



**infectionvectors.com**  
**September 2004**

## Introduction

An infectionvectors.com mailbox was established and unpublished (except in a page on the site) in an attempt to unscientifically judge how long it takes to get onto the spam lists by way of spam spider.

Spiders are tools that crawl the web (hence the name) looking for specific content. Search engines may use them to grab and index all sorts of content, whereas others may use them for very specific items. Spammers use spiders to harvest email addresses from the Web. Many believe that publishing an email address on an Internet site will eventually lead to its inclusion in a spam target list (one story on how it happens and how to protect accounts: <http://www.alistapart.com/articles/spam/>).

The infectionvectors.com email account did not receive any mail until 2 weeks after its creation. The first two pieces of mail were a scam letter and a worm, very telling of the state of the Internet: profits are to be had in mass mailings, both securing the anonymous relays and selling products/scamming. The details of each message are below, although the interest for this site and most readers is with the virus code.

## Message 1: I Need Your Help

The Nigerian email scam has taken a number of forms and is likely quite boring to anyone reading this report. If not, a search for the topic will turn up more than enough samples and stories to round out this description. The letter basically wants the reader to begin dialogue concerning a large sum of money (generally left in financial limbo because of the death of someone very important). At some point, the sender asks for monetary help to facilitate the “transfer” of funds. Considering the press these scams have received, it seemed like an appropriate first message to the account.

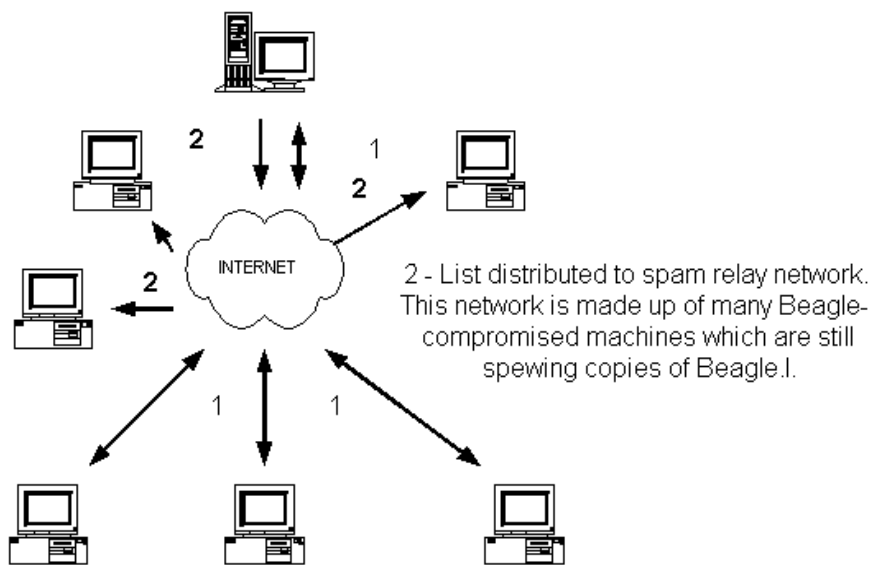
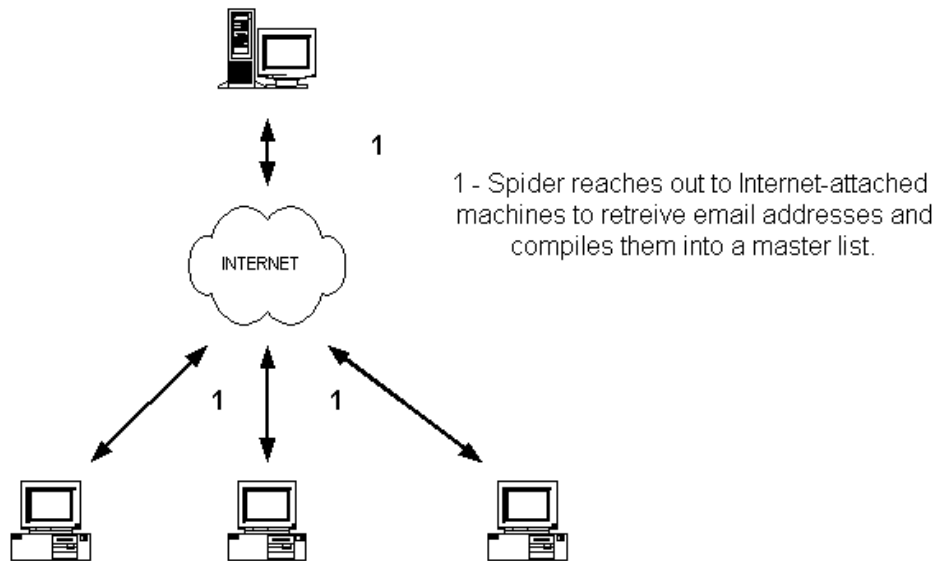
The fact that this is a big business may be surprising to many readers. However, someone paid for the spider and/or the list of addresses that it harvested. In addition, the scam is generating a lot of income, and has been around since at least the 1980s. There are some reports that these scams are the 2<sup>nd</sup> or 3<sup>rd</sup> largest pieces of Nigeria’s GNP, although that seems a little difficult to verify. Either way, there’s money in scamming, if evidenced only by the fact that it takes money to distribute the scam.

