October 6, 2009, 1:06 PM

Malware Economy is Thriving

TORONTO -- The legitimate economy may be in rough shape right now, but the same cannot be said for the underground economy. Malware authors and botmasters are thriving, experts say, with some online criminals charging as much as $3,500 for their attack toolkits.

But don't be intimidated by the high price point. That's a premium product. More basic exploit kits can be had for as little as $100. But even at that price, the attackers are doing just fine, thank you.

"The bad guys are doing really great," said Roy Firestein of Digital Defence, speaking in a session on modern crimeware toolkits at the SecTor 2009 conference here. "How are the good guys doing? Not so good."

Firestein has been researching a variety of malware families, exploit toolkits and botnets and found a wide range of options, pricing schemes and capabilities. At the top of the heap sit kits such as the Adrenalin botnet kit, which sells for $3,500 right now and can be customized to suit the needs of even the most demanding attacker. Adrenalin includes 24x7 technical support, built-in exploits, the ability to steal digital certificates and the option to encrypt the stolen data.

Following the lead of other recent malware packages, Adrenalin also will take the extra step of removing other bots and attack toolkits from infected machines.

Several of the packages that Firestein described also include comprehensive statistical engines that report the number of each kind of browser that's been infected, how many machines total have been attacked and can even create graphs.

Firestein spent quite a bit of time on the notorious Zeus Trojan, which has been busily creating a massive botnet in the last few months, a network that some estimates have put in the millions. Zeus is an all-in-one package that gives buyer's the ability to infect a large volume of machines as conveniently as possible.

"It's the infection point and the command and control panel all in one," Firestein said. "You put it up and just start infecting people. You put up some iFrames on other sites and start linking to them and you're set."

View the forum thread.

About Digital Underground

Veteran security reporter Dennis Fisher writes the Digital Underground blog on Threatpost. He previously served as executive editor of the Security Media Group at TechTarget and news editor of eWeek magazine and has been covering security for nearly 10 years. On Digital Underground, Dennis delivers insightful analysis, fast-breaking industry news and in-depth features.
Contact Dennis

THU, 10/08/2009 - 07:59

ThreatPost tweeted "Operation 'Phish Phry' Nets 100 Cyber Criminals | http://bit.ly/Nrhzu..." 7:59am #

ThreatPost tweeted "Citing Cybercrime, FBI Director Doesn't Bank Online | http://bit.ly/1famAa..." 7:58am #

WED, 10/07/2009 - 10:38

ThreatPost was mentioned - "Twitter Mention - rex_plantado: RT @threatpost Researcher Banished for Showing How to Hack PayPal | http://bit.ly/13UYmm..." 10:38am #

ThreatPost was mentioned - "Twitter Mention - jespinhara: RT @threatpost Researcher Banished for Showing How to Hack PayPal | http://bit.ly/13UYmm..." 8:56am #

ThreatPost was mentioned - "Twitter Mention - devilok: Researcher Banished for Showing How to Hack PayPal | http://bit.ly/13UYmm (via @threatpost)..." 8:46am #

more

Stay Connected

Facebook Twitter LinkedIn RSS

Feeds

Ones and Zeros Digital Underground Punditry Overflow Watchlist Hearsay Cybersecurity Black Hat Briefings VB Conference 2009