06.09.2020
DIVISIÓN DE REDES Y SEGURIDAD INFORMÁTICA
DEPARTAMENTO CSIRT

COMUNICADO SOBRE ALERTA CIBERNÉTICA
ANÁLISIS DE VECTORES DE ATAQUES ACTIVOS

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRTGOB, realizó un análisis a partir de múltiples fuentes, sobre uno de los vectores de ataques que está circulando en el ecosistema nacional. No se descarta que este vector pueda estar involucrado en el ataque dirigido a las entidades privadas de la economía local en las últimas horas.

El atacante analizado fue 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 el 2019.

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.

Los investigadores de Symantec han detectado campañas de ransomware Sodinokibi dirigidas a buscar software de tarjetas de créditos o puntos de venta (PoS). Además han informado que utilizan el malware básico de Cobal Strike para dirigirlo a las víctimas. Otro punto importante que utilizan herramientas legítimas para ingresar a los sistemas como sistema de control remoto, aprovechando la infraestructura de servicios como cloudfront, Amazon, Pastebin para alojar cargas útiles y para crear la infraestructura de C&C, utilizan infraestructura legitima para no ser detectado y el tráfico no sea marcado sospechoso y ser bloqueado.

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.

Otras investigaciones han detectado que no necesariamente requiere conectarse a C&C para intercambiar las claves de cifrado si no utiliza algoritmo de programación de claves asimétricas, permitiendo que funcione sin ninguna conexión de red. Los datos del sistema y del usuario son transmitidos a varios dominios web legítimos.

HASH Sodinokibi obtenidos de la sandbox Any Run:

B10D9A62EDB6081AA9F7FC865554064BB212555392B1181DC40040E12927F988
2AF156B23D936ECE676FA3AD220672970547F5E3218D2359D2596E47A5BF5D3B
8C5FD31F75250360C0EDC225ECB0C4EF82C27FEF30760B9A8C11241FB0F99092
BBCAEE51155609D365F6BB297D124EFEA685DF0243EC1D4EFB5043D9AFE5963D
879F9F1BDF1FA95606DB35CB23F09E35815984C47BEFA90BF364EB46AB16B107
D621795F5D960A48A332CFED70E1C5EC4F64E02273C82EC4FE03F68B4AFD31C4
51372400BBE34A1744901245949FBA88E6150AB7A1C7BC0A9B3B4D64BF792EFF
63427BEE1D18F5EB9F76A29AE2087EF4FE876480D5998A4D75397BEE7F9F82BC
AAD3F0A2DFC2BFCE8DA3523CC4A4A302D44415EB14DA8586C10B09752B249C39
6727EDBB5D6ABEE908851A8C5FD7B4ACA6D664634FDCDFC15E04502B960ABBC5
36FA3F72AFC2DD6F206A295FC618038FEF5E241BC48BD5451AC9BAB9128734DD
6450C40C8927CA544E562B6FBAA126EA051BC562E7FF09767ACDD84D3EE5D72D
3CDCD89FCAB0C7C765DB551CE38CD021BD740EBC7200B8EA8A255BCDD4318859
8B15999CFF808E9477D25BF0F839AC7C93FA4E62710FB6AE29D33787F1A05F12
D0043EEBE34E492A3827730217F3B4EBA270FD783A3A4D76CEB7CCB64477FD87
D27B1E7E1417B78653E52E0090B1ECE16D18F2C43BCD246E953E7DE6557E6254
6671809C7CF4981D0EF027241B33BA9620CA52422A944129891366FC46758D46
DD6D818BFF148772767D53E19F65BB3C644512BA150DF5110D7A549624055DFB
281A12D96C0436E3B2C3202D7827EB6BED4752E321875764D465727FEF60F24F
368DFD0CE07C2010B0BCFC05B60C653D285B9B201C0DA60C3BE6F6110A89140D

CSIRT sugiere implementar las siguientes recomendaciones a la brevedad posible:

- Aumentar el monitoreo de tráfico no usual,
- Mantener los equipos actualizados, tanto sistemas operativos como otros 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 AntiSpam, 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
- Verificar periódicamente los indicadores de compromisos entregados por Csirt en los informes 2CMV20.
- Segmentar las redes en base a las necesidades de sus activos, permitiendo solamente los puertos necesarios.

En caso de advertir anomalías, CSIRT solicita comunicarse a la brevedad posible al teléfono +(562) 2486 3850, disponible en modalidad 24x7.

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.

Tengan presente que estas actividades o incidentes pueden tipificarse como delitos informáticos según la ley vigente Ley 19.223.

Agradecemos su atención y colaboración,

CSIRT Gobierno de Chile

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática
Subsecretaría del Interior
Gobierno de Chile