Malware aimed at disrupting US and Europe's energy supplies

WASHINGTON, USA: Cyber-attackers, possibly even state sponsored, have been targeting energy operations in the United States and Europe since 2011 and were capable of causing significant damage, security researchers have claimed.

Powerlines, transport networks and critical infrastructure in Europe and the USA could be crippled by Dragonfly malware claims Symantec. Image: Ukraine Business

The US security firm Symantec said it identified malware targeting industrial control systems which could sabotage electric grids, power generators and pipelines.

"The attackers, known to Symantec as Dragonfly, managed to compromise a number of strategically important organisations for spying purposes," Symantec said in a blog post.

"If they had used the sabotage capabilities open to them, (they) could have caused damage or disruption to energy supplies in affected countries," it added.

The researchers said this malware is similar to Stuxnet, a virus believed to have been developed by the United States or Israel to contain threats from Iran.

"Dragonfly bears the hallmarks of a state-sponsored operation, displaying a high degree of technical capability," Symantec said.

"Its current main motive appears to be cyber-espionage, with potential for sabotage a definite secondary capability," it claimed

Cyber-attacks could cripple infrastructure

Symantec said the Dragonfly, also known as Energetic Bear, appeared to be an operation based in Eastern Europe calculated by the hours of activity of those involved.It said one of the tools was a Trojan that appeared to have originated in Russia.

Officials in the US and elsewhere in recent months have expressed growing concerns about cyber-attacks which could cripple critical infrastructure systems such as power grids, water systems or transportation networks.

The Dragonfly group has used several infection tactics including spam email with malicious attachments and browser tools that are capable of installing malicious.

Once installed on a victim's computer, the malware gathers system information and can extract data from the computer's address book and other directories.

"The Dragonfly group is technically adept and able to 'think' strategically," Symantec said.

"Given the size of some of its targets, the group found a 'soft underbelly' by compromising their suppliers, which are invariably smaller, less protected companies," it said.

Symantec said it had notified victims of the attacks as well as relevant national authorities, such as the US Computer Emergency Response Team.

The affected companies were not named, but Symantec said targets of Dragonfly included energy grid operators, major electricity generation firms, petroleum pipeline operators, and energy industry equipment providers.

Most targets were located in the United States, Spain, France, Italy, Germany, Turkey, and Poland.

Source: AFP via I-Net Bridge