PHYS ORG

Kaspersky team reveals Stuxnet family of weapons

December 29 2011, by Nancy Owano

(PhysOrg.com) -- The Stuxnet cyber weapon that was designed to cripple control systems in Iran's nuclear plant was just one of five weapons engineered in the same lab, and three have not been released yet. That is the word from Moscow based Kaspersky Lab. What's more, according to Kaspersky's director of global research, Costin Raiu, these Lego-like weapons work as modules, in that they are designed to fit together with each having different functions. They were developed on a single platform whose roots trace back at least to 2007; the creators have used the same software development environment ever since.

Raiu told Reuters about the findings on Wednesday based on the evidence that his team has gathered. He cited Stuxnet--the Iran-targeted weapon-- and a related Duqu--the data-scoffing Trojan targeting design documents that showed up this year in Europe-- as two of what might be a lethal assembly—three of the weapons have yet to be released.

Besides Kaspersky, other anti-virus leaders such as Symantec and Trend Micro incorporated technology into their products to protect systems against Stuxnet and Duqu; Raiu says that these viruses may be more sophisticated than previously known.

Kaspersky named the platform "Tilded" because many of the files in Duqu and Stuxnet have names beginning with the tilde symbol "~" and the letter "d." What Kaspersky recently discovered is that shared components search for at least three other unique registry keys, It is possible that at least three other pieces of malware have been built that use the same platform. It would be relatively easy for the developers of those highly sophisticated viruses to create other weapons.

Developers can build new cyber weapons by simply adding and removing modules, he told Reuters, "It's like a Lego set. You can assemble the components into anything: a robot or a house or a tank.”

The Kaspersky team cited 2007 because installed code by Duqu was compiled from a device running Windows on August 31, 2007. Kaspersky sources did not name a country responsible for the cyber weapons. When contacted by the press about Kaspersky’s findings, the Pentagon declined comment.

Kaspersky Lab is a vendor of security software. In 1999, Kaspersky Labs, says the company, was the first to introduce integrated antivirus software for workstations, file servers and application servers running on Linux/FreeBSD operating systems.

More information:
via Reuters

© 2011 PhysOrg.com

Citation: Kaspersky team reveals Stuxnet family of weapons (2011, December 29) retrieved 19 April 2024 from https://phys.org/news/2011-12-kaspersky-team-reveals-stuxnet-family.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.