14.11.2020
DIVISIÓN DE REDES Y SEGURIDAD INFORMÁTICA
CSIRT DE GOBIERNO

COMUNICADO SOBRE INCIDENTE INFORMÁTICO
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 un incidente que afecta a un sector de la economía local. El análisis identificó la presencia del ransomware Egregor en el ecosistema nacional. Este ransomware implementa técnicas de anti-análisis, como la ofuscación de código y cifrados de carga útil. En una de sus etapas de ejecución la carga útil de Egregor solo se puede descifrar si se proporciona la clave correcta en la línea de comando del proceso. Egregor puede recibir parámetros adicionales a través de la línea de comandos.

CSIRT, cumpliendo el mandato establecido en el Instructivo Presidencial N°8, solicita a los Encargados de Ciberseguridad del Estado tomar las precauciones necesarias para proteger los activos informáticos resguardados por cada una de sus organizaciones, así como el análisis del estado de seguridad de cada una de sus plataformas, lo anterior para evitar que sus unidades se vean afectadas por interrupciones en los servicios que ofrecen a la ciudadanía.

La medida se acompaña de la elevación del estado de alerta de nuestra comunidad a un Nivel Alto.

El Nivel Alto de seguridad que se activa a partir de este momento, implica que existe una amenaza que podría tener un impacto significativo en los sistemas del Estado. Por lo tanto, se advierte a toda la comunidad y entidades asociadas, que CSIRT activará controles de reforzamiento remoto para monitorear y evaluar la situación. De igual forma, todos los encargados de seguridad de la información que participan de esta comunidad deben incrementar el monitoreo de sus sistemas, y evaluar si las características del riesgo requieren del perfeccionamiento de algún procedimiento o de la implantación de alguna medida extraordinaria. De igual forma, deben informar al Equipo CSIRT en caso de detectar alguna afectación de los sistemas, el que estará disponible para apoyar cualquier incidente en modalidad 24x7.

Para conocimiento de la comunidad, CSIRT comparte los IoC recopilados sobre el incidente:

HASH:
81DB87E45619188073E0CAC8E67B9C8DB4361297
FA33FD577F5EB4813BC69DCE891361871CDA860C
069EF8443DF750E9F72EBE4ED93C3E472A2396E2
ED5B60A640A19AFE8D1281BF691F40BAC34EBA8A
7BC6C2D714E88659B26B6B8ED6681B1F91EEF6AF
F0215AAC7BE36A5FEDEEA51D34D8F8DA2E98BF1B

BD8C52BB1F5C034F11F3048E2ED89B7B8FF39261
07D4BCB5B969A01FB21DC28E5CB1B7CEB05F2912
03CDEC4A0A63A016D0767650CDAF1D4D24669795
E27725074F7BC55014885921B7EC8B5319B1EF8F
AC634854448EB8FCD3ABF49C8F37CD21F4282DDE
F73E31D11F462F522A883C8F8F06D44F8D3E2F01
D2D9484276A208641517A2273D96F34DE1394B8E
E0CAAE0804957C5E31C53DD320CA83A5465169C9
D7CB471C1A6F400B04EF0CE19C3CE782F91F37C9

IP:
185.82.126.8

URL:
ozcsgqmpjwromp[.]com
wsjlbbqemr23[.]com
xjkwkzdyfcabhr[.]com
fvkmmwlzvsqdod[.]com
dmvbdfblevxvx[.]com
tczzzlwpss[.]com
txvzmlfzlklhtf[.]com
xtngmptkcqk[.]biz
ihvxmjmdvbn[.]biz
qukqkdcjriz[.]ws
mtafdrvjmif[.]com
kcijbcqvdfv[.]org
tnlttlmxuhc[.]com
txmxffytum[.]biz
vjzwvzjmoc[.]com
ktmjqztagkm[.]org
saalzvhzgkk[.]cc
bvhtxgzwob[.]cc
vrfgwwcesy[.]org
uozwtmgpogg[.]info
qammsjskgkm[.]cc
jfbmnpxgpi[.]ws
hvwvrxpinnv[.]cn
mshrgnslzmqobm[.]com
twcdkhmttfeipv[.]com
sekhmetleaks[.]top
sekhmet[.]top
egregoranrmzapcv[.]onion
wikiegregor[.]top
egregorwiki[.]top
egregor[.]top

http[:]//egregor4u5ipdzhv[.]onion/
https[:]//id-ransomware[.]malwarehunterteam[.]com/identify[.]php?

CSIRT sugiere implementar las siguientes recomendaciones a la brevedad posible:

- Mantener los equipos actualizados, tanto sistemas operativos como otros software instalados.
- Aumentar el monitoreo de tráfico no usual,
- 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
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.11.14 13:31:40 -03'00'

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