antivirus.
- Verificar el funcionamiento, y si no es necesario, bloquear las herramientas como PsExec y Powershell.
- Mantener especial atención sobre el tráfico sospechoso que tengan conexiones a los puertos 135TCP/UDP y 445TCP/UDP
- Segmentar las redes en base a las necesidades de sus activos, permitiendo solamente los puertos necesarios.
- Configurar contraseñas robustas en las cuentas de administrador de dominio, de más de 10 caracteres alfanumericos que incluya caracteres especiales.
- Configurar contraseñas en los servicios de antivirus para evitar configuración o desactivación por parte del malware.
- Validar que la vulnerabilidad CVE-2018-8453 se encuentra remediada en estaciones de trabajo y servidores, con esto mitigar un vector de entrada a la red interna del banco y mitigar en parte el riesgo de invasión e integridad de datos.
- Es importante tener los equipos actualizados con los últimos parches de seguridad, se como por ejemplo la vulnerabilidad CVE-2018-8453, la cual puede consultar más información en el siguiente link https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2018-8453

INDICADORES DE COMPROMISO (IOC) Se envia como un documento adicional Anexo1, por la cantidad de IOC obtenidas.

Recuerden, el objetivo de una rápida notificación es poder colaborar en contener, mitigar o analizar el incidente según la línea de tiempo en la que se encuentre.

Cordialmente,

GammaCSOC-CERT
By Gamma Ingenieros