

## Cisco Security Agent live demonstration

Written by Alexei Spirin

Saturday, 12 January 2008 07:07 - Last Updated Saturday, 25 October 2008 09:25

---

For those who interested in Cisco Security Agent (CSA) i've prepared the live demonstration of an attack and how CSA can stop that. The first part of demo includes Internet Explorer remote exploitation, which gives remote shell to the 'villain' and the second part shows what happens if CSA intalled on victims computer.

The matter is that I was astonished by simplicity how almost anyone could be compromised by just clicking on &quot;harmless&quot; link. How many links do you click every day? Hundreds? Thousands? A lot! And any of them could be as dangerous as a villain wants that to be. Remote access to your PC, VNC-server installation? A piece of cake.

And by the way, firewall isn't an option here.

The demo consists of two files and available at [Downloads page](#) . The first of them shows how unprotected user could be compromised by clicking on some link. The second example shows how CSA could protect user's PC.

Additional info: CSA is installed with default policies (that why it shows some questions to the end-user); Windows XP SP1 was used as a victim OS; [Metasploit framework](#) was &quot;editor's choice&quot; for a demonstration ;).