Where have the worms and viruses gone?—new trends in malware

E. Eugene Schultz, Ph.D., CISSP, CISM
High Tower Software

Although many new worms and viruses surface every week, they are becoming less widespread than those in previous years. In contrast, bots and botnets are becoming more prolific and troublesome; botnets consisting of hundreds of thousands of bots or even more are not uncommon. Bot writers and botnet operators have numerous motives for engaging in their sordid activity, but the desire to make money has become by far the chief motivator. Meanwhile, the nature of current worms and viruses is also changing considerably—a growing number of them uses instant messaging (IM) to replicate, and worms and viruses that target handheld computing devices are also becoming more prevalent. Bots and botnets pose very elevated levels of risk, risk that needs to be controlled through a variety of security countermeasures.

Introduction

Worms and viruses are have for many decades been part of the proverbial IT landscape. Both are self-reproducing programs that infect systems, although the reproduction mechanisms for each are somewhat different. A worm is self-reproducing code that spreads independently of human intervention, whereas a virus is self-reproducing code that requires human intervention to replicate (SCHU01). Many worms and viruses that surface are in reality hybrids—a cross between worms and viruses. They might, for example, have two means of reproduction—one that is independent of and another that depends on human intervention. Self-reproducing malware (as opposed to malware that cannot replicate itself) constitutes a special threat in that it has the ability to spread prolifically before anti-virus software vendors become aware of it and identify and include its signature in their software. Worms and viruses can thus cause a very number large number of infections before anti-virus software can detect and eradicate them.

Not too long ago two messages, each with a suspicious attachment, arrived in my email inbox. Having learned a long time ago that opening any unexpected attachments is extremely unwise, I refrained from opening them, even though they appeared to be sent by colleagues at work with whom I constantly interact. My suspicion was quickly justified; I Googled for the names of the attachments, one of which was richarde.zip, the other of which was humphrie.zip, and discovered that a new worm, Beagle.CQ, created attachments with such names. I quickly alerted the system administrator that a new worm appeared to have gotten through both the virus wall and mail server before the virus signatures in both could be updated (something that lamentably is an all-too-common occurrence in IT settings). Fortunately, this new worm never infected any machines in the local network.

New worms and viruses are found and identified all the time, yet this was the first one that I have encountered in a real life setting in well over one year. Checking Web sites such as Symantec's site (http://www.symantec.com/avcenter/global/index.html) or any other anti-virus software vendor's virus alert site will quickly dispel any notion that worms and viruses are extinct—a very large number of them continue to surface every week. Today's worms and viruses are, however, not anywhere nearly as prolific as many worms and viruses that have surfaced before 2004. Symantec, for example, has estimated that the MSBlaster worm and its many variants infected over one million PCs in 2003 (SYMA03). In 2001 Code Red worm infected nearly 360,000 computing systems in less than 14 hours (MOOR01). Even the less prolific (but possibly the most disruptive over a short time span ever) Slammer worm managed to infect approximately 75,000 systems in 10 hours in 2003 (MOOR03). In contrast, even though a mutant of the Sober worm and another of the Beagle worm spread fairly rapidly within the last year, their spread did not by any stretch of the imagination approach that of MSBlaster, Code Red, or Slammer.

Bots and Botnets: changes in the nature of malware

As Bradbury points out, the trend in malware has shifted dramatically from worms and viruses towards bots and botnets in the last few years (BRAD06). A bot is a program used to perform a certain function. In the context of this paper, a bot (see Note 1) is defined as a malicious program that is under the control of a master program used by a perpetrator to achieve a variety of sordid goals. A botnet consists of multiple bots that respond to a central source of control. Bots are not self-reproducing, although a worm or virus can install bots in computing systems that it has compromised. Botnets are much more prevalent than people realize. For example, three Dutch perpetrators built a botnet that may have consisted of up to one and a half million bots (SAND05), in all likelihood the largest botnet identified to date. Neither bots nor botnets are new, however; both originally emerged in connection with distributed denial of service (DDoS) attacks that started in the late 1990s.

Original reasons for creating botnets

Malware writers originally built botnets for several reasons, including:

- Knocking others who were competing with them for limited chat channel bandwidth off of the channels—this was in fact the original reason for writing and deploying bots.

- Crashing multitudes of hosts or rendering networks unusable mainly to prove that it could be done—a type of "proof of concept" exercise.
- Gaining recognition among peers—the more spectacular the functionality of bots and the larger botnet, the higher in esteem within the Black Hat community the malware writer tended to be held.

