ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (137-143), Month: April-June 2014, Available at: www.researchpublish.com

Computer Viruses as an Artificial Life A Narrative Summary

Mr.Shyam Sundar.R[#1], Mrs.Rathi[#2], R.Sushmitha[#3]

Student[#1,#3] Professor[#2]
CSE Department, Saveetha School Of Engineering, Saveetha University, Thandalam , chennai,India

Abstract: **There has been hefty interest in pc viruses since they 1st appeared in 1981, and particularly within the past few years as they need reached epidemic numbers in several per- measuring instrument pc environments. Viruses are written concerning as a security downside, as a social downside, and as a doable means that of playing helpful tasks in an exceedingly distributed computing setting. Scientists are questioning and confirming whether or not the pc viruses are style of artificial life like self replicating organism or not. The target of this paper is to gift a completely unique approach to explain however a malicious program can be thought-about as a synthetic life.**

Keywords: **Epidemic, Sonar, Self-replicating, Artificial Life, malicious program, Organism.**

I. INTRODUCTION

The ``Computer Virus" downside was 1st delineate in 1984 [1], once the results of many experiments and substantial theoretical work showed that viruses might unfold, primarily unrestrained, even within the most `secure' pc systems; that they might cause widespread and primarily unlimited injury with very little effort on the a part of the virus writer; that detection of viruses was undecidable; that several of the defences that might be devised in comparatively order were ineffective against a heavy attacker; which the most effective defences were restricted transitivity of knowledge flow, restricted operate so mathematician capability [2] was out of stock, and restricted sharing.

In ensuant papers; it absolutely was shown that restricted sharing, within the most general case, would cause the data flow in an exceedingly system to create a partly ordered set of knowledge domains [3]; it absolutely was tested that limiting of transitivity, practicality, and sharing were the sole `perfect' defence [4]; and it absolutely was advised that a quality primarily based defensive against viruses can be sensible [5]. It absolutely was conjointly shown [4] that viruses might `evolve' into any result that a Turing machiner|information processing system} might compute, therefore introducing a severe downside in detection and correction, alteration the association between pc viruses and artificial life, and introducing the likelihood that viruses can be a awfully powerful tool in parallel computing. Just because pc viruses don't exist as organic molecules might not be enough reason to dismiss the classification of this type of “vandal ware” as a style of life. This paper begins with an outline of however pc viruses operate and their history, and of the assorted ways in which pc viruses are structured. It then examines however viruses meet properties related to life as outlined by some researchers within the space of artificial life and self- organizing systems. The paper concludes with some comments directed towards the definition of unnaturally “alive” systems and experimentation.

II. VIRUS STRUCTURE AND OPERATION

True viruses have 2 major components: one that handles the unfold of the virus, and a “payload” or “manipulation” task. The payload task might not be gift (has null effect), or it should look a group of planned circumstances before triggering. For a malicious program to figure, it somehow should add itself to alternative viable code. The infective agent code is sometimes dead before the code of its infected host (if the host code is ever dead again). One style of classification of pc viruses relies on the 3 ways a plague could add itself to host code: as a shell, as AN add-on, and as intrusive code. A fourth type, the alleged companion virus, isn't extremely a plague in any respect, however a style of malicious program that uses the execution path mechanism to execute in situ of a traditional program. Not like all alternative infective agent forms, it doesn't alter Any existing code in any fashion: companion viruses produce new viable files with a reputation kind of like an existing program, and chosen so they're ordinarily dead before the “real” program. As companion viruses aren't real viruses unless one uses a additional encompassing definition of virus, they'll not be delineate more here. The subsequent sub section discusses concerning differing kinds of viruses dominates the IT systems and networks.

Shell viruses: A shell virus is one that forms a “shell” (as in “eggshell” instead of “Unix shell”) round the original code. In effect, the virus becomes the program, and also the original host program becomes an indoor subprogram of the infective agent code. AN extreme example of this might be a case wherever the virus moves the first code to a replacement location and takes on its identity. Once the virus is finished execution, it retrieves the host program code and begins its execution. The majority boot program viruses may be classified as shell viruses.

Add-on viruses: Most viruses are add-on viruses. They operate by appending their code to the host code, and/or by relocating the host code and inserting their own code to the start. The add-on virus then alters the beginning up data of the program, execution the infective agent code before the code for the most program. The host code is left nearly utterly untouched; the sole visible indication that a plague is gift is that the file grows larger, if that may so be detected.

