Global Information Assurance Certification Paper

Cost of Malicious Code to Businesses

Erik Williams
william022
Security Essentials Practical
Capitol SANS
December 2000

Abstract

Computer infection from viruses, worms, and Trojan Horses, collectively known as malicious code, is a growing cost concern for businesses. An Internet search of the cost to businesses reveals that several different costs are measured –cost to prevent, cost to repair each infection, cost to repair all infections over time. These different measures of the cost of malicious code will be used to provide an overall picture of the cost of malicious code infection.

Malicious Code Types

There are several malicious code types that have infected computers. The Symantec AntiVirus Backgrounder Page [1] provides a description of the various types. Viruses, worms, and Trojan Horses vary in their sites and modes of infection and payload.

A virus is a file designed to spread from one file to another in a single computer [1]. Viruses may infect boot sectors and/or files of various types. Virus writers have also developed methods to make their products more destructive, harder to remove, and easier to propagate.

Viruses either reside in code that is necessary to the operation of the computer or hide in files that appear to contain only data but really contain executable code. Boot sector viruses infect (copy themselves to) the boot sector of logical drives – floppy disks (bootable or not, with or without data) and hard disks. The boot sector is a necessary part of the storage media that contains information about the format of the disk and a boot program. If a computer is booted from a boot sector infected floppy, the boot sector virus will infect the host computer's memory and boot sector of the hard disk and, from there, infect all floppy disk boot sectors used in the computer until all traces of the virus are removed from the computer hard disk boot sector and memory. Most of these

viruses were written for DOS, and with fewer DOS machines present on the market, the presence of these viruses in the wild is on the decline. File infector viruses corrupt .COM, .EXE, .SYS or other necessary system files. File infector viruses spread when uninfected programs are opened with the virus resident in computer memory. Macro viruses hide in files, such as word processing files, that used to contain only data. Modern word processors, however, now contain powerful executable code to automate processes. Macro viruses spread by individuals sharing innocuous-looking infected files with their macro protection turned off. To ensure the delivery of the virus payload, virus writers have made viruses that infect both files and boot sectors (multi-partite viruses), viruses that mutate (polymorphic viruses), viruses that hide themselves (stealth viruses), and viruses the attack anti-virus software (retro viruses). "W97M.Bablas.BR" is an example of a Microsoft Word macro virus.
Worms are bits of code that use a network to spread. The goal of a worm writer is to infect as many machines as possible, so they rely much less on human intervention to spread. Worms, unlike viruses, do not rely on attaching themselves to certain (system) files or sectors to spread [2]. Worms, as they are much more independent of the files resident on the computer and human intervention, can spread throughout a network very quickly because the means to do so are automated into the code. "PrettyPark" is an example of a worm.

A trojan horse is a program that performs some action that the victim did not intend [3]. Trojans, unlike worms and viruses, may not (though they may) seek to replicate themselves, but because they are disguised as something benign, spread by human intervention. "Trojan.Mirc.Abuser" is an example of a trojan horse.

For the discussion that follows, anti-virus includes anti-worm and anti-trojan-horse. Because the marketing departments of anti-malicious code vendors call products that are engineered to detect and remove, if possible, viruses, worms, and trojan horses, anti-virus products will include other forms of malicious code from here forward.

Cost to Prevent Infection

The cost to prevent infections is hard to measure. Measurements based on company reported data includes revenue from activities other than the sale of anti-virus

products. Measurement is further complicated by not knowing whether such sales are in response to an active infection that may be present on the buyer's computer or network. In some cases, this revenue might better be measured in the cost to repair. These revenues also include monies received for products and services related to providing customers with information assurance and security solutions (such as consulting, installing, and configuring firewalls) that are not strictly anti-virus prevention activities. Nevertheless, the numbers provided by some companies is helpful in indicating (not showing or proving) that companies and people spend considerable monies on

In their January 17, 2001 press release, Symantec Corp. reported revenues of $219.3 million for the quarter (third) ending 29 December 2000 [4]. On 22 January 2001, McAfee.com announced fourth quarter revenues of $12.1 million for the quarter ending 31 December 2000 [5]. Alladin Knowledge systems reported revenues of $11.8M for the quarter ended 31 December 2000 [6]. F-Secure earned 10.9 Million euros for the latest quarter reported 9 November 2000 [7].