Botnets for sale

Malware writers soon realized that there was potential for financial gain in connection with using botnets. Perpetrators thus started to build botnets and then sell them to "hacker wannabes" who were incapable of building their own botnets or who were too impatient to do so. Selling botnets in this manner is a practice that is very much alive and well today.

Botnets and extortion attempts

Perpetrators also realized that more could be done to make money from botnets than selling them; botnets could be directed against websites as well as against servers such as DNS and mail servers, causing them to be unreachable, or if not, at least extremely slow in responding to requests. The practice of attempting to extort money from organizations and individuals in return for leaving their Web sites and other servers alone started not long afterwards (SCHU04). The use of botnets in connection with extortion attempts has not by any means subsided today. Lamentably, operators of online betting Web sites and other types of sites targeted by extortionists often pay sums of money every month to avoid having extortionists launch DDoS attempts against them (LEYD05). Worse yet, once a payment to an extortionist is made, things often only get worse. Evidence shows that those who pay extortionists are likely to be targeted in further extortion attempts (PAPP05).

Botnets and spamming operations

Malware writers also discovered that they could profit from botnets by using them to send spam on behalf of individuals and organizations who were incapable of engaging in spamming operations or who were unwilling to send spam from their own computing systems for fear of being caught and punished. The perpetrators starting sending spam from a large number of bot-infected hosts, thereby not only making tracing the origin of spam messages for the most part pointless, but also helping spammers get around spam filters. In one case Anthony Scott Clark of Oregon created a botnet that consisted of about 20,000 bot-infected hosts and then used the botnet to send massive quantities of spam in return for financial compensation (SPAM05). Clark is serving a sentence for his illegal activities.

Botnets and adware

Another way in which botnets are being used for financial gain is delivering unsolicited advertising. A number of malware writers have written and then installed bots that download and display adware on the systems on which they run. These perpetrators are paid by the organizations on behalf of which the adware runs. For instance, Christopher Maxwell of California is now serving a sentence after he pleaded guilty to charges of committing computer fraud and deliberately damaging a protected computer by attempting to install adware on a large number of vulnerable computing systems. Maxwell's activities, which severely disrupted the network of Northwest Hospital and Medical Center in Seattle and US Department of Defense (DoD) computing systems, reportedly earned Maxwell $100,000 (SANJ06).

Botnets and fraudulent advertising charges

Botnets are even being used to swindle advertisers who pay for Google Adword, an advertising system in which advertisers are charged for each click on each advertiser's Web site (LEYD06). A large proportion of the money that Google receives from advertisers is passed on to publishers who set up banners for the advertisers. Some publishers have been working in connection with botnet owners to illegally increase the amount of money that the publishers receive by having the botnet owners program their bots to click on the advertiser's Web sites, thereby increasing the revenue the publishers receive from Google. Some of this revenue in turn goes back to the botnet owners. In one instance, bots in a small botnet were clicking on advertisers' sites 15 times each day. The low number of clicks was deliberate; it helped masquerade the bots' activity (LEYD06).

The need for stealth: a critical consideration

A final consideration in analyzing the shift from worms and viruses to bots and botnets is perpetrators' desire to be clandestine. Releasing a rapidly proliferating worm or virus to do anything, creating a massive botnet included, is counterproductive in that doing so will invariably attract a considerable amount of attention, attention that is likely to trigger intervention on the part of technical staff and intrusion detection systems (as well as possibly by automated measures initiated by intrusion prevention systems). Intervention measures are in turn likely to result in discovering and eradicating the worm or virus in systems that have been infected. Anyone who wants to profit from using malware needs to strongly consider using methods that minimize the probability of detecting activity related to its installation and behavior (BRAD06).

Other possible reasons that worms and viruses have become less prolific

The trend towards greater use of bots and botnets as opposed to worms and viruses by computer criminals is difficult to dispute. Nevertheless, the fact that worms and viruses have become less prolific over the last several years is in all likelihood not exclusively due to worms and viruses being supplanted by bots and botnets. This section proposes and discusses five hypotheses that potentially account for the reduction in prolific worms and viruses.

Hypothesis 1: More organizations and individuals are deploying antivirus measures.

