Viral Evolution
infectionvectors.com
December 2004

Overview

The virtual world of computer viruses often draws parallels out of the biological world. This is no surprise as the entire notion of "catching a virus" on one's PC is lifted directly from the medical realm of how germs migrate and propagate. This article examines one area of research from the biological sphere and how it may relate to Internet virus analysis: the evolution of viruses.[1]

It's Alive

In the December issue of "Scientific American," Luis Villarreal examines the debate concerning biological viruses and evolution.[2] He notes that although there is still much to be learned about how and whether these agents evolve, the impact they have had on the world around them (and in turn the evolution of other biological systems) should be analyzed. This article takes the same approach, introducing the possibility of "evolution" and computer viruses and how these virtual agents affect the world around them. Viruses are analyzed from two fronts: how they react to external forces and how they act as a catalyst for changing their environment, namely the Internet.

Does malware evolve? The use of the term "evolution" when describing a virus certainly elicits the notion that they adapt to changes on their own, something that most people would concede does not happen.[3] Although some polymorphic worms do change their appearance, this is constrained by routines coded into the program. Viruses, however, do change quite frequently; a worm may become much more potent (or destructive) based on the improvements made by its author. Virus coders learn from previous releases and computer technology improves, both of which provide an author with new tools from which to build malware. In this way, viruses are much more about innovation than evolution.

If the development of virus code (vice evolution) is taken for granted, there is still a prevalent use of the word "evolution" in research literature.[4] Through their creators, viruses do show constant improvements; changes in the computing and networking (Internetworking) world result in changes in worms. The use of the term evolution has been debated in the biological world as well. Although well beyond the scope of this article, a recent publication on the matter does make one point that may be significant to the electronic virus world as well: that whether or not viruses evolve themselves, they play a role in the evolution of things around them.

Prior to the Internet explosion, the April 1991 issue of "Virus Bulletin" briefly addressed the issue, specifying that something akin to evolution could be witnessed when examining a family of viruses, in cases where variants are spawned from an original program.[5] The analysis even draws parallels to Darwin's theory of Natural Selection, pointing out that some variants will simply die off while others will change in ways that make them much stronger. The remainder of this report examines the improvements seen in some well-known worms and how these worms have affected their world, specifically how the Internet has changed as a result of viruses.

A Worm's Life

Once released, attempted propagation is one trait that all viruses have in common. Whether the author coded routines to establish a proxy on a machine, destroy files, or steal passwords every virus has a means of spreading to other devices. That is the only thing that ensures the survival of a virus; sooner or later even the stealthiest virus will be discovered and added to antivirus signatures. To that end, some worms establish new propagation mechanisms for themselves over their lifecycles. Two especially successful worms, Lovgate and Beagle, are briefly discussed below.

Lovgate was originally released in February of 2003.[6] The mass mailer included 10 different email messages in an attempt to trick users into opening the attachment and to slow the spread of warning messages keyed off of specific email strings/subject lines. The worm also spread by attempting to log into Windows boxes on the victim's local subnet. Over the two months following its initial release, Lovgate saw improvements to the way it sent attachments (by using extensions other than EXE) and to its email wrapper. By the middle of 2004, however, Lovgate's changes were much more profound. In addition to simple file sharing and mass mail propagation, Lovgate's author added routines that allowed the worm to spread via the popular RPC DCOM exploit. The worm now sends a mass mailing as well as a response email to any message that arrives while it controls a machine. Lovgate also began infecting other executable files, a somewhat rare function in widespread modern viruses.

The evolution of the Beagle worm has been documented by previous reports and is certainly a prime example of an author learning from the successes of their code and the successes of those trying to stop it from spreading.[7] The use of ZIP files (generally allowed by corporate gateways), and then password protected ZIP files (which could not be scanned by antivirus software), and then password protected ZIP files without including a text password (only a picture file) shows a good deal of creativity and innovation, using the available technology to the best of one's ability, while crafting malware.

In most cases the new traits of viral code can be traced to one goal: survival. In this way studying the lifecycle of a virus is very much like studying the traditional view of evolution. As will be explored in the next section, this evolution in not confined to malware research.

Gravitational Pull

The force of virus code on the Internet (and computing in general) has been great. The development of new technology to defeat malware is just one area where this is true.

Worms have had a dramatic impact on the spread of spam, and vice versa.[8] Without the anonymous relays provided by worms like Beagle, spammers would likely have a more difficult time getting the volume of messages in front of users. Although SMTP is not especially secure in its basic form, the traceability of known spamming domains and subnets would make it easier for large mail gateway operators to dump unsolicited bulk email. Multiple worms have been tied to spamming, whether by stealing addresses, establishing mail relays for anonymous re-mailing, or both.

