Stuxnet code : Free Download, Borrow, and Streaming : Internet Archive

Stuxnet is believed to be a jointly built American-Israeli cyber weapon and computer worm. These claims have never been confirmed by either nation state. According to anonymous US officials speaking to the Washington Post, the worm was developed during the administration of George W. Bush to sabotage Iran's nuclear program with what would seem like a long series of unfortunate accidents.

Stuxnet has three modules: a worm that executes all routines related to the main payload of the attack; a link file that automatically executes the propagated copies of the worm; and a rootkit component responsible for hiding all malicious files and processes, preventing detection of the presence of Stuxnet.

Stuxnet is typically introduced to the target environment via an infected USB flash drive. The worm then propagates across the network, scanning for Siemens Step7 software on computers controlling a PLC. In the absence of either criterion, Stuxnet becomes dormant inside the computer. If both the conditions are fulfilled, Stuxnet introduces the infected rootkit onto the PLC and Step7 software, modifying the codes and giving unexpected commands to the PLC while returning a loop of normal operations system values feedback to the users.

Addeddate
: 2015-09-12 11:24:48

Collection_added
: usgovernmentmirrors
: government-documents

Identifier
: Stuxnet

Identifier-ark
: ark:/13960/t3hx5022b

Scanner
: Internet Archive HTML5 Uploader 1.6.3

comment

Reviews (1)

49,617 Views

32 Favorites

1 Review

DOWNLOAD OPTIONS

Uploaded by Unknown on September 12, 2015
