Fuente. http://thehackernews.com/2014/06/stuxnet-like-havex-malware-strikes.html

# Investigadores de seguridad han descubierto una nueva Stuxnet como malware, llamado como "Havex", que fue utilizado en una serie de ataques cibernéticos anteriores contra las organizaciones en el sector energético.

Al igual Gusano famoso Stuxnet, que fue especialmente diseñado para sabotear el proyecto nuclear iraní, el nuevo troyano Havex también está programado para infectar a los softwares de sistemas de control industrial de los sistemas SCADA e ICS, con la capacidad de desactivar posiblemente represas hidroeléctricas, sobrecargue las centrales nucleares, e incluso puede apagar la red eléctrica de un país con sólo pulsar una tecla.

Según la firma de seguridad F-Secure, que descubrió por primera vez como Backdoor:. W32 / Havex.A, es un troyano de acceso remoto genérico (RAT) y, recientemente, se ha utilizado para llevar a cabo el espionaje industrial contra una serie de empresas en Europa que utilizan o desarrollar aplicaciones industriales y máquinas.

SMARTY PANTS, TROJANIZED INSTALLERS.

Para lograr esto, además de métodos de infección tradicionales como explotan kits y correos electrónicos de spam, los ciberdelincuentes también utilizaron un otro método eficaz para difundir Havex RAT, es decir, la piratería los sitios web de las empresas de software ya la espera de los objetivos para instalar versiones de troyanos de aplicaciones legítimas.