The use of a worm as a delivery mechanism for a spam relay is only one example of how viruses enable profitable Internet crime. Not only are spammers interested in ways to quickly compromise random boxes, but also criminals hoping to make money in extortion. Bot net applications such as Agobot can be used to initiate denial-of-service (DoS) attacks against those that refuse to pay "protection" money. In addition, unscrupulous companies can initiate attacks against their competitors, or hire Internet criminals to carry out the attacks for them.[9] The FBI posted an alert for such an offender, wanted for initiating DoS attacks against competitors' sites.[10]

Patch management as a whole (both in terms of security fixes and simple upgrade/maintenance) has been affected by the release of successful worms.[11] Discussions of the Slammer worm invariably turn to patching processes (or lack thereof).[12] It is these large-scale events (such as Slammer) that cost companies a great deal of time and money, resulting in the attention of the media and CEOs. That attention puts the focus on patch management.

Software development (especially operating system development) has shifted focus due in large part to viruses. When discussing the latest features of new operating systems and service packs, Microsoft leadership has identified malicious code, and specific viruses as the incidents that should help drive improvements to software security.[13] Most relevant is the description provided by Bill Gates in a letter to Microsoft customers. He describes the battle as a fundamental shift in thinking about security and virus protection:

"It is not a case of simply fixing a few vulnerabilities and moving on. Reducing the impact of viruses and worms to an acceptable level requires fundamentally new thinking about software quality, continuous improvement in tools and processes, and ongoing investments in resilient new security technologies designed to block malicious code before it can wreak havoc."[14]

Natural Selection

Whether or not the "evolution" argument is concluded, it is possible to see the best traits of successful worms being passed onto new pieces of malicious code. Although the true

origins of any particular trait are debatable, the table below shows a few popular worms and the trait that was picked up in later applications.[15]

Malcode	Trait	Noticeable Descendants
ILOVEYOU/"Anna Kournikova"	Mass Mail as a transport	Mass Mailers as a whole
Blaster	Modified P2P Propagation	Sasser
Benjamin	File swap transport (KaZaA)	Multiple worms
Nimda	"Blended threat" approach	Multiple/bot nets
Sircam	Multi-language messages	Sober/Zafi
Beagle	Deliver link to exploit/worm files	Bofra
Slammer	UDP transport	Witty

Within the family trees of many popular worms it is possible to see the "natural selection" of the most successful infection strategies. Mass mailers like Beagle will use the same basic infrastructure to compromise boxes, changing only the external shell (the subject lines, messages bodies, etc.).

This discussion raises a significant issue: are the changes simply required as technology changes or do viruses actually improve, getting stronger, faster, and more destructive? The answer is likely different for each virus and variant thereof, however, this question takes the debate out of a simple academic exercise and makes it relevant to virus detection and mitigation efforts. If a virus is altered simply to make it work on a new system (one example might be an offset changes so that a particular exploit works on multiple versions of Microsoft Windows, as in the case of the RPC DCOM exploits of 2003), then existing detection will probably continue to succeed. In the case of worms that change their composition in an effort to hide from scanners, however, detection must change as well. This is evidenced the use of generic detections for entire families of viruses, and the requirements to add new entries to signature files as viruses like Agobot change enough to prevent capture with existing malware definitions.

If the reader accepts that viruses evolve (at least in the sense that the constant development and innovation results in improved code), then it is not a stretch to also assume that virus writing evolves as well. The discipline as a whole may be advanced by particular variants of code that show improved ways of distributing programs. It is also advanced by more philosophical changes, such as the use of viruses to generate income and launch distributed attacks.

As the Internet is analyzed in a historical sense, it is important that the history and evolution of viruses is included. Results of their force can already be seen in the changes made to Internet-facing systems. It is largely because of the global awareness to vulnerabilities that they produce that holes are discovered and fixed in a timely manner. Both the future security and criminal use of the Internet will be due largely to the influence of viruses, whether the balance is more in favor of the former or latter is up to the developers of today.

References

1. The author is in no way attempting to validate evolution as a theory, either in the biological, virtual, or philosophical sense. In fact, the result of reading this article may well be to reject the notion that viruses improve at all. It is accepted as a given for the purposes of this exercise that "evolution" simply refers to the mutation and/or improvement of a system over time as a result of interacting with its surroundings.

2. "Are Viruses Alive?" Luis P. Villarreal. Scientific American. December 2004, pp 101-105. Villarreal notes in the introduction to his fascinating discussion on viruses, "Finally, however, scientists are beginning to appreciate viruses as fundamental players in the history of life." Maybe the same will be said for computer viruses, that they play a fundamental role in the history of the Internet.

