Endpoint Protection

symantec.com/connect/blogs/spyeye-bot-versus-zeus-bot

Back to Library

SpyEye Bot versus Zeus Bot

0 Recommend

Feb 04, 2010 01:36 PM

Migration User

The Zeus crimeware toolkit has been around now for a while and has grown over time to be the most established crimeware toolkit in the underground economy. In late December 2009 a new crimeware toolkit emanating from Russia—known as SpyEye V1.0—started to appear for sale on Russian underground forums. Retailing at $500, it is looking to take a chunk of the Zeus crimeware toolkit market. Symantec detects this threat as Trojan.Spyeye. Since it is relatively new, we are not seeing a lot of SpyEye activity yet. However, given some time and the observed rate of development for this crimeware toolkit, SpyEye could be a future contender for king of the crimeware toolkits.

SpyEyeLogo.JPG

The SpyEye toolkit is similar to Zeus in a lot of ways. It contains a builder module for creating the Trojan bot executable with config file and a Web control panel for command and control (C&C) of a bot net. Some of the advertised features online are:

- Formgrabber (Keylogger)
- Autofill credit card modules
- Daily email backup
- Encrypted config file

- Ftp protocol grabber
- Pop3 grabber
- Http basic access authorization grabber
- Zeus killer

New revisions of SpyEye, with additional features, are being released on a regular basis. The latest version (V1.0.7) contains an interesting new feature called “Kill Zeus” that we have yet to substantiate. SpyEye hooks the same Wininet API (Wininet.dll) HttpSendRequestA as used by Zeus for communications. If a compromised system infected with SpyEye was also infected with Zeus, this in turn would allow SpyEye to grab and report on http requests sent to the Zeus C&C server.

ZeusCommReport.JPG

An example of Zeus C&C server report taken from underground forum

The new Kill Zeus feature is optional during the Trojan build process, but it supposedly goes as far as allowing you to delete Zeus from an infected system—meaning only SpyEye should remain running on the compromised system. If the use of SpyEye takes off, it could dent Zeus bot herds and lead to retaliation from the creators of the Zeus crimeware toolkit. This, in turn, could lead to another bot war such as we have seen in the past with Beagle, Netsky, and Mydoom.

SpyEyeBuilder.JPG

An example of the SpyEye Trojan builder control panel

Another feature of SpyEye is the ability to load additional threats onto infected SpyEye systems, by country, using the SpyEye control panel GUI as shown below:

SpyEyeCountryPanel.JPG

Symantec will continue to monitor the progression of this toolkit and update detection as necessary. Remember to keep your definitions up to date to ensure you have the best protection against new threats.

Special thanks to Mario Ballano Barcena for his analysis.

Statistics

0 Favorited

0 Views

0 Files

0 Shares

0 Downloads

Tags and Keywords

Related Entries and Links

No Related Resource entered.