Web sites that disseminate information concerning patterns of Internet usage such as http://www.connections-usa.com/employee-internet-usage.html almost invariably claim that nearly every organization (see Note 2) now deploys anti-virus measures such as host-based AV software, virus walls, and/or mail server-based AV software), something that was not true only a few years ago. Provided that these organizations ensure that anti-virus measures are regularly updated, the ability of worms and viruses to spread should be substantially reduced. This may to some degree be true, but available statistics suggest that the great reduction in the number of extremely successful worms and viruses and worms over the last few years cannot be linked to a massive reduction in the number of worm and virus infections per se. A recent FBI survey, for example, showed that 83.7 percent of organizations that responded to the survey had experienced worm and virus infections over the last year and that worms and viruses were the major cause of incident-related financial loss (FBI05). Similarly, McAfee's Web site (see http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=99040) provides statistics that indicate that worms and viruses are still causing fairly large numbers of infections. If a radical increase in the number of organizations and individuals deploying and regularly updating anti-virus tools were responsible for the reduction in widely success worms and viruses, the number of worm and virus infections should in general be greatly reduced. Anti-virus software, after all, does not discriminate between "prolific," "potentially prolific," and "regular" worms and viruses. Available statistics, however, show otherwise; worms and viruses continue to infect systems at a sufficiently high rate that widespread deployment of anti-virus tools cannot in and of itself explain the recent reduction in the number of highly successful worms and viruses.

Hypothesis 2: There are now substantially fewer vulnerabilities to exploit.

Worms (but not viruses) generally work by exploiting vulnerabilities in operating systems and applications. In many ways worm attacks can in fact be viewed as "programmed hacker attacks." Windows operating systems have traditionally had a large number of vulnerabilities, vulnerabilities that worms such as Nimda and Sircam have exploited. The overwhelming preponderance of worm infections over the years has in fact been in PCs that run Windows operating systems. In 2002 Microsoft, however, initiated its Trusted Computing Initiative (TCI) in which among other things this software giant required that its software be developed in accordance with principles of secure code development. TCI appears to have made a reasonable amount of difference, as evidenced by the fact that so far the number of identified vulnerabilities in Windows Server 2003 (a product developed in accordance with the TCI) is considerably less than in Windows 2000 three years after the later was released. At the same time, however, there have nevertheless been many vulnerabilities in Windows Server 2003, Exchange Server 2003, Office, and other Microsoft products, something that casts doubt on the hypothesis that there are fewer worms because there are now substantially fewer vulnerabilities in Windows products to exploit.

Hypothesis 3: Boredom has demotivated worm and virus writers.

Another possibility is that worm and virus writers have become bored with writing worms and viruses and have moved on to working on developing other types of malware. The first virus, after all, surfaced over 25 years ago (Note 3); the first worm surfaced shortly afterwards. Most worms and viruses are not very original; each mutation is usually a somewhat (often minimally) changed version of a previous one. Sooner or later it would seem logical that challenges associated with worm and virus writing would diminish and that worm and virus writers would move on to something else. The fact that very few talks at so called "hacker conferences" cover worm and virus writing any more provides at least some support for this hypothesis, although there is really little if any direct evidence to supports it.

Hypothesis 4: Worm and virus writers now fear repercussions.

Potential repercussions of writing and releasing worm or virus code has potentially serious criminal ramifications in numerous countries around the world. Although for many years worm and virus writers continued their activity with impunity, a considerable amount of legislation that prohibits writing and releasing malware such as worms and viruses has gone into effect since then. Equally importantly, law enforcement in many countries appears to be doing considerably better in identifying worm and virus authors and bringing them to justice. Perhaps not coincidentally, no prolific worm or virus has surfaced since the arrests and sentencing of confessed worm writers Sven Jaschan of Germany and Jeffrey Lee Parson of the US. Although this hypothesis is viable, it is not likely that fear of consequences is by itself accountable for the recent disappearance of prolific worms and viruses, however.

Hypothesis 5: Many of today's worms and viruses target devices in which massive spreading is far less likely.

Today's generation of worms and viruses does not exclusively attack conventional computing systems. Some worms and viruses attack mobile phones, for example; others attack Personal Data Assistants (PDAs). Both must be turned on if they are to become infected, whereas many conventional computing systems are on continuously. Additionally, numerous devices such as PDAs and BlackBerry devices have limited ranges, making it less likely that another such device will infect them. Finally, whereas conventional computing systems have complete operating systems that worms and viruses can potentially take advantage of in many ways, mobile phones and handheld devices do not. Although tenable, this hypothesis, like the others, cannot in and of itself explain the fact that widespread worms and viruses have not surfaced lately.

Of the above hypotheses, all but hypothesis 2 are credible. However, any plausibility of these hypotheses should not overshadow the main point—that the major motivation in malware writers' shift from worms and viruses to bots and botnets has been the desire to make money. There may also be other reasons for this shift, but the others are all secondary.

Changes in current worms and viruses

The rapid growth of bots and botnets constitutes a significant trend in malware, but as mentioned previously, this is not by any means to imply that worms and viruses have gone away. The functionality and mechanisms of many current worms and viruses have changed considerably, however, as explained in the following section.

