

Massachusetts Senate Race queries on search engines could install malware

Rogue antivirus is the winner in the confrontation between the Democrat Martha Coakley and Republican Scott Brown

Malware authors continue to exploit the same social engineering vector of curiosity to lure their victims into endangering their data. Inquiring users employing unprotected systems could be exposed by simply clicking the apparently innocent links related to the election topic.

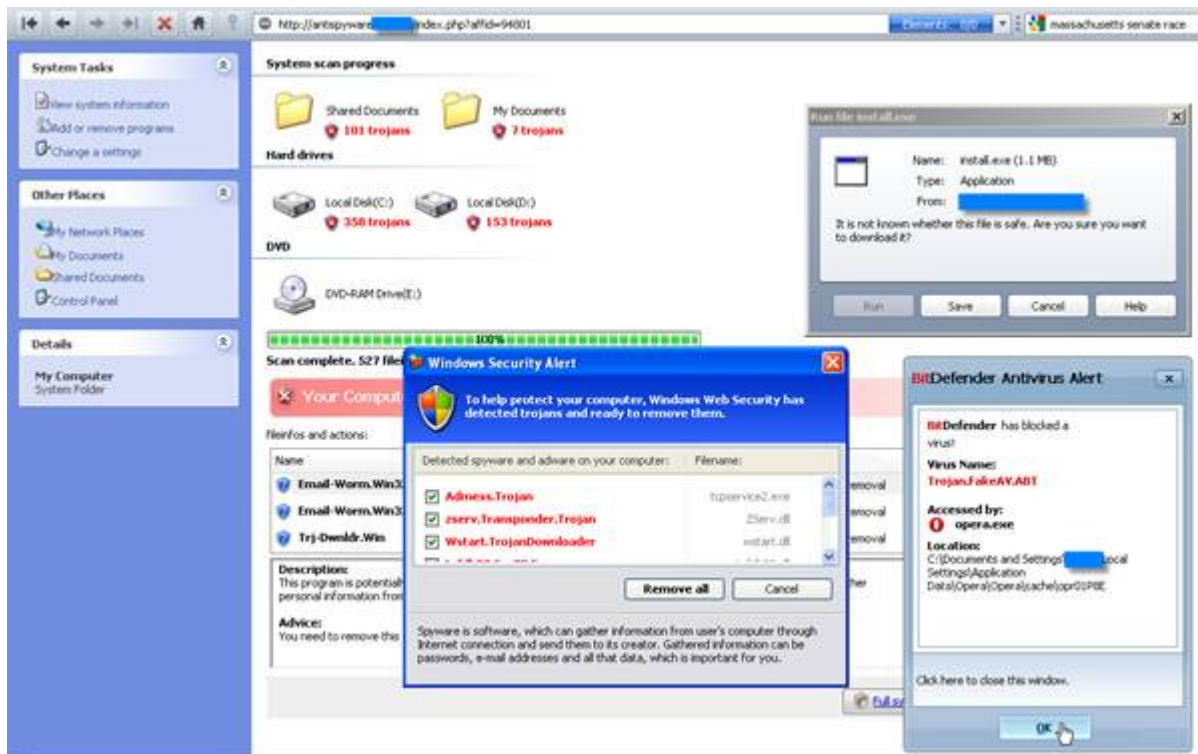
The M.O. is classical: when clicked, the link of an apparently legitimate Web site displayed in the search results page automatically redirects the browser towards a Web page that infects the unwary user with a variant of **System Security Rogue** detected by BitDefender as [Trojan.FakeAV.ABT](#).



Its behaviour is similar to its older “relatives” – XP Antivirus, Antivirus 2009, AV360, Personal Antivirus or Total Security Rogue: when landing on the malware distribution Web page, the browser window is automatically minimized and a warning message simultaneously displays, notifying the user about several computer infections and the availability of **System Security**.



By clicking either OK or Cancel buttons of the several pop-up windows invading the screen, the user triggers a fake movie that plays in the restored browser window. The movie mimics an on-going scanning process that supposedly detects loads of malware onto the system, while other fake pop-up windows should swindle the user into downloading the malware.



System Security Rogue tries to trick the user into registering the fake product by giving notices of false detections, more and more at each so called scan. Once on the machine, it alters or irremediably damages the content of several system files and delivers numerous pop-ups with bogus system problems and fake infections, while also incessantly requesting the user to buy/renew a license. To be more persuasive, it also removes the users' desktop wallpaper and blocks multiple applications.

To protect your systems and data and avoid compromising your systems and data, follow the five security tips below:

- install and activate a reliable [antimalware, firewall solution and spam filter](#), such as those provided by [BitDefender](#).
- update your antimalware, firewall and spam filter as frequent as possible, with the latest virus definitions and suspicious applications/files signatures.
- scan your system frequently.
- check on a regular basis with your operating system provider – download and install the latest security updates and malicious removal tools, as well as other patches or fixes.
- do not download or save files from sources you don't know; avoid opening or copying onto your system any file, even if it comes from a trusted source, before running a complete antimalware scan.