Stonesoft finds new threat to company computer networks

October 18 2010

Stonesoft logo. The Finnish company Stonesoft said Monday it had found new techniques that bypass current security systems which cyber-criminals could use to gain access company productivity applications.

The Finnish company Stonesoft said Monday it had found new techniques that bypass current security systems which cyber-criminals could use to gain access company productivity applications.

Stonesoft said that as a result of the advanced evasion techniques (AETs) "companies may suffer a significant data breach including the loss of confidential corporate information."

In addition these AETs "could be used by organised crime and cyber-terrorists to conduct illegal and potentially damaging activities," the company said in a statement.

These AETs are a sort of "stealth plane that isn't detectable by radar and which leaves the door open to cyber-criminals and gives them the time and leisure to test various vulnerabilities" in corporate systems, Stonesoft's director in France and the Benelux countries Leonard Dahan told AFP.

By bypassing today's network security systems the AET's provide cyber-criminals with a "master key" to access vulnerable systems such as customer relationship management (CRM) and enterprise resource planning (ERP) applications, said the company.

Stonesoft said it had notified CERT-FI, which is charged with globally coordinating response to vulnerabilities among network security vendors and ICSA Labs which offers third-party testing and certification of security products and network-connected devices.

Dahan said that "given the enormity of what has been discovered, it is important for Stonesoft that one can work together with other R and D teams to move as quickly as possible to develop solutions."

"When one looks at the news over the past 10 months, such as a student who managed to penetrate NASA's network or that one can gain control of Siemens systems in Iran by bypassing all known security systems, that is because hackers use evasion techniques that are not detectable today..." said Dahan.

A self-replicating piece of malware called Stuxnet was publicly identified in June lurking on Siemens industrial systems, particularly in Iran, India, Indonesia and Pakistan.

Analysts say Stuxnet may have been designed to target Iran's nuclear facilities, especially the Russian-built first atomic power plant in the southern city of Bushehr.

(c) 2010 AFP