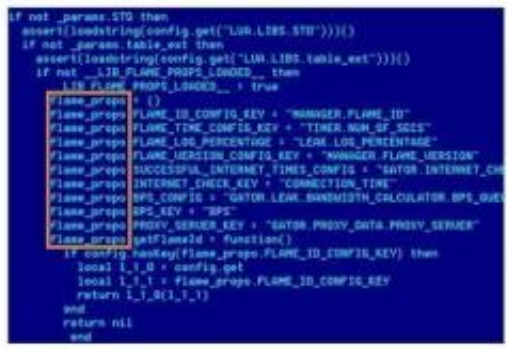
Mystery virus sought 'designs from Iran': Russian firm

June 5 2012



Code from the computer virus known as Flame. A mystery computer virus discovered last month and deployed in a massive cyberattack chiefly against Iran sought to steal designs and PDF files from its victims, a Russian firm said.

A mystery computer virus discovered last month and deployed in a massive cyberattack chiefly against Iran sought to steal designs and PDF files from its victims, a Russian firm said.

Kaspersky Lab, one of the world's biggest producers of anti-virus software, announced last month the discovery of the Flame virus, which it described as the biggest and most sophisticated malware ever seen.

In the latest update on Kaspersky's analysis of the virus, released late Monday, the firm's chief security expert, Alexander Gostev, said the malware's creators had focussed on file formats such as PDF and

AutoCAD, a software for computer design and drawing.

"The attackers seem to have a high interest in AutoCAD drawings," Gostev said in a statement.

The malware also "goes through PDF and text files and other documents and makes short text summaries," he added.

"It also hunts for e-mails and many different kinds of other 'interesting' (high-value) files that are specified in the malware configuration."

He confirmed that Iran was by far the biggest target with a count of 185 infections, followed by 95 in Israel and the Palestinian Territories, 32 in Sudan and 29 in Syria.

The discovery of Flame immediately sparked speculation that it had been created by US and Israeli security services to steal information about Iran's controversial nuclear drive.

Intriguingly, Kaspersky said that hours after the existence of the virus was first announced on May 28, "The Flame command-and-control infrastructure, which had been operating for years, went dark."

It gave no further information over the possible perpetrators of the mystery attack, though it identified about 80 domains that appear to belong to the Flame infrastructure, in locations from Hong Kong to Switzerland.

Kaspersky said it had used a procedure known as sinkholing -- which allows Internet security experts to gain control of a malicious server -- to analyse the operation.

During the sinkholing it found that on three computers in Lebanon, Iraq

and Iran the Flame versions changed, suggesting Flame upgraded itself in the process.

The New York Times reported last week that President Barack Obama has accelerated cyberattacks on Iran's nuclear programme in an operation codenamed "Olympic Games" that uses a malicious code developed with Israel.