SpyEye’s "Kill Zeus" Bark is Worse Than its Bite

0 Recommend

Apr 26, 2010 06:50 AM

Migration User

In an earlier blog entry we mentioned SpyEye as a new, up-and-coming crimeware toolkit to look out for. In that blog we highlighted the Kill Zeus feature, which had just been added to the SpyEye Trojan builder at that time. We can now substantiate that this Kill Zeus feature does actually work. Well, some of the time. In my opinion the Zeus toolkit creators don’t need to lose any of their precious sleep just yet.

Our analysis has shown that the kill Zeus feature seems to work on a limited number of Zeus samples. In March 2010, Symantec alone counted 9,779 new unique samples of what we call Trojan.Zbot. We estimate that only a small percentage of these samples can be successfully removed by SpyEye’s Kill Zeus feature. The samples we observed it working successfully on are most likely created with one version of the Zeus Trojan builder, of which there are now several. To soften the blow even more, the version of the Zeus Trojan builder that the feature works on seems to be an earlier one, now widely available for free. The SpyEye creator most likely got a hold of a copy of this Zeus builder and based his detection and remediation on backwards-engineering the samples it created. If anything, this Kill Zeus feature might actually convince Zeus builder users to upgrade to a paid version.

The following video shows what happens when a computer compromised by Trojan.Zbot is subsequently infected with Trojan.Spyeye, using the Kill Zeus feature (when it works correctly).

New revisions of both the Zeus and SpyEye crimeware toolkits are being released on a regular basis, with additional features or protection added. As always, Symantec recommends that you keep your definitions up to date in order to ensure protection against these threats and others.

Thanks to Cathal Mullaney for his input on this blog entry.

Statistics

0 Favorited

0 Views

0 Files

0 Shares

0 Downloads

Tags and Keywords

Related Entries and Links

No Related Resource entered.