The total revenues for the companies listed above in their self-reported latest quarters is roughly $250 Million. This figure does not include the money earned by privately held companies and shareware authors who do not have the same reporting requirements as publicly held companies. There are also many freeware anti-virus programs available. The money value of the time spent on these activities has not been adequately measured.

Cost to Repair

It appears that much more time and money is spent repairing the effects of malicious code than in preventing the same effects. According to Internet Week (in 1999) in North America, 6822 person-years were spent responding to virus, denial-of-service, and other cyberattacks. Virus attacks cost North American companies $1.6 Trillion in lost revenue. According to the Bureau of Economic Statistics, private industry's portion of the gross domestic product was $8.14 Trillion. The costs incurred by individuals were not measured in the survey.

As far as the cost of a single attack is concerned, Computerweek reports that the LoveLetter worm infected 90%

of all the computers in North America and Europe. The worldwide cost to business for this one infection was estimated to be $1 Billion.

Conclusion

While large sums of money are being spent on anti-virus prevention activities, absolutely staggering amounts of money are spent to repair the damage from malicious code. The insurance industry is trying, along with many other industries, to measure exactly what the costs being measured should be. There are business interruption costs, losses to other parties that may need to be compensated, and personal computing losses. Should a malicious code attack result in the loss of confidentiality of a trade secret, it will be very difficult to quantify what the loss of that property of the data will mean to the company. There is a similar problem with respect to personal computing and the less easily quantified problems associated with identity theft should a malicious code attack yield personal identifiers, account numbers and other data.

It appears that for every dollar spent on prevention in a given year, within the accuracy of this admittedly limited study, roughly $1000 dollars are saved from the repair cost. This conclusion is derived from multiplying the latest quarterly revenue figures quoted above and multiplying by 4 to get a yearly prevention expenditure. The rise in revenue is not considered. The cost to repair in the survey is divided by the yearly prevention expenditure. This is a reasonable first order of magnitude estimate – it does not appear that the data will support stating that $1 spent on prevention will save (on average) either $100 (one order of magnitude too low) or $10000 (one order of magnitude too high). This estimate, however, does indicate that there is a case to be made that malicious code protection is part of the due care standard because a reasonable and small effort (prevention) may yield an unreasonably large benefit or prevent an unreasonably large loss.

It is apparent that measuring the labor associated with repair and prevention is inexact. Preventing malicious code attacks is usually part of the information assurance and information security tasks that a responsible organization will undertake within their level of acceptable risk. Other activities that improve the

effectiveness of malicious code prevention include installing and maintaining perimeter protection in the form of properly configured firewalls and guards, reviewing audit logs, conducting integrity checks of critical systems files, and educating users and administrators on the proper use of the information system. It is clear that preventing malicious code attacks is one layer of a whole strategy to provide information assurance with defense in depth using technology, people, and operations.

Recommendation

Further research should be conducted into defining what activities constitute preventive activities. Activity based cost accounting methods should be used to measure more accurately the overall cost of each infection to each business and to measure more accurately the overall cost of infections to all businesses. Finally, the revenues and contributions of private companies and shareware authors should also be measured as well as the cost to persons and personal data.

Sources

[1] www.symantec.com/avcenter/virus.backgrounder.html (access date 20 February 2001).
[2] www.ca.com/virusinfo/virus_intro.htm (access date 20 February 2001).
[3] info.astrian.net/jargon/terms/t.html#Trojan_horse (access date 20 February 2001).
[4] www.ghost.com/press/2001/n010117b.html (access date 20 February 2001).
[5] www.mcafee.com/aboutus/press_room/press_releases/Jan2320012.asp? (access date 20 February 2001).
[6] www.avp.ru/ (access date 20 February 2001).
[7] http://www.f-secure.com (access date 20 February 2001).
[8] www.internetweek.com/story/TWB20000905S0001 (access date 20 February 2001).
[9] www.bea.doc.gov/bea/dn2/gpoc.htm (access date 20 February 2001).
[10] www.computerweek.co.za/news/2000/000508/monday_1iloveyou.htm (access date 20 February 2001).

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event