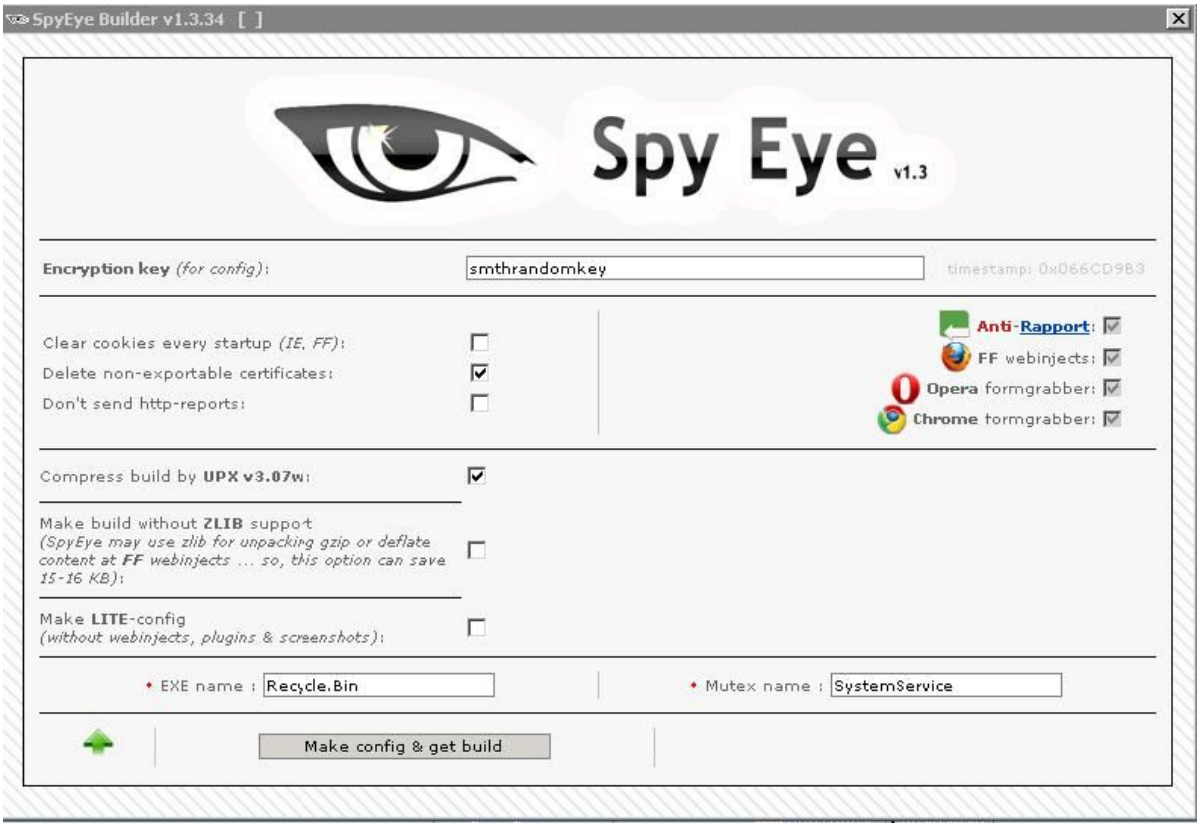
SpyEye Targets Opera, Google Chrome Users

krebsonsecurity.com/2011/04/spyeye-targets-opera-google-chrome-users/

The latest version of the **SpyEye trojan** includes new capability specifically designed to steal sensitive data from Windows users surfing the Internet with the **Google Chrome** and **Opera** Web browsers.

The author of the SpyEye trojan formerly sold the crimeware-building kit on a number of online cybercrime forums, but has recently limited his showroom displays to a handful of highly vetted underground communities. KrebsOnSecurity.com recently chatted with a member of one of these communities who has purchased a new version of SpyEye. Screenshots from the package show that the latest rendition comes with the option for new “form grabbing” capabilities targeting Chrome and Opera users.



SpyEye component in version 1.3.34 shows form grabbing options for Chrome and Opera

Trojans like ZeuS and SpyEye have the built-in ability to keep logs of every keystroke a victim types on his or her keyboard, but this kind of tracking usually creates too much extraneous data for the attackers, who mainly are interested in financial information such as credit card numbers and online banking credentials. Form grabbers accomplish this by stripping out any data that victims enter in specific Web site form fields, snarfing and recording that data before it can be encrypted and sent to the Web site requesting the information.

Both SpyEye and ZeuS have had the capability to do form grabbing against Internet Explorer and Firefox for some time, but this is the first time I've seen any major banking trojans claim the ability to target Chrome and Opera users with this feature.

Aviv Raff, CTO and co-founder of security alert service Seculert, said that both SpyEye and ZeuS work by "hooking" the "dynamic link library" or DLL files used by IE and Firefox. However, Chrome and Opera appear to use different DLLs, Raff said.

This strikes me as an incremental yet noteworthy development. Many people feel more secure using browsers like Chrome and Opera because they believe the browsers' smaller market share makes them less of a target for cyber crooks. This latest SpyEye innovation is a good reminder that computer crooks are constantly looking for new ways to better monetize the resources they've already stolen. Security-by-obscurity is no substitute for good

security practices and common sense: If you've installed a program, update it regularly; if you didn't go looking for a program, add-on or download, don't install it; if you no longer need a program, remove it.