3. Princeton's WordNet Definition of Evolution
http://www.cogsci.princeton.edu/cgi-bin/webwn?stage=1&word=evolution

4. Examples of the use of "evolution" in the virus research world include:

"Evolution of computer viruses: history of viruses Part I"
http://www.pandasoftware.com/about/press/viewnews.aspx?noticia=4942&entorno=&ver=&pagina=&producto=

"Survival of the Fittest – The Evolution of Computer Viruses and other forms of Malware" June 27, 2004.
http://www.cit.cornell.edu/computer/security/seminars-past/virus-june02/survival/

The author of this work uses the term "evolution" to describe the steady improvements in worms such as Beagle. "History of the Beagle Worm" Parts 1 and 2: http://www.securityfocus.com/guest/24228; http://www.securityfocus.com/guest/24231

"Malware Evolution: October Roundup" Pavel Zelensky November 2004.
http://www.viruslist.com/en/analysis?pubid=155435843

5. This three-paragraph analysis of viral evolution crystallizes the issues that form the basis for this report and provide a foundation for asking how viruses will be viewed in the history of the Internet.
"Virus Evolution" Technical Notes. Fridrik Skulason, Technical Editor, "Virus Bulletin." April 1991.
http://www.virusbtn.com/magazine/issues/pdf/1991/199104.pdf

6. Information on the Lovgate virus from Symantec Security Response:
http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.lovgate@mm.html

And infectionvectors:
http://www.infectionvectors.com/archive/lovgate.htm

7. Beagle information from Trend Micro:
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_BAGLE.AL

And a report by the author: "The Beagle Worm History Part 2"
http://downloads.securityfocus.com/library/beagle_lessons_2.pdf

8. The general insecurity of SMTP as it relates to worms/spam
"Sobig's Success Prompts Calls for Secure Email" Paul Roberts, September 12, 2003.
http://www.pcworld.com/news/article/0,aid,112411,00.asp

Beagle's ties to spam/seeding
"New virus spread through burst of spam" Bob Sullivan, August 9, 2004.
http://www.msnbc.msn.com/id/5652313/

9. Two very good looks at virus writing for profit:
"The real impact of viruses" Dinah Greek, January 6, 2004.
http://www.vnunet.com/features/1151775

"Online Extortion Works" Scott Granneman, SecurityFocus, December 12, 2004.
http://www.securityfocus.com/columnists/283

10. FBI Most Wanted Alert for Saad Echouafni for Computer Intrusion and Distributed Denial of Service
http://www.fbi.gov/mostwant/alert/echouafni.htm

11. For example, PatchLink's product literature:
http://www.patchlink.com/products_services/patchlink_update.html

12. "Microsoft 'slammed' by its own vulnerability" Paul Roberts, January 28, 2004.
http://www.computerworld.com/securitytopics/security/story/0,10801,77945,00.html

"Microsoft to revamp patch management software" John Fontana, September 1, 2003.
http://www.nwfusion.com/news/2003/0901mspatch.html

Microsoft Path Management Briefs (Slammer, etc.):
http://www.microsoft.com/technet/security/guidance/secmod193.mspx

13. Microsoft changing OS due to worms/bounty
"Executive E-mail: Microsoft Progress Report: Security" March 31, 2004.
http://www.microsoft.com/mscorp/execmail/2004/03-31security.asp

"Microsoft CEO Steve Ballmer Gives Cyber Security Speech" April 7, 2004.
http://www.bsa.org/usa/press/newsreleases/Cyber-Security-Speech.cfm
Steve Ballmer discussed new Windows technology:

"Other advances: Internet Explorer will automatically block unwanted pop-ups or downloads coming in from Web sites, which can carry damaging code. E-mail and Instant Messaging will handle file attachments in better and safer ways. The new Windows Security Center will help monitor and notify users about key security information on their systems. And new technology will help make it harder for worms and viruses to exploit what are called buffer overruns in a computer memory."

14. Gates' Letter to Microsoft Customers Outlining the "Microsoft Progress Report: Security"
http://www.nwfusion.com/news/2004/0405cybersecurity.html

Additional context is provided by John Leyden:
"Security is our 'biggest ever challenge' – Gates" John Leyden, April 1, 2004. "The Register"
http://www.theregister.co.uk/2004/04/01/security_is_our_biggest_ever/
"It is not a case of simply fixing a few vulnerabilities and moving on. Reducing the impact of viruses and worms to an acceptable level requires fundamentally new thinking about software quality, continuous improvement in tools and processes, and ongoing investments in resilient new security technologies designed to block malicious code before it can wreak havoc."
He singles out four recent viral epidemics: Slammer, Blaster, Sobig and Mydoom. These show how viruses and worms can spread more rapidly than ever before. Blaster in particular shows the threats posed by malicious

code are evolving. In response, software vendors have to make it easier for users (particularly consumers) to keep themselves secure."

15. Info on Benjamin worm:
http://securityresponse.symantec.com/avcenter/venc/data/w32.benjamin.worm.html

Information on blended threats like Nimda:
"Blended Threats: Case Studies and Countermeasures" Symantec Corporation, December 2001.
http://enterprisesecurity.symantec.com/Content/displaypdf.cfm?PDFID=152&EID=0

Copyright © 2004 infectionvectors.com All rights reserved.