Case: Stuxnet Worm 2010

Stuxnet Worm 2010: Iran's Nuclear Program Blocked

Video Youtube

Stuxnet is an extremely sophisticated computer worm that exploits multiple previously unknown Windows zero-day vulnerabilities to infect computers and spread. Its purpose was not just to infect PCs but to cause real-world physical effects. Specifically, it targets centrifuges used to produce the enriched uranium that powers nuclear weapons and reactors.

Stuxnet was first identified by the infosec community in 2010, but development on it probably began in 2005. Despite its unparalleled ability to spread and its widespread infection rate, Stuxnet does little or no harm to computers not involved in uranium enrichment. When it infects a computer, it checks to see if that computer is connected to specific models of programmable logic controllers (PLCs) manufactured by Siemens. PLCs are how computers interact with and control industrial machinery like uranium centrifuges. The worm then alters the PLCs' programming, resulting in the centrifuges being spun too quickly and for too long, damaging or destroying the delicate equipment in the process. While this is happening, the PLCs tell the controller computer that everything is working fine, making it difficult to detect or diagnose what's going wrong until it's too late.

...

In October 2011, Duqu came to light5. This is a descendent of Stuxnet. It used a zero-day exploit to install spyware that recorded keystrokes and other system information. It presages a resurgence of Stuxnet-like attacks but we have yet to see any version of Duqu built to cause cyber-sabotage.Various long term attacks against the petroleum industry, NGOs and the chemical industry6also came to light in 2011. And hactivism by Anonymous, LulzSec and others dominated security news in 2011

Opgaven

1. Wat is een *Windows zero-day vulnerabilitie*?
2. Wat is een computer worm?
3. Zoek op internet hoe deze worm (waarschijnlijk) het gebouw is binnengekomen.

4. Voor deze hack is er (waarschijnlijk) gebruik gemaakt van een zogenaamde rootkit, leg uit wat dat is.
5. Als je deze hacks leest aan welk€ OWASP Risks denk je dan?

Revision #3
Created 2019-10-10 07:41:22 UTC by Admin
Updated 2019-10-10 07:49:15 UTC by Admin