Video: Análisis de Stuxnet (3 min)

Usted sabe que cuando se trata de noticias de seguridad, la información siempre es confusa. Como espectadores de este espectáculo, saben que existe un ritmo muy regular de problemas de seguridad siempre latentes debajo de la superficie y se requiere de algo verdaderamente profundo para llamar la atención del público. Bueno, una nueva amenaza que se expandió tuvo la combinación ideal de ingredientes el verano pasado. Stuxnet. Quiero decir que tiene sentido, ¿correcto? Ataques a computadoras, energía atómica. Gobiernos extranjeros, sabotaje. Espía contra espía, pero ¿qué es real? Basta decir que es una señal de los tiempos.

Ahora, como todas las buenas amenazas, los detalles seguirán evolucionando, pero creo que hay cinco elementos que vale la pena analizar aquí. El primero es la distribución no trivial. Principalmente, se propaga mediante dispositivos USB. Piense en los sistemas sin conexión a Internet que luego se propagan al extender los niveles de privilegios con ataques de día cero, notables por el hecho de que los ceros verdaderos son especiales y solo son valiosos por un breve período de tiempo. Muy costoso, muy difícil de conseguir. El siguiente es la sofisticación. Es un gusano inteligente. Inicialmente apunta a las computadoras con Windows, donde incluso instala sus propios controladores con un certificado robado pero legítimo. El certificado que produce la falla se revoca por supuesto, pero luego se agrega otro en un plazo de 24 horas. Nuestro tercer punto es la codificación modular. Esta cosa puede cambiar sobre la marcha. Varios servidores de control. Primero en Malasia, luego en Dinamarca, ahora más, incluso entre pares. De hecho, cuando dos de ellos se encuentran, comparan versiones y se aseguran de estar actualizados. El cuarto punto es el alcance único. Windows es solo el intermediario, el amigo del amigo. Stuxnet busca un modelo específico de PLC. Ese es el controlador lógico programable, que técnicamente no es SCADA como se informa a menudo. Estos son pequeños sistemas de control Condustrial integrados que ejecutan toda clase de procesos automatizados, desde fábricas hasta refinerías de petróleo y hasta centrales nucleares. Stuxnet aprovechará la vulnerabilidad del software del controlador para alcanzar y cambiar bits de datos muy específicos. Apague las cosas. No engrase un cojinete a bolas durante 10 minutos. No suene una alarma. Realmente es conocimiento exclusivo. Habilidades respetables de codificación que implican un mayor nivel de paciencia de los buenos recursos de financiación. Nuestro último punto es el motivo. Stuxnet no funciona… Lo siento. No constituye una amenaza. Lleva a cabo un sabotaje. Realmente, no tiene un foco delictivo. No se propaga indiscriminadamente ni roba la información o las credenciales de inicio de sesión de las tarjetas de crédito. No agrupa sistemas en un botnet. Apunta a la infraestructura, nuestras necesidades más esenciales como la energía, el agua, la seguridad y mucho, mucho más. Usted sabe que son sistemas antiguos. Muy establecido. Ejecutar generalmente con la mentalidad de Miren, si no se rompe no lo arreglen. Los técnicos que comprenden este tipo de cuestiones no vigilan ni colocan parches en estas cosas. Al menos no de momento. Por lo tanto, manténgase conectado. Esto no está hecho. Todos tenemos mucho que aprender y alguien está trabajando arduamente para enseñarnos.