Kaspersky Lab: Duqu, Stuxnet... Team created other malicious programs

MOSCOW, RUSSIA: New information on the infections with the Duqu and Stuxnet Trojans confirms that one team is behind this family of malicious programs, and also permits the assumption that a single platform was used, which is flexibly adaptable to specific targets. Besides, this platform may have been developed long before the Stuxnet epidemic and used more actively than has been thought up to now.

Such a conclusion was made by Kaspersky Lab experts based on detailed analysis of the drivers used for infecting systems with Duqu and Stuxnet, and also some malicious programs details of which are as yet unknown.

The platform, which has been dubbed "Tilded" (because of the tendency of its creators to use files that start with the tilde symbol (~)), in the opinion of Kaspersky Lab's experts was used for the creation of Stuxnet and Duqu, and also other malicious programs.

The connection between Duqu and Stuxnet was revealed during the analysis of one of the incidents with regard to Duqu. During the investigation of the infected system thought to have been attacked in August 2011, a driver was found that was similar to the one used by one of the versions of Stuxnet. Though there were clear likenesses between the two drivers, there were also some differences in the details, such as the date of signing of the digital certificate. Other files which it was possible to attribute to the activity of Stuxnet were not found, but there were traces of activity of Duqu.

Similar characteristics

The processing of the obtained information and the further search in the database of malicious programs of Kaspersky Lab allowed to reveal one more driver with similar characteristics. It was discovered more than a year ago, but the file was compiled in January 2008, a year before the creation of the drivers used by Stuxnet. Kaspersky Lab experts found seven types of drivers with similar characteristics. It is noteworthy that for three of them there is as yet no information about specifically which malicious program with which they were used.

Alexander Gostev, chief security expert at Kaspersky Lab, said: "The drivers from the still unknown malicious programs cannot be attributed to activity of the Stuxnet and Duqu Trojans. The methods of dissemination of Stuxnet would have brought about a large number of infections with these drivers; and they can't be attributed either to the more targeted Duqu Trojan due to the compilation date. We consider that these drivers were used either in an earlier version of Duqu, or for infection with completely different malicious programs, which moreover have the same platform and, it is likely, a single creator-team".

Separate projects, single platform

According to Kaspersky Lab's experts' version, the cybercriminals behind Duqu and Stuxnet create a new version of the driver several times a year, which is used for loading the main module of the malicious program. Upon planned new attacks, with the help of a special program several parameters of the driver are changed, for example like the registry key.

Depending on the task, such a file can also be signed by a legal digital certificate, or remain without a signature at all.

Thus, Duqu and Stuxnet are separate projects, which were created on the basis of a single platform - Tilded - which was developed around the end of 2007 and the beginning of 2008. It is most likely that this project was not the only one, but the aims and tasks of the different variants of the Trojan program are as yet unknown. It cannot be ruled out that this platform continues to develop; moreover, the discovery of Duqu by security experts will mean further changes are being or will be made to the platform.

The full version of the report of Alexander Gostev and Igor Sumenkov is available at Securelist.