BIZCOMMUNITY

Insight on Duqu - the step-brother of Stuxnet?

MOSCOW, RUSSIA: The spread across the Internet of several versions of the malicious program Duqu has become a main news item in the IT security industry of late.

In no small part is this due to some similarities between this new worm and last year's infamous Stuxnet worm. What is alarming in this case, however, is that the ultimate objective of Duqu remains unknown. Anti-malware experts at Kaspersky Lab have carried out their analysis of the new malware, the main findings of which are as follows.

The Duqu worm was first detected in early September 2011, after a user in Hungary uploaded one of the components of the malicious software to the Virustotal website, which analyses infected files with anti-virus programs of different manufacturers (including Kaspersky Lab's). However, this first-detected sample turned out to be one of several components that make up the whole of the worm. A little later, in a similar way, the Kaspersky Lab anti-malware experts received a sample of another module of the worm via Virustotal, and it was specifically its analysis that resembled Stuxnet.

Similar worms, but significant differences

Though there are some overall similarities between the two worms Duqu and Stuxnet, there are also significant differences. Shortly after several variants of Duqu had been found, the Kaspersky Lab experts started to track real-time infection attempts by the worm among users of the cloud-based Kaspersky Security Network. What was surprising was that during the first 24 hours only one system had been infected by the worm. Stuxnet, on the other hand had - assumedly - infected tens of thousands of systems all around the world. However, it had a single ultimate target - industrial control systems used in Iran's nuclear programs.

The only infection with the Duqu worm on the other hand, among users of the Kaspersky Security Network, is an infection with one of the several modules that presumably make up the worm. Instances of infection by the second module, which is in essence a separate malicious program - a Trojan-Spy - have not yet been found. It is specifically this module of Duqu that possesses the malicious functionality - it gathers information about the infected machine and also tracks key strokes made on its keyboard.

Duqu may have specific targets

Alexander Gostev, chief security expert with Kaspersky Lab, said: "We've not found any instances of infections of computers of our clients with the Trojan-Spy module of Duqu. This means that Duqu may be aimed at a small quantity of specific targets, and different modules may be used to target each of them."

One of the yet-to-be-solved mysteries of Duqu is its initial method of penetration into a system - the installer or "dropper" needed for this has not yet been found.

Experts at Kaspersky Lab are continuing their ongoing investigation into the new malicious program Duqu and since discovering the first samples of the malicious program, four new instances of infection have been detected - thanks to the cloud-based Kaspersky Security Network. One of these was tracked down to a user in Sudan and the other three were located in Iran.

Exploiting vulnerabilities

In each of the four instances of Duqu infection a unique modification of the driver necessary for infection was used. More importantly, regarding one of the Iranian infections, there were also found to have been two network attack attempts exploiting the MS08-067 vulnerability. This vulnerability was used by Stuxnet too, and also another, older, malicious program, Kido. The first of the two network attack attempts took place on 4 October, the other on 16 October 2011, and both originated from one and the same IP address - formally belonging to a US Internet provider. If there had been just one such attempt, it could have been written off as typical Kido activity - but there were two consecutive attack attempts: this detail would suggest a targeted attack on an object in Iran. It is also possible that in its operation other vulnerabilities of software were exploited.

Gostev said: "Despite the fact that the locations of the systems attacked by Duqu are located in Iran, to date there is no evidence of there being industrial or nuclear program-related systems. As such, it is impossible to confirm that the target of the new malicious program is the same as that of Stuxnet. Nevertheless, it is clear that every infection by Duqu is unique. This information allows one to say with certainty that Duqu is being used for targeted attacks on pre-determined objects."

Detailed results of the new investigation on Duqu are available here at Securelist.