A major change in recent worms and viruses is in the way they spread—instant messaging (IM) is being used increasingly as the distribution channel of many new worms and viruses. The IM.Myspace04.AIM worm, for example, sets up what is ostensibly a chat session with users by sending a bogus IM message and then responding to any reply to that message. Users who click on a URL in the messages that this worm sends infect their systems. IM.Myspace04.AIM then reads the AIM buddy list in each infected system and sends messages to any addresses it has found. Additionally, this worm attempts to stop security software and install a backdoor Trojan on each infected computer. Another example is the Sdbot-ADD worm, which also spreads using AOL Instant Messenger (AIM). After infecting a system, it installs a rootkit, several types of adware and spyware, and additional malicious programs, some of which try to halt security programs. Aimdes.E is a final example of an IM worm; it spreads by appearing to be an electronic greeting card.

Another change in current worms and viruses is that they are being used increasingly to create botnets. For example, both the previously discussed IM.Myspace04.AIM and Sdbot-ADD worms attempt to install bots in systems that they infect. Installing botnets may in fact be the major motive for writing IM worms and viruses. Recent versions of the Beagle worm also attempt to install bots. As mentioned previously, however, using worms and viruses to install bots is a less than optimal method because worm and virus outbreaks tend to be so noticeable.

Mobile phone viruses are also on the rise. Examples include the Cabir worm family and The CommWarrior.A worm. The Cabir worms spread using a specially formatted Symbian Installation System (SIS) file designed to look like a security management utility. Infected phones scan for other vulnerable mobile phones using a short-range Bluetooth wireless connection and send a worm-infected file to any such phones that have been discovered. These worms can infect only phones that run the Bluetooth wireless feature in “discoverable mode,” a mode of operation that allows new connections to be created. Additionally, the Cabir worms can infect a mobile phone only if users press a key to suppress a warning concerning the risk of installing software with an unknown origin and then choose OK to an additional one that queries whether the file that has been downloaded should be installed.

The CommWarrior.A worm infects Symbian Series 60 mobile phones, reproducing using the Mobile Messaging Service (MMS) that allows cellular phone users to transmit multimedia data such as photos to other cell phones. It locates phone numbers in the phone book of cell phones that it has infected and then sends MMS messages with attachments containing its code to these numbers. Messages are worded in a manner intended to deceive recipients into opening the attachments. Users who open a CommWarrior.A attachment cause their phones to be infected, causing this worm to send infected attachements in messages to phone numbers that it has found. This worm can also infect Bluetooth devices. Fortunately, CommWarrior.A has spread rather slowly among phone users and its impact has been minimal because eradicating a CommWarrior.A infection is fairly easy. Individuals whose cell phones are infected with this worm must simply press and hold the menu button on their mobile phones, select CommWarrior.A from the list of displayed applications, and then press the “C” (clear) button. File management tools can then find and delete any files that the worm has placed on the infected system.

Reconsidering malware-related Risk

Risks associated with damage, disruption and loss resulting from worm and virus infections is generally high. The risk that bots and botnets pose is in contrast generally even higher for several reasons:

- The risk due to botnets grows in proportion to the size of the botnet. The potential for all kinds of harm, especially the kind of harm that massive DDoS attacks produce, is generally higher for botnets consisting of a large number of bots within a network compared to the same number of worm- or virus-infected machines within the same network. The effects of worm and virus infections are usually limited to certain operating systems, normally to Windows machines, whereas bots can readily be programmed to disrupt entire networks consisting of many different operating systems and applications.
- Once a bot infects a machine within a network, whoever has control of the bot can now more easily launch attacks against other machines within the same network because that network’s “security perimeter” has been breached. Worms and viruses also breach security perimeters when they infect a machine within a network, but worms and viruses are generally not under the control of a perpetrator once they are launched.
- Bots are more insidious, as discussed earlier in this paper. Once installed in a computer, they are likely to remain undiscovered while they perform whatever dire function(s) they have been programmed to do.
- A growing proportion of bots now also incorporate keystroke logging functionality. By capturing every keystroke entered on a compromised system, those who can access the captured information can glean names, addresses, credit card numbers, Social Security numbers and the equivalent in countries outside the US, usernames and passwords for accounts, and other information that can be useful in identify theft and other

kinds of criminal activity. Bots with keystroke loggers can also be used to spy on individuals—to not merely record Web sites visited (as does conventional spyware), but also to glean the content of email messages, reports that are being written, and so on.

