



RE: Open points

Marco Valleri

Sent: Thursday, February 7, 2013 at 7:45 AM

To: 'Mostapha Maanna'; 'Daniele Milan'; 'naga'

Cc: 'vale Bedeschi'; 'm.bettini Bettini'; 'd.vincenzetti Vincenzetti'; 'g.russo Russo'

Ecco le risposte:

1 & 2) As you noticed, the installer doesn't require to click on the UAC prompt anymore. It makes the installation process more silent and secure. As a side effect it doesn't grant full administrative privileges to the agent, that is not able to interact with drivers and services anymore (DeepFreeze and MsConfig)

3) The AV Report is sent on each new release that modifies the agents' cores. If we notice that the agent is not resistant to one of the supported AV anymore, we release an agent upgrade with a new AV Report. If you receive no reports it means that no changes has been noticed in the AVs behavior.

4) Digitally Signing an executable file requires a special certificate, and we cannot require a certificate as HackingTeam for obvious reasons. The old OPM Security certificate has been compromised so we obtained a new one as Kamel Abed. You can sign the agent with your own Digital Certificate if you can obtain it: the import procedure is straightforward.

--

Marco Valleri

CTO

Hacking Team

Milan Singapore Washington DC

www.hackingteam.com