In the next section, the results of using mass mailers to create spam relays is considered in light of one of the most successful, the Beagle worm.

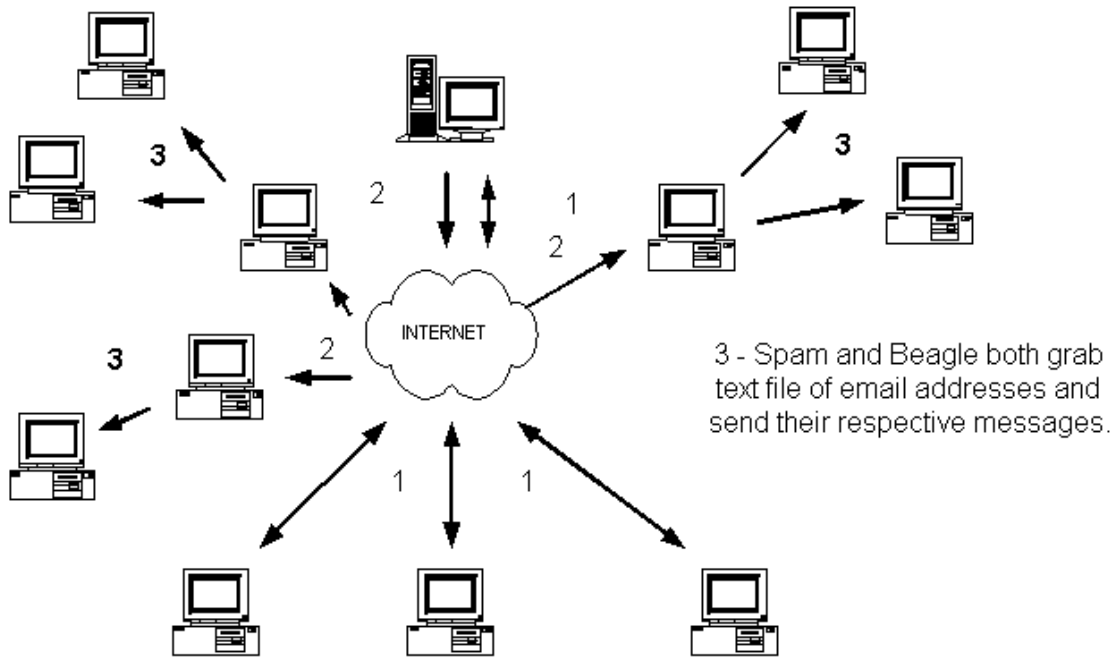
Message 2: Barking Beagle

The second message was an email generated by Beagle.I (released March 1, 2004). The email was surprising as the worm had long since seen its peak back in the spring of 2004 and the message was received in September. The interesting part of the story is the email's origin: why would an old email worm appear in a fresh inbox so quickly unless the spam/worm writer link was very tight?

The most likely scenario is that the list created by the spider was pushed out to the various email relays used by spammers. That's how the list actually begins to justify its costs, by going into action and sending profit-generating messages.



The final diagram shows the possible exponential growth of the virus once the spider's list has been delivered to the email relays. These relays are often Beagle-compromised machines, which still have the worm running. Once they are fed a new list of email addresses, it is entirely possible that the worm will harvest these targets and send out mail of its own.



Certainly there are other possibilities here. The email may be a coincidence; someone could have been poking around and discovered the email address in the HTML code for the site, and also have a 6-month-old virus. The virus-infected machine may belong to someone who purchased the spider's list. Possibly the machine that has the spider is infected with Beagle.I. All are possible, however, they appear less likely than the scenario presented above.

If the virus has been running on a machine that was used to complete high-end processing such as a web crawler, it seems likely the owner would know about it. The worm would degrade the performance of the server greatly, cutting into profits. Also, the spider server would have been churning out Beagle.I messages for months, making the worm much more successful than it has been. [The worm appears in Trend Micro's Top Ten only in South America at the time of this writing, and it is lumped together with 5 other variants to get that score.] It is likely that the generator of the list would have a reason to use the list as well, if only to attempt to compromise more machines as relays. However, the servers associated with Beagle.I have been taken out of circulation themselves, making the intentional use of this particular code unlikely.

Although there is no way to tell for certain how the Beagle worm and scam message arrived at the same new box on the same day, there are things to learn from the occurrence. The speed with which targets and new relays can be assimilated is not a barrier to scammers/spammers/worm writers. The economy of scale is rather small as well; a spider could be constructed with tools such as wget in a pinch. Patient spammers can obtain a great number of targets; those with money to spend can obtain the list faster. The link between the spam industry and worm writers has been explored before, this provides additional evidence for the link and shows ways they may be working together and not even realizing it.

### References

Nigerian Mail Scheme Around for Decades

<http://www.wired.com/news/culture/0,1284,53818,00.html>

People Taken, Killed in Nigerian Email Scams

[http://www.wired.com/news/culture/0,1284,53818-2,00.html?tw=wn\\_story\\_page\\_next1](http://www.wired.com/news/culture/0,1284,53818-2,00.html?tw=wn_story_page_next1)

Copyright © 2004 infectionvectors.com. All rights reserved.