Intrusive viruses: Intrusive viruses operate by overwriting some or all of the first host code with infective agent code. The replacement can be selective, as in exchange a subprogram with the virus, or inserting a replacement interrupt vector and routine. The replacement may be in depth, as once massive parts of the host program ar utterly replaced by the infective agent code. Within the latter case, the first program will now not operate properly. Few viruses ar intrusive viruses.

III. VIRUSES GENERATION

Since the primary viruses were written, we've got seen what could also be classified as 5 “generations” of viruses. every new category of viruses has incorporated new options that create the viruses harder to discover and take away. Here, like alternative classification and naming problems associated with viruses, completely different researchers use different terms and definitions. The subsequent list presents one classification derived from variety of those sources. Note that these “generations” don't essentially imply chronology. for example, many early viruses (e.g., the “Brain” and “Pentagon” viruses) had hiding and armoured characteristics. Rather, this list describes increasing levels of sophistication and quality portrayed by pc viruses within the DOS setting.

First Generation: Simple:

The first generation of viruses were the straightforward viruses. These viruses did nothing terribly husband than replicate. several new viruses being discovered nowadays still fall under this class. injury from these easy viruses is sometimes caused by bugs or incompatibilities in computer code that weren't anticipated by the virus author. 1st generation viruses do nothing to cover their presence on a system, so that they will sometimes be found by means that as easy as noting a rise in size of files or the presence of a particular pattern in AN infected file.

Second Generation: Self- Recognition:

One downside encountered by viruses is that of continual infection of the host, resulting in depleted memory and early detection. Within the case of boot sector viruses, this might (depending on strategy) cause an extended chain of joined sectors. within the case of a program-infecting virus, continual infection could end in continual extension of the host program when it's re-infected. There are so some older viruses that exhibit this behaviour.

To stop this needless growth of infected files, second-generation viruses sometimes implant a singular signature that signals that the file or system is infected. The virus can check for this signature before trying infection, and can place it once infection has taken place; if the signature is gift, the virus won't re-infect the host. a plague signature may be a characteristic sequence of bytes at a notable offset on disk or in memory, a selected feature of the directory entry (e.g., alteration time or file length), or a special call on the market only the virus is active in memory. The signature presents a mixed blessing for the virus. The virus now not performs redundant infections which may gift a clue to its presence, however the signature will offer a technique of detection. Virus sweep programs will scan files on disk for the signatures of notable viruses, or perhaps “inoculate” the system by providing the infective agent signature in clean systems to stop the virus from trying infection.

Third Generation: Stealth:

Most viruses could also be known on a contaminated system by means that of scanning the auxiliary storage and sorting out a pattern of knowledge distinctive to every virus. To counteract such scans, some resident viruses use hiding techniques. These viruses subvert hand-picked system trip interrupts after they ar active. Requests to perform these operations are intercepted by the virus code. If the operation would expose the presence of the virus, the operation is redirected to come back false data.

For example, a standard virus technique is to intercept I/O requests that may scan sectors from disk. The virus code monitors these requests. If a scan operation is detected that may come back a block containing a duplicate of the virus, the active code returns instead a duplicate of the information that may be gift in AN antiseptic system. During this approach, virus scanners ar unable to find the virus on disk once the virus is active in memory. Similar techniques could also be utilized to avoid detection by alternative operations.

Fourth Generation: Armoured: As anti-virus researchers have developed tools to analyse new viruses and craft defences, virus authors have turned to ways to alter the code of their viruses. This “armouring” includes adding confusing and needless code to create it harder to analyse the virus code. The defences may take the shape of directed attacks against anti-virus computer code, if gift on the affected system. These viruses appeared beginning in 1990.

Fifth Generation: Polymorphic:

The most recent category of viruses to look on the scene are the polymorphic or self-mutating viruses. These are viruses that infect their targets with a changed or encrypted version of themselves. By variable the code sequences written to the file (but still functionally comparable to the original), or by generating a distinct, random encoding key, the virus within the altered file won't be recognisable through the utilization of easy computer memory unit matching. To discover the presence of those viruses needs that a additional advanced algorithmic rule be used that, in effect, reverses the masking to see if the virus is gift.

Several of those viruses became quite wide-spread. Some virus authors have free virus “toolkits” that may be incorporated into an entire virus to offer it polymorphic capabilities. These toolkits are circulated on varied bulletin boards round the world, and incorporated in many viruses.

IV. DEFENCES AND OUTLOOK

Activity Monitors: Activity monitors are programs that are resident on the system. They monitor activity, and either raises a warning or take special action within the event of suspicious activity. Thus, tries to change the interrupt tables in memory, or to rewrite the boot sector would be intercepted by such monitors. this type of defence may be circumvented (if enforced in software) by viruses that activate earlier within the boot sequence than the monitor code.

