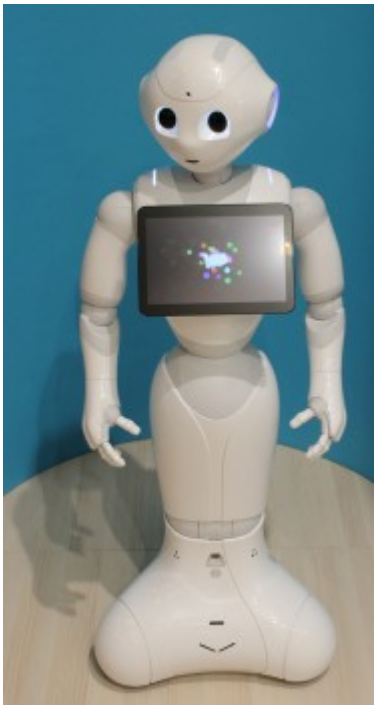
Robot vulnerado: potencialmente peligroso

Lucas Apa y Cesar Cerrudo, dos investigadores de seguridad de la empresa IOActive, han demostrado que un malware instalado en un robot vulnerado lo hace potencialmente peligroso, ya sea para solicitar un rescate o mandar la información que tiene a un cibercriminal, ofender a un cliente si es utilizado en una tienda, o hasta hacer daño físico a una persona.



De acuerdo con su investigación "Hackeando a un robot antes que Skynet", la cual fue demostrada en un video, Apa y Cerrudo hacen ver lo sencillo que es controlar a un robot NEO de SoftBank, desarrollando un ransomware que puede someterlo y obligarlo a exigir dinero, mostrar pornografía en lugares públicos (si se trata de un robot Pepper) e insultar a los clientes.

Este tipo de extorsión a través del ransomware resulta mucho más fácil para los ciberdelincuentes en comparación del ransomware informático tradicional que amenaza a los clientes cifrando su información personal. En la situación presentada por los investigadores de IOActive, sólo necesitan tomar el control del robot y, al impedir que funcione autónomamente, comenzará a hacer que la empresa pierda dinero.

El ransomware no sólo deshabilita a los humaniodes. Apa explicó cómo un atacante podría utilizar a los robots para mostrar imágenes pornográficas o emitir comentarios despectivos a los clientes, si no se quiere pagar el rescate.

Inclusive explica que pueden controlarlo remotamente, para causar daño a una persona. Si bien este malware en particular se enfocaba en el robot NAO, Apa dijo que el mismo código funcionaría en Pepper, que es el robot más utilizado para hacer negocios en tiendas departamentales, comida rápida como Pizza Hut, o para el manejo de pagos digitales con MarterCard.

Los robots sexuales no se quedan fuera. El informe explica que puede convertirse en el blanco perfecto de extorsión, ya que la privacidad y la intimidad son la preocupación principal del usuario,

por lo que antes de contactar al soporte técnico y organizar la recolección del humanoide para su desbloqueo, prefieren pagar un rescate.

Hasta ahí, lo más peligroso que puede pasar es que el robot sexual divulgue los datos y secretos más íntimos de su usuario.

Cuidado en las fábricas

En una fabrica sería diferente. Ahí, en las líneas de trabajo en donde los robots colaborativos están ganando terreno como una herramienta valiosa en la industria manufacturera, cada vez es más normal verlos trabajar mano a mano con obreros, que en muchas ocasiones no usan casco por el grado de confianza que se les tiene.

Los investigadores imaginan una escena en donde los también llamados CoBots son vulnerados y sus protocolos de seguridad que impiden dañar a los humanos son desactivados.

“Pudimos desactivarlos, porque no hay aislamiento de la configuración de seguridad en el robot y los demás componentes”, dijo Apa.

“No hay aislamiento una vez que pirateas el robot y puedes desactivar todo tipo de seguridad”.
Estas fragilidades del sistema son muy peligrosas, de acuerdo con Apa, pues algunos de estos CoBots tienen la facilidad y fuerza suficiente para fracturar un cráneo humano.

Recordemos que un foco rojo fue encendido el año pasado cuando IOActive pudo tomar el control de UBTech, una máquina que después fue reconfigurada para pedir Bitcoins o apuñalar a las personas con un desarmador.

El problema, según Apa, es que muchas de las compañías que desarrollan estos robots no ofrecen formas efectivas de restablecer sus productos de fabrica, anteponiendo el marketing ante la seguridad.