Uroburos rootkit: Belgian Foreign Ministry stricken

gdatasoftware.com/blog/2014/05/23958-uroburos-rootkit-belgian-foreign-ministry-stricken

The advanced and highly complex spyware first became a media item in February 2014 following extensive analysis by experts at G DATA. Straightaway the indications were that Uroburos was not designed to target everyday users. Following the cyber attack on the Belgian Foreign Ministry, information has now been published concerning the affliction of a government institution.

On Saturday Belgian Foreign Minister Didier Reynders stated that "information and documents on the crisis in Ukraine" had been smuggled out of the government institution's networks, reported Die Welt and other news media. At this time neither the origin nor the nature of the attack had been clarified by official sources. However, Belgian financial newspaper De Tijd named Moscow as the source of the attack shortly after, and Le Soir was also connecting it with Russia.

Today: infection by Uroburos rootkit confirmed

"The effort put in by the developers and contracting authorities behind Uroburos is only justifiable if the targets are worthwhile, i.e. for spying on major enterprises, national institutions, news services and similar targets," said G DATA experts in their initial blog article on the subject.

Belgian daily newspaper De Standaard considers the source for their article today to be trustworthy. It confirmed that the government institution had been infected with the spyware Uroburos, which is also called "Snake" in some cases. Experts at the military intelligence service are currently working on counter-measures and cleaning up the network, it said. French newspaper Le Soir also reported the Uroburos attack on the Belgian government in today's edition. The Belgian intelligence service is named as the source of the information.

Is this just the tip of the iceberg?

Even though the level of detail of the information that has been publicly disclosed on this cyber attack is low, and may well remain so, there is nevertheless little doubt that the Uroburos software has caused significant damage. The G DATA experts expect that the recent development in Belgium is just the tip of the iceberg, all the more so since Le Soir reported last Saturday that other European countries had found the same problem.

- Malware
- Vulnerabilities
- CyberCrime