They are more at risk of virus alteration if used on machines while not hardware memory protection — as is that the case with all common personal computers. Another style of monitor is one that emulates or otherwise traces execution of a suspect application. The monitor evaluates the actions taken by the code, and determines if any of the activity is comparable to what a plague would undertake. acceptable warnings are issued if suspicious activity is known.

Scanners: Scanners are the foremost fashionable and widespread style of virus defences. A scanner operates by reading information from disk and applying pattern matching operations against an inventory of notable virus patterns. If a match is found for a pattern, a plague instance is declared. Scanners are quick and straightforward to use, however they suffer from several disadvantages. Foremost among the disadvantages is that the list of patterns should be unbroken up-to-date. within the DOS world, new viruses are showing by as several as many dozen every week. Keeping a pattern file up-to-date during this apace dynamical setting is troublesome. A second disadvantage to scanners is one amongst false positive reports. As additional patterns are value-added to the list, it becomes additional possible that one amongst them can match some otherwise legitimate code. an extra disadvantage is that polymorphic viruses can't be detected with scanners.

Integrity Checking: Integrity checking conjointly has drawbacks. On some systems, viable files amendment whenever the user runs the file, or once a replacement set of preferences is recorded. Continual false positive reports could lead the user to ignore future reports, or disable the utility. it's conjointly the case that a amendment might not be detected till when AN altered file has been run and a plague unfold. Additional significantly, the initial calculation of the check code should be performed on a known-unaltered version of every file. Otherwise, the monitor can ne'er report the presence of a plague, in all probability leading the user to believe the system is antiseptic. many vendors have begun to make self-checking into their merchandise. this can be a style of integrity make certain is performed by the program at varied times because it runs. If the self-check reveals some sudden amendment in memory or on disk, the program can terminate or warn the user. This helps to signal the presence of a replacement virus quickly so more action could also be taken.

V. VIRUS AS PATTERNS IN HOUSE TIME

There is a close to match to the present characteristic. Viruses are portrayed by patterns of pc directions that exist over time on several pc systems. Viruses aren't related to the physical hardware, however with the directions dead (sometimes) by that hardware. pc viruses, like all purposeful code, are merely manifestations of algorithms. The algorithms themselves conjointly represent an underlying pattern. it's questionable if these patterns exist in house, however, unless one extends the definition of house to “cyberspace,” as portrayed by a automatic data processing system. The patterns of the viruses ar a brief set of electrical and force field changes within the memory or storage of pc systems. The existence of the virus is merely inside these patterns of energy. Arguably, the code for every virus can be written in ink on paper, leading to a additional substantiating existence. That, however, is simply a illustration of truth virus, and may not be viewed as existence any longer than an image of an individual is itself the person.

VI. SELF-REPRODUCTION OF VIRUSES AND STORAGE

One of the first characteristics of pc viruses is their ability to breed themselves (or AN altered version of themselves). Thus, this characteristic looks to be met. one amongst the key characteristics is their ability to breed. However, it's maybe additional attention-grabbing to look at this facet in lightweight of the agent of copy. The virus code isn't itself the agent, the pc is questionable if this may be thought-about enough for functions of classification as artificial life. The blueprints for a Xerox machine are capable of self-reproduction: once outside agents follow the directions in this, it's doable to provide a replacement machine that may then be wont to create a duplicate of them. it's not the blueprint (algorithm; virus) that's the agent of amendment, however the entity that interprets it. Storing of self-representation is that the most evident match for pc viruses. The code that defines the virus may be a guide that's utilized by the virus to duplicate itself. this can be kind of like the deoxyribonucleic acid molecules of what we tend to acknowledge as organic life.

VII. VIRUS METABOLISM

This property involves the organism taking in energy or matter from the setting and victimisation it for its own activity. pc viruses use the energy of computation gone by the system to execute. they are doing not convert matter, however create use of the current gift within the pc to traverse their patterns of directions and infect alternative programs. during this sense, they need a metabolism. Again, however, we tend to are forced to alter this read if we tend to examine the case additional closely. The expenditure of energy isn't by the virus, however by the underlying automatic data processing system. If the viruses weren't active, and an interactive game was being run instead, identical quantity of energy would be used. In most systems, albeit no program is being run, the energy use remains constant. Thus, we tend to should conclude that viruses don't even have a metabolism. Again, however, we tend to are forced to alter this read if we tend to examine the case additional closely. The expenditure of energy isn't by the virus, however by the underlying automatic data processing system. If the viruses weren't active AN interactive games were being run instead, identical quantity of energy would be used. In most systems, albeit no program is being run, the energy use remains constant. Thus, we tend to should conclude that viruses don't even have a metabolism.

