SpyEye vs. ZeuS Rivalry

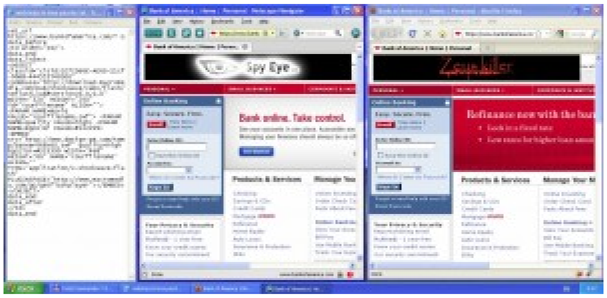
krebsonsecurity.com/2010/04/spyeye-vs-zeus-rivalry/

It’s common for malware writers to taunt one another with petty insults nested within their respective creations. Competing crime groups also often seek to wrest infected machines from one another. A very public turf war between those responsible for maintaining the Netsky and Bagle worms back in 2005, for example, caused a substantial increase in the volume of threats generated by both gangs.

The latest rivalry appears to be budding between the authors of the Zeus Trojan — a crime kit used by a large number of cyber thieves — and “SpyEye,” a relatively new kit on the block that is taking every opportunity to jeer at, undercut and otherwise siphon market share from the mighty Zeus.

Symantec alluded to this in a February blog post that highlighted a key selling point of the SpyEye crimeware kit: If the malware created with SpyEye lands on a computer that is already infected with Zeus, it will hijack and/or remove the Zeus infection.

Now, just a few months later, the SpyEye author is releasing a new update (v. 1.1) that he claims includes the ability to inject content into **Firefox** and **Internet Explorer** browsers, just as Zeus does (this screen shot shows the result of a demo configuration file on the left, which instructs the malware to inject SpyEye and “Zeuskiller” banner ads into a live Bank of America Web site). It is precisely this injection ability that allows thieves using Zeus to defeat the security tokens that many banks require commercial customers to use for online banking.



The new version comes as the Zeus author is pushing out his own updates (v. 1.4), along with a hefty price tag hike. The old Zeus kit started at around $4,000, while the base price of the newer version is double that. According to research from Atlanta-based security firm **SecureWorks**, Zeus plug-ins that offer additional functionality raise the price even more. For example:

-Windows7/Vista compatibility module – $2,000
-Backconnect module (lets criminals connect back to victim and make bank transactions through that PC) – $1,500
-Firefox form grabbing (copies out any data entered into a form field, such as a user name and password) – $2,000
-Jabber notification (a form of instant message) – $500

-FTP clients saved credentials grabbing module – $2,000
-VNC module — $10,000 (like GoToMyPC for the bad guys, reportedly no longer being sold/supported)

The SpyEye author declined to be interviewed for this story. But it’s clear from his Flash banner ads reproduced here that he plans to keep up the public relations campaign against Zeus, with a focus on the relatively low price: SpyEye costs just $500 (although the new Firefox injection tool runs an extra $1,000).

SecureWorks has noted that the latest versions of Zeus include anti-piracy technology that uses a hardware-based licensing system that can only be run on one computer. “Once you run it, you get a code from the specific computer, and then the author gives you a key just for that computer,” SecureWorks wrote. “This is the first time we have seen this level of control for malware.”

Not to be outdone, the SpyEye author now claims his malware builder also includes a hardware lock, using **VMProtect**, a Russian commercial software protection package.