



THE MALWARE REPORT

McColo Shutdown: Will Spam Levels Decrease?

Participants

Matt Grant, host

Randy Abrams, director of technical education, ESET LLC

The Malware Report Transcript

Title: McColo Shutdown: Will Spam Levels Decrease?

Episode: 100

Location: http://www.eset.com/podcasts/112408_ESET_McColo%201.mp3

December 18, 2008

[Begin recorded material]

Matt Grant: Hi, this is Matt Grant; you're listening to The Malware Report with Randy Abrams. Hi Randy, thanks for being here.

Randy Abrams: Hey Matt, great to be back; thanks.

Matt Grant: A few weeks ago a notorious ISP called McColo was shutdown, and the volume of spam in circulation fell by as much as two-thirds after the upstream providers pulled the plug. I was hoping you could tell us a little bit more about the impact that this is having on the level of spam?

Randy Abrams: Unfortunately, long term there's not a lot of impact. There's a lot of corruption in the ISP space and while the upstream from McColo shut them down, which was a great thing, there are plenty of ISP's throughout the world that are willing to pick up the traffic. McColo will end up segmenting and using a variety of ISP's, which is bad, but

there is a lot of hope because McColo is the second in a few months that has been shut down. The trend that we're seeing that's really important is iCan, which is the Internet Registry Organization, and ISP's are becoming more responsible. It's going to make it harder for the McColo's, but you have to understand that this is crime. Crime has not been eliminated by technology in the history of the world. For thousands of years we've had technologies to combat crime, and the good guys do their best to combat it but there are myriad of ways for criminals to act. It's really good news that the upstream for McColo was shutdown. However, they had a Swiss Internet provider that they had a back-up arrangement for, and it took several hours after they transitioned to that Swiss Internet provider to shut them down again. During that time, they transitioned many of the bots, which were the infected computers, to report to new servers so they could continue their badness.

Matt Grant:

I'm sure as you know McColo hosted the command and control infrastructure for some of the world's most prolific spam botnets. IT systems were also used to peddle porn and support credit-card fraud, and other cybercrime activities. How were they able to find them and shut them down?

Randy Abrams:

It was through the work of a lot of dedicated professionals; working volunteer. These people have full-time jobs with IT companies. People like Paul Ferguson from Trend Micro, I know Trend Micro is a competitor of ESET, but you have to give credit where it's due. Paul and many other professionals dedicate their own time to try and get rid of the Internet trash. I take my hat off to them, they did a fantastic job. These people work continuously to help shut these guys down, and work continuously with iCan to improve the policies so that when a good guy reports a bad guy they can get things shut down. We're a

long way from having it a perfect system, but things are actually getting better and that's encouraging.

Matt Grant: Absolutely, is this an example that we are getting tougher on these rogue ISP's?

Randy Abrams: It's definitely an example that we're making progress in being able to fight the grime. It's really a huge step; I can't understate the importance of it. It's not going to make the problem go away, but we're doing a better job now; a much better job than even a year ago.

Matt Grant: With this shutdown being recent, obviously now we're seeing the volume of spam in circulation less, but do you think that's going to increase pretty quickly here?

Randy Abrams: Definitely, it will increase pretty quickly. We're a long ways from shutting down all the avenues. There are still many places in the world that do not have proper legislation to prevent this kind of thing from happening. It's going to take years before we shut down all the avenues, and we'll never shut them all down, there will always be holes. Crime happened for years, for millennium, there will always be opportunities. But this is a really big step in making things harder, and this year we've really seen drastic improvements in Internet service providers stepping up to the plate and saying, "No, this is not acceptable behavior." I'm quite hopeful. I don't expect it to disappear; I expect spam volumes to increase, because fundamentally, the one thing that will shut down spam is consumers not buying from spam.

Matt Grant: Do you think we should feel more secure after this shutdown or would that just be a false sense of security?

Randy Abrams: That would be a false sense of security, there are so many avenues that the bad guys can come after you through. You have to be on guard, don't feel more secure. Take pleasure that one of the big bad guys has been hampered.

Matt Grant: You're absolutely right, and I think that's a key statement. It comes down to user education, and once they can stop getting money from the users, then obviously we'll see spam reduce to a lot less. Well Randy, I certainly appreciate you taking the time to chat with us on this topic. This has been Matt Grant; you're listening to The Malware Report with Randy Abrams.

[End of recorded material]