VIII. PURPOSEFUL INTERACTIONS AND INTERDEPEDENCE

Viruses perform examinations of their host environments as a part of their activities. They alter interrupts, examine memory and disk architectures, and alter addresses to cover themselves and unfold to alternative hosts. They terribly clearly alter their setting to support their existence. several viruses accidentally alter their setting as a result of bugs or unforeseen interactions. the most important portion of harm from all pc viruses may be a results of these interactions. Living organisms can't be willy-nilly divided while not destroying them. Identical is true of pc viruses. Ought to a malicious program have some of its "anatomy" excised, the virus would in all probability stop to operate ordinarily, if at all. Few viruses are written with superfluous code, and notwithstanding, the operating code can't be divided while not disabling the virus. However, it's attention-grabbing to notice that the virus may be reassembled later and regain its purposeful standing. If a living organism (as we all know them) were to be divided into its element elements for a amount of your time, then obtaining reassembled, it might not become "alive" once more. During this sense, pc viruses are additional like easy machines or chemical reactions instead of instances of living things.

IX. VIRUS STABILITY UNDERMEATH PERTURBATIONS

Computer viruses run on a range of machines underneath completely different in operation systems. several of them are ready to compromise (and defeat) anti-virus and duplicate protection mechanisms. They will regulate on-the-fly to conditions of low storage, disk errors, and alternative exceptional events. Some are capable of running on most variants of fashionable personal computers underneath nearly any computer code configuration — a stability and hardiness seen in few business applications.

X. VIRUS EVOLUTION AND GROWTH

Here, too, viruses show a distinction from systems we tend to historically regard "alive." No pc viruses evolve as we tend to ordinarily use the term, though it's conceivable that a awfully advanced virus can be programmed to evolve and alter. However, such a plague would be thus massive and complicated on be several orders of magnitude larger than most host programs, and doubtless larger than the host in operation systems. Thus, there's some doubt that such a plague might run on enough hosts to permit it to evolve. (Note that "evolve" implies a amendment in operate or attributes; polymorphic viruses represent cases of random changes in structure however not practicality.) Higher-level mutations of viruses do exist, however. There are variants of the many notable viruses, with over a dozen notable for a few IBM computer viruses. The variations concerned may be terribly tiny, on the order of 2 or 3 directions distinction, to major changes involving variations in messages, activation, and replication. The supply of those variations seems to be programmers (the original virus authors or otherwise) WHO alter the viruses to avoid anti-viral mechanisms, or to cause completely different forms of injury. Polymorphic viruses alter their copies to avoid detection, however the pattern of alteration is ultimately somebody's product. These changes don't represent evolution, however. apparently, there's conjointly one case wherever 2 completely different strains of a Macintosh virus are notable to act to create infections not like the "parents," though these interactions sometimes turn out "sterile" offspring that are unable to breed more. This likewise doesn't seem to be evolution as we all know it. Viruses definitely do exhibit a style of growth, within the sense that there are additional of them in an exceedingly given setting over time. Some transient viruses can infect each file on a system when solely some activations. The unfold of viruses through business computer code and public bulletin boards is another indication of their wide-spread replication. though correct numbers are troublesome to derive, reports over the previous couple of years indicate AN approximate yearly doubling within the variety of systems infected by pc viruses. Clearly, pc viruses are exhibiting vital growth.

XI. ALTERNATIVE BEHAVIOURS OF VIRUS

As already noted, computers viruses exhibit "species" with well-defined ecological niches supported host machine sort, and variations inside these species. These species are custom-made to specific settings and can not survive if affected to a distinct environment. Some viruses conjointly exhibit predatory behaviour. for example, the DenZuk virus can search out and write instances of the Brain virus if each are gift on identical system. Alternative viruses exhibit territorial behaviour — marking their infected domain so others of identical sort won't enter and contend with the first infection. Some viruses conjointly exhibit self-protective behaviour, as well as camouflage techniques. it's necessary to notice, however, that none of those characteristics came from the viruses themselves. Rather, every amendment and addition to virus behaviour has been shaped by an outdoor agency: the software engineer. These changes are in reaction to a perceived got to “enhance” the virus — sometimes to create it harder to search out. it'd somewhat be argued that additional ancient living organisms may bear amendment from while not. As AN example, background could cause occasional random mutations. However, programmers are the sole supply of amendment to pc viruses, and this distinction is price noting; alternative living systems bear changes to themselves and their issue while not obvious outside agencies.

