MINISTERIO DE DEFENSA

DELEGACION DE DEFENSA EN LA COMUNIDAD VALENCIANA

SUBDELEGACION DE DEFENSA EN VALENCIA

**BOLETIN ESPECIAL MARZO 2020**
**INFORMATIVO DE CIBERDEFENSA**

## *Boletín especial: STIC 02/20: CIBERAMENAZAS RELACIONADAS CON EL COVID-1920*

### *16 de marzo de 2020*

La pandemia provocada por el coronavirus COVI0-19 se ha convertido en una excelente oportunidad para los clberdelincuentes, que aprovechan tanto la avidez de Información de los ciudadanos como la adopción masiva de soluciones de teletrabajo, no siempre con las debidas garantías.

En los últimos días están apareciendo campañas de phishing ofreciendo productos milagro o con falsos resultados de analíticas, ataques de ransomware a hospitales, distribución de malware en aplicaciones informativas sobre la epidemia o campañas de desinformación que aprovechan estas circunstancias. Las siguientes recomendaciones contribuyen a reducir el riesgo.

**Phishing:**

- Sea muy cuidadoso con los correos recibidos con información sobre el COVID-19.
- No pulse enlaces ni abra archivos adjuntos en correos electrónicos, mensajes de texto, WhatsApp, etc.
- Desconfíe de correos que soliciten donaciones a supuestas víctimas.
- Ignore enlaces a páginas web donde ofrezcan vacunas o tratamientos para superar la enfermedad.
- Sospeche de posibles oportunidades de inversión en compañías que afirman poder detectar, prevenir o incluso curar los efectos del virus.
- Nunca conteste al remitente. Uno de sus objetivos es simplemente confirmar direcciones de e-mail.

**Malware:**

Una de las últimas amenazas relacionadas con la pandemia es la difusión de aplicaciones o la aparición de webs maliciosas que ofrecen noticias o mapas interactivos con la expansión de la enfermedad. Estas webs y aplicaciones copian datos de fuentes legítimas, pero su verdadero objetivo es el robo de información sensible, como contraseñas, datos bancarios, contactos, etc . La App más difundida responde al nombre de Corona-Virus·Mop.com. Se trata de un troyano que creará una puerta trasera en nuestro dispositivo, proporcionando acceso remoto a los clberdellncuentes.

- No descargue aplicaciones no oficiales para seguimiento de la epidemia, ni lo haga a través de webs no confiables.

**Teletrabajo:**

Numeroso personal está operando en modalidad de teletrabajo, con el objetivo de reducirlas tasas de contagio. Esto abre una amplia gama de posibles ataques aprovechando debilidades y vulnerabilidades en los equipos y las conexiones.

De forma general, se recomienda lo siguiente:

- Para el acceso a las redes y sistemas de Información del Ministerio desde Internet se debe hacer uso delos mecanismos establecidos por el Nodo de Extranet del Nodo de Interconexión, cumpliendo con todos los requisitos establecidos. Cualquier otro intento de acceder está absolutamente prohibido.
- Compruebe que los equipos usados están correctamente configurados y sus antivirus actualizados.
- No se reenvíe información a otras cuentas de correo externas.
- Nunca trabaje sobre información CLASIF ICADA. Tampoco sobre información sensible aunque no esté formalmente clasificada.
- Restrinja el uso de dispositivos extraibles como pendrlves, discos duros extraíbles, etc. que no hayan sido verificados por el personal de seguridad del emplazamiento. Estos dispositivos deben ser de uso estrictamente personal y no deben ser compartidos con familiares, compañeros y/o amigos.
- Utilice contraseñas seguras para acceder a sus redes inalámbricas y tenga en cuenta con quien las comparte.

**Desinformación:**


Las campañas de desinformación pueden provocar discordia, manipular a la opinión pública, influir en decisiones políticas, alterar el mercado y en general, favorecen la desestabilización de la sociedad, abriendo así nuevas oportunidades para las actividades maliciosas de los ciberdelincuentes .

A la hora de informarse:

- Use fuentes de informaciones seguras y fidedignas, como páginas web de organismos oficiales o medios de comunicación de reconocido prestigio.
- No contribuya a la difusión de información sin contrastar mediante su reenvío a amigos o conocidos.
- No comparta mensajes que pudieran generar alarma social.

## AYUDA CON TU COMPORTAMIENTO A NO COMPLICAR ESTA DIFICIL SITUACIÓN

.

Siempre atento para no picar en los “anzuelos”

Referencias del documento:
Articulo refundido y modificado por la Subdelegación de Defensa en Valencia.
Artículo original publicado en el Boletín de Concienciación del Mando Conjunto de Ciberdefensa.