Este Es ‘Killer USB’, Y Puede Explotar Tu Ordenador

¿Pueden los hackers **convertir un ordenador remoto en una bomba** y explotar paraa matar a alguien, igual que lo hacen en las películas de hackers? Espera, espera! Antes de responder a eso, Déjame decirte una historia interesante sobre el controlador **USB Killer**:

Un hombre que camina en el metro robó una unidad flash USB en el bolsillo exterior de la bolsa de otra persona. El pendrive había «128» escrito en él. Después de llegar a casa, e insertar el pendrive en su ordenador portátil y en su lugar de encontrar datos útiles, quemó la mitad de su ordenador portátil. El hombre entonces sacó el pendrive USB, sustituyo el texto «128» por «129» y se lo puso en el bolsillo exterior de su maleta …

Estoy seguro, de que realmente no te imaginarias ser la víctima 130 de este perdrive Killer ;)

Esta historia fue contada por un investigador ruso, apodado **Dark Purple**, el cual encontró el concepto muy interesante y desarrolló su propio asesino pendrive USB, capaz de freír el ordenador.

Él está trabajando con la empresa de fabricación de productos electrónicos desde donde ordenó algunas placas de circuitos de China para la creación de **su propio asesino USB**.

> *«Cuando nos conectamos al puerto USB, una convertidor invertido DC/DC y carga los condensadores a -110V», explicó el investigador. «Cuando se alcanza la tensión, el convertidor DC/DC se apaga. Al mismo tiempo, el transistor de campo se abre.»*

Por fin, desarrolló con éxito un pendrive USB asesino que funcione bien, el cual es capaz de destruir eficazmente los componentes sensibles de un equipo cuando es conectado.

> *«Se usa para aplicar el -110V para señalar las líneas de la interfaz USB. Cuando el voltaje en los condensadores aumenta a -7V, el transistor se cierra y el DC/DC comienza. El ciclo se ejecuta hasta que todo sequema. Quienes están familiarizados con la electrónica ya han adivinado por qué usamos tensión negativa aquí «.*

No es posible para el hardware evitar todo daño a los sistemas físicos en algunos escenarios. Puede ser posible para un atacante explotar vulnerabilidades SCADA y eliminar los controles de seguridad utilizados por las centrales o ponerla en un estado inestable.

El gusano Stuxnet es uno de los ejemplo real de este tipo de ataques cibernéticos, que fue diseñado para destruir las centrifugadoras en la planta nuclear y todo esto comenzó desde una unidad USB.

También en 2014, una empresa de seguridad demostró un ataque en el ordenador Mac de Apple por razones imperiosas de controles de temperatura, lo cual puede hacer arder en llamas la computadora.

Así que si decimos que una computadora podría convertirse en una bomba, entonces por supuesto que es verdad, un hacker probablemente puede hacer que tu equipo también explote.

Por lo tanto, la próxima vez cuando encuentres una **unidad flash USB** desconocida, sólo ten cuidado antes de insertarlo en tu computadora portátil. Porque esta vez no va a despedir de

sus archivos o datos importantes almacenados en su ordenador portátil como lo haría un malware, sino que va a quemar tu ordenador portátil.