CIBERSEGURIDAD

El COVID-19 que llega a través de la Red.

El CISO de CastroAlonso, Facundo Gallo nos escribe sus impresiones sobre los peligros del Coronavirus a través de la Red en forma de emails o dominios maliciosos.

Facundo Gallo. BSc (Hons) CISO at CASTROALONSO LET | 16/03/2020 - 18:32h.

En medio de una situación que requiere de la resiliencia y el temple justo en su debido momento, no todas las medidas a adoptar pasan por la higiene personal o el uso de materiales profilácticos. Cuando el virus se ramifica hacia los confines del ciberespacio ¿Cómo podemos estar seguros en nuestras casas, ahora que se han transformado en improvisadas oficinas? Y es que hablamos también de enemigos invisibles, que están ahí, que pasan desapercibidos, y precisamente de eso se trata; son riesgos tecnológicos que han ido in crescendo a medida que la importancia del coronavirus se ganaba su posición estrella en los medios de comunicación, y por extensión, en internet. Como sucede tras un hecho de gran repercusión, se juntó el trending y el desconcierto social en una misma coctelera para poner en bandeja tragos poco apetecibles, servidos desde diferentes países a todas horas.

Muchos ya están hablando de las mil y una fake-news que nos bombardean día y noche, y que por desgracia siguen acaparando tanta atención como los medios oficiales; otros tantos sacan a relucir las problemáticas asociadas a configuraciones in-extremis de VPNs para habilitar el teletrabajo, sobre cómo no fiarnos de todas las soluciones que prometen lo que no está escrito, o como conectarnos de una forma responsable; pero al margen de todo este compendio de información, no debemos olvidar la existencia de otros riesgos independientes a nuestra conexión contra el firewall, el concentrador de VPNs, o lo que hayamos decidido utilizar para acceder a los ficheros de la red empresarial; desde el lado del cibercrimen, es necesario hacer un llamamiento a la población para extremar la precaución contra las nuevas campañas de correos maliciosos, phishing y scam, que intentan explotar la confianza de los usuarios con respecto a ciertos dominios; siguiendo esta línea, las principales firmas de anti-spam y anti-malware están catalogado una cantidad considerables de dominios que contienen la palabra «coronavirus», y que buscan confundir al público general con información que aparenta ser muy interesante, pero que está muy lejos de serlo.

A modo divulgativo, este es un listado de dominios a los que debemos ignorar por completo en caso de tenerlos en nuestra bandeja:

corona-virus.healthcare

survivecoronavirus.org

vaccine-coronavirus.com

coronavirus.cc

bestcoronavirusprotect.tk

coronavirusupdate.tk

coronavirusstatus.space

coronavirus-map.com

blogcoronacl.canalcero.digital

coronavirus.zone

coronavirus-realtime.com

coronavirus.app

bgvfr.coronavirusaware.xyz

coronavirusaware.xyz

¿Qué tipo de mensajes nos pueden llegar a través de estos dominios?

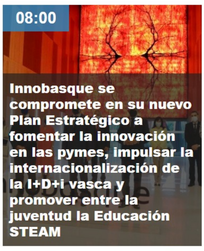
Por lo general, dos elementos anexos a los que la mayoría ya están acostumbrados a ver en este tipo de correos:

Documentos en formato Word.Enlaces a contenido externo.

¿Cuál está siendo la evolución de estas amenazas? ¿Podemos protegernos por nuestros propios medios?

Aplicar reglas de detección basadas en expresiones regulares para encontrar coincidencias en el propio dominio del sender, el header o el cuerpo del mensaje, pueden resultarnos útiles siempre y cuando el valor sea constante, el problema al cual nos enfrentamos es el uso de cadenas variables, y aquí ya dejan de aplicar medidas concretas, dependiendo de la capacidad analítica no solo de las herramientas de seguridad, sino también del personal técnico; un ejemplo de la variación en campañas de estafa vía mail, lo encontramos estos últimos días donde, sin explotar la palabra «coronavirus» en el origen, se generaron supuestos comunicados oficiales del gobierno bajo un dominio visualmente cercano al oficial; pero eso no es todo, seguramente más de uno pudo acceder estos días a su correo y encontrar una lista considerable de e-mails sobre supuestas ventas de mascarillas.

LO ÚLTIMO



LO + VISTO