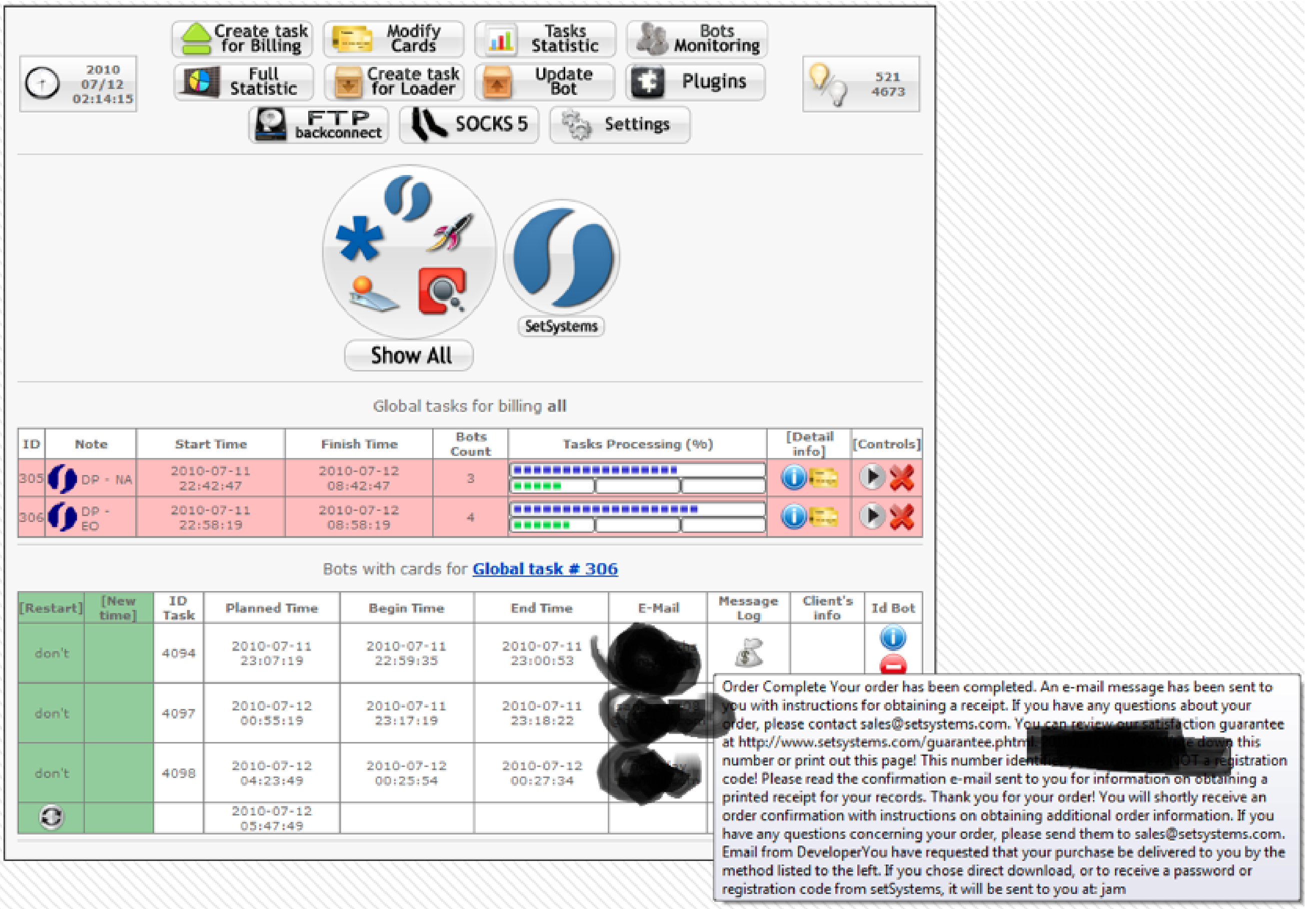
SpyEye Botnet’s Bogus Billing Feature

krebsonsecurity.com/2010/09/spyeye-botnets-bogus-billing-feature/



Global tasks for billing **all**

ID	Note	Start Time	Finish Time	Bots Count	Tasks Processing (%)	[Detail info]	[Controls]
305	DP - NA	2010-07-11 22:42:47	2010-07-12 08:42:47	3			
306	DP - EO	2010-07-11 22:58:19	2010-07-12 08:58:19	4			

