Que tipo de amenza es?

Vyveva comparte múltiples similitudes de código con muestras más antiguas de Lazarus que son detectadas por los productos ESET como pertenecientes a la familia del malware NukeSped.
NUKESPED es un troyano de puerta trasera que se dirige a usuarios de Mac en Corea.

Como comienza y se propaga esta amenaza?
Los investigadores de ESET han descubierto un backdoor previamente indocumentado utilizado en un ataque a una empresa de logística de carga en Sudáfrica.
Este backdoor consta de varios componentes y se comunica con su servidor de C&C a través de la red Tor.

Hay mas de una amenaza aplicada?
hemos logrado encontrar tres de los múltiples componentes que componen Vyveva: su instalador, loader y backdoor. El instalador es cronológicamente la etapa más temprana encontrada y, dado que espera que otros componentes ya estén presentes en la máquina, sugiere la existencia de una etapa anterior desconocida: un dropper. El loader sirve para descifrar el backdoor utilizando un algoritmo de descifrado XOR simple.

Que solución o medida recomendarian?

Que no usen internet y se queden en casa.