Flame malware constitutes a 'cyber weapon'

Kaspersky Lab argues there is an urgent need for an international convention to control the use of cyber weapons.

By Duncan McLeod: @mcleodd 1 Jun 2012

The Flame malware that infected computers across the Middle East and North Africa is a "cyber weapon", probably developed by a nation state for the purpose of espionage.

This is the view of Vitaly Kamluk, chief malware expert at Russia's Kaspersky Lab, the antivirus company t played an instrumental role in uncovering the malware, which has been described as the most sophisticate software of its kind ever detected.

Kamluk was speaking to TechCentral from Moscow on Wednesday [30 May 2012]. He says Kaspersky ha been unable to determine the origin of the malware or how it was first propagated, but says it is a highly complex piece of software - 20 times more complex than the Stuxnet worm, discovered in 2010, that targeted Siemens industrial software and equipment. It's been speculated that Israel and/or the US were behind development of both Flame and Stuxnet. Stuxnet targeted five Iranian organisations, reportedly damaging Iran's nuclear programme.

Through its antivirus software, Kaspersky is aware of the virus infecting 600 machines, but Kamluk believe there are probably thousands of machines that were compromised. It can record audio, grab screenshots and monitor keyboard activity and network traffic. It can even record Skype conversations and download contact information from nearby Bluetooth-enabled mobile phones.

Kamluk says it appears the developers and controllers of the Flame malware, which spreads through Microsoft Windows-based computers, were able to use it to obtain vital information use it to "destroy" operating systems, rendering machines "completely broken".

Flame, Kamluk says, is part of a "small group of malicious applications that can be referred to as 'cyber weapons'". With all its modules, the virus is 20MB in size, which is unusually large for malware.

Kaspersky Lab has tried to determine who wrote the software, but admits it hit a brick wall in its investigations. "There was obviously no contact information in the body of the malware, so we tried to find out what it does and where it is controlled from," Kamluk says. "We discovered dozens of servers located different countries."

Continue reading the full story on www.TechCentral.co.za.

ABOUT DUNCAN MCLEOD: @MCLEODD

Award-wining Duncan McLeod is the founder and editor of TechCentral (www.TechCentral.co.za, @TechCentral]]), South Africa's latest technology news site offering breaking news depth analysis and opinion that launched in September 2009. Before that, he was associate editor at the *Financial Mail*/*FM*. Contact Duncan on email duncan at techcentral dot co dot and follow him on Twitter at @mcleodd.
View my profile and articles...