Bots with cards for Global task # 306

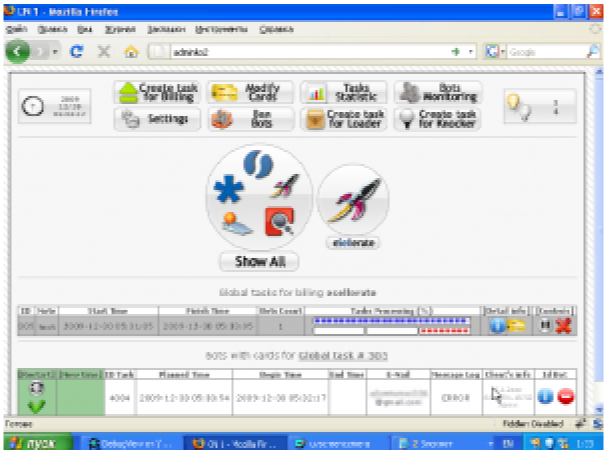
[Restart]	[New time]	ID Task	Planned Time	Begin Time	End Time	E-Mail	Message Log	Client's info	Id Bot
don't		4094	2010-07-11 23:07:19	2010-07-11 22:59:35	2010-07-11 23:00:53	[redacted]			
don't		4097	2010-07-12 00:55:19	2010-07-11 23:17:19	2010-07-11 23:18:22	[redacted]			
don't		4098	2010-07-12 04:23:49	2010-07-12 00:25:54	2010-07-12 00:27:34	[redacted]			
			2010-07-12 05:47:49						

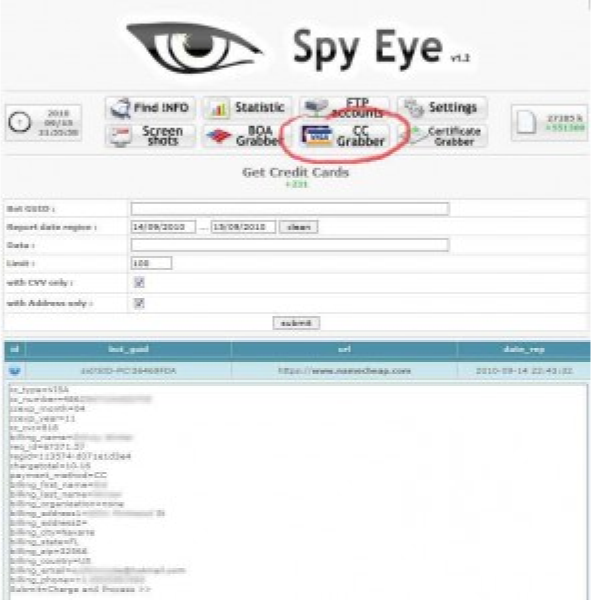
Order Complete Your order has been completed. An e-mail message has been sent to you with instructions for obtaining a receipt. If you have any questions about your order, please contact sales@setsystems.com. You can review our satisfaction guarantee at http://www.setsystems.com/guarantee.phtml. [redacted] this number or print out this page! This number ident[redacted] a registration code! Please read the confirmation e-mail sent to you for information on obtaining a printed receipt for your records. Thank you for your order! You will shortly receive an order confirmation with instructions on obtaining additional order information. If you have any questions concerning your order, please send them to sales@setsystems.com. Email from DeveloperYou have requested that your purchase be delivered to you by the method listed to the left. If you chose direct download, or to receive a password or registration code from setSystems, it will be sent to you at: jam

Miscreants who control large groupings of hacked PCs or “botnets” are always looking for ways to better monetize their crime machines, and competition among rival bot developers is leading to devious innovations. The **SpyEye** botnet kit, for example, now not only allows botnet owners to automate the extraction of credit card and other financial data from infected systems, but it also can be configured to use those credentials to generate bogus sales at online stores set up by the botmaster.

As I noted in a post in April, SpyEye is a software package that promises to make running a botnet a point-and-click exercise. A unique component of SpyEye is a feature called “billinghammer,” which automates the purchase of worthless or copycat software using credit card data stolen from victims of the botnet.

The SpyEye author explained this feature in detail on several hacking forums where his kit is sold, even including a video that walks customers through the process of setting it up. Basically, the scam works like this: The botmaster acquires some freeware utility or legitimate program, renames it, claims it as his own and places it up for sale at one of several pre-selected software sales and distribution platforms, including ClickBank, FastSpring, eSellerate, SetSystems, or Shareit. The botmaster then logs in to his SpyEye control panel (picture above), feeds it a list of credit card numbers and corresponding cardholder data, after which SpyEye opens an Internet Explorer Window and — at user-defined intervals — starts auto-filling the proper fields at the botmaster's online store and making purchases.





The billinghammer module also is set up to evade anti-fraud controls at the online software stores, by funneling each transaction through a SpyEye-infected system whose Internet address traces back to a geographic location that approximates the cardholder's street addresss.

In the video that shows how to use this portion of the bot kit, it appears that SpyEye customers have the option either to make sales at their own stores, or to use some that are apparently set up by the author of the bot kit himself.

In an e-mail to KrebsOnSecurity.com, FastSpring's chief customer service officer Ken White said: "We understand what this system tries to do, and how the bad guys attempt to use it to convert stolen cards into cash. We haven't yet been exploited successfully and believe we have a good system in place to prevent it."

All other software sales and distribution systems coded into the SpyEye bot kit are entities operated by **Digital River**, which did not respond to repeated requests for comment. It's not clear how many — if any — SpyEye customers are using the billinghammer plug-in. But assuming that there are some scammers out there abusing these services through SpyEye, it seems that it would be a great way to catch botmasters in the act. After all, the check or wire transfer for any bogus software sales has to be sent somewhere.