Control measures

There are no easy solutions to address the dramatic shift in risks that new trends in malware are causing. One might, for example, urge organizations and individuals to deploy frequently updated anti-virus tools, something that would do a considerable amount of good, but something that in and of itself cannot solve the entire problem. Anti-virus tools are generally superb for detecting worms and viruses, but they are not nearly as proficient in detecting the presence of a sizable proportion of bots. Integrity checking tools are usually another valuable but also non-comprehensive solution, as are firewalls, intrusion detection systems, intrusion prevention systems, and security event management tools. Even if organizations deploy all of these technology control solutions, they will still not have a complete solution to the problem, however, because the "people problem" would not be addressed. Users will always be the weak link; even if superb technology controls are in place, perpetrators are likely to be able to exploit human naïveté and trust to get malware installed where they want it unless suitable countermeasures are implemented. Countermeasures such as suitable information security policy provisions and procedures as well as training and awareness are thus additional necessities in the effort to suitably manage the ever-changing risks related to malware.

Conclusion

Perpetrators continue to develop and use various types of malware, but the likelihood of massively spreading worms and viruses is diminishing in comparison to the likelihood of massive bot infections. Only four years ago Staniford et al. predicted that an "uberworm," one that would virtually take over the Internet, would be created and released in the wild (STAN02). While this prediction generated a considerably amount of media attention as well as anxiety within IT circles, many skeptics, myself included, seriously doubted the wisdom of such a prediction. In "black hat" circles, new attacks are usually improved only to a point over time. Before an attack method can be optimized, attention generally shifts towards developing a different attack method. The same appears to be true in the malware arena. Writing worms and viruses that cause massive infections is apparently no longer a central focus; writing better bots and creating larger botnets is. The real challenge now is thus for organizations to adjust their control strategies to address the new risks that have surfaced as a result of this new trend in malware.

Notes

Note 1. "Bot" is short for "robot."

Note 2. Tired of paying for the massive amount of network traffic that worms and viruses typically generate, an increasing number of Internet Service Providers (ISPs) have in particular been much more aggressively combating worms and viruses in recent years.

Note 3. The first virus to exist "in the wild" is widely believed to be the Elk Clone virus, a virus that infected Apple II systems in 1980.

References

BRAD06 – Bradbury, D., The metamorphosis of malware writers. Computers and Security, 25, pp. 89-90, 2006.

FBI05 – 2005 FBI Computer Crime Survey. http://www.fbi.gov/page2/jan06/computer_crime_survey011806.htm

LEYD05 – Leyden, J., Victims coughing up to online extortionists, Web posting, October 6, 2005. http://www.theregister.co.uk/2005/10/06/ibm_botnet_vb/print.html

LEYD06 – Leyden, J., Botnet implicated in click fraud scam. Web posting, May 15, 2006. http://www.theregister.co.uk/2006/05/15/google_adword_scam/print.html

MOOR01 – Moore, D. & Shannon, C., The spread of the Code-Red Worm (CRv2). Web posting, 2001. www.caida.org/analysis/security/code-red/coderedv2_analysis.xml

MOOR03 – Moore, D., Paxson, V., Savage, S., Shannon, C., Stanirod, St., & Weaver, N., Inside the Slammer Worm. IEEE Security & Privacy, pp. 33–39, 2003.

PAPP05 – Pappalardo, D. & Messmer, E., Extortion via DDoS on the rise: Criminals are using the attacks to extort money from victimized companies. Web posting, 2005. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=101761&pageNumber=1

SAND05 – Sanders, T., Botnet operation controlled 1.5m PCs. Web posting, October 21, 2005.
http://www.vnunet.com/vnunet/news/2144375/botnet-operation-ruled-million

SANJ06 – San Jose Mercury Press, Man pleads guilty in computer attack. Web posting, May 5, 2006.http://www.mercurynews.com/mld/mercurynews/news/breaking_news/14508386.htm

SCHU01 – Schultz, E. & Shumway, R., Incident Response: A Strategic Guide for Handling Security Incidents. Indianapolis: New Riders, 2001.

SCHU04 – Schultz, E., Denial of service attacks. In Bidgoli, H. (Ed.), Encyclopedia of Internet Security, Volume I, pp. 424-433, 2004.

SPAM05 – Spam Daily News, Zombie master pleads guilty to eBay Internet attack. Web posting, December 29, 2005
http://www.spamdailynews.com/publish/master_pleads_guilty_to_eBay_Internet_attack.asp

STAN02 – Staniford, S., Paxton, V., & Weaver, N. How to own the Internet in your spare time. Proceedings of the 11th Security Symposium, Usenix Association, pp. 149-167, 2002.

SYMA03 – Symantec Corporation, "W32.Blaster.Worm," August 29, 2003. http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html