XII. CONCLUSION

Our study of pc viruses initially suggests they're near what we would outline as “artificial life.” However, upon nearer examination, variety of serious deficiencies may be found. This cause conclude that, pc viruses are either not “alive” or is it doable to refine them thus on create them “alive” while not drastically sterilization the definition of “life”. To counsel that pc viruses are alive conjointly implies that some a part of their setting — the computers, programs, or in operation systems — conjointly represents artificial life. will life exist in AN otherwise barren and empty ecosystem? A definition of “life” ought to in all probability embrace one thing concerning the setting within which that life exists. beyond any doubt, it's necessary to regulate our definitions and characteristics to cover pc viruses or to higher exclude them. This illustrates one amongst the basic difficulties with the complete field of artificial life: a way to outline essential characteristics in such the way on unambiguously outline living systems. PC viruses offer one attention-grabbing example against that such definitions could also be tested. From this, it may be discovered that pc viruses (and their kin) offer a motivating means that of modelling life. For a minimum of this reason, analysis into pc viruses (using the term in an exceedingly broader sense, ala Cohen) could also be of some scientific interest. By modelling behaviour victimisation pc vi- ruses, we tend to could also be ready to gain some insight into systems with additional advanced interactions. analysis into competition among pc viruses and alternative computer code, as well as anti-viral techniques, is of sensible interest similarly as scientific interest. changed versions of viruses like Thimble by’s Liveware may encourage be of final price. analysis into problems on virus defence ways, medicine, and on mutations and mixtures conjointly might offer valuable insight into computing. The matter with analysis on pc viruses is their threat.

True viruses are inherently unethical and dangerous. They operate while not consent or information, expertise has shown that they can't be recalled or controlled, and that they could cause in depth losses over a few years. Even viruses written to be begin causes vital injury as a result of sudden interactions and bugs. To experiment with pc viruses is such as experimenting with variola major or anthrax microbes— there could also be knowledge base to be gained, however the potential for fateful consequences looms massive. In one sense, we tend to use “computer viruses” daily. Editors, compilers, backup utilities, and alternative common computer code meet some definitions of viruses. However, their general nature is understood to their users, and that they don't operate while not a minimum of the inexplicit permission of these users. moreover, their replication is usually underneath the shut management or observation of their users. it's these variations from the informal malicious program that creates the latter thus attention-grabbing, however. These variations are exactly what counsel that pc viruses approach a style of artificial life. If we tend to ar to still analysis pc viruses, we'd like to search out fail-safe ways in which of doing thus. this can be a significant analysis topic in itself. The danger of making and accidentally cathartic additional refined viruses is just too nice to risk, particularly with our increasing reliance on computers in essential tasks. One approach can be to construct custom computing environments for study, completely different enough from all existing pc systems that a malicious program underneath study would be utterly non-functional outside it. this can be AN approach kind of like what has been soft on Core Wars. Another approach is to solely study existing viruses in notable environments.

REFERENCES

[1] F. Cohen, ``Computer Viruses - Theory and Experiments", originally showing in IFIP-sec eighty four, conjointly showing in DOD/NBS seventh Conference on pc Security, and IFIP-TC11 ``Computers and Security", V6(1987), pp22-35 and alternative publications in many languages.

[2] A. Turing, ``On calculable Numbers, with AN Application to the Entscheidungs problem", London maths Soc Ser two, 1936.

[3] F. Cohen, ``Protection and Administration of knowledge Networks with Partial Orderings", IFIP-TC11, ``Computers and Security", V6#2 (April 1987) pp 118-128.

[4] F. Cohen, ``Computer Viruses", treatise at the University of Southern CA, 1986.

[5] F. Cohen, ``A quality primarily based Integrity Maintenance Mechanism", Conference on data Sciences and Systems, university, March 1986.

[6] W. Gleissner, ``A Mathematical Theory for the unfold of pc Viruses", ``Computers and Security", IFIP TC-11, V8#1, Jan. 1989 pp35-41.

[7] F. Cohen, ``A Short Course on pc Viruses", ASP Press, PO Box 81270, Pittsburgh, PA 15217, 1990.

[8] H. Highland, ``Computer Virus Handbook", Elsevier, 1990.

[9] S. White, ``A standing Report on IBM malicious program Research", Italian malicious program Conference, 1990.

[10] K. Brunnstein, ``The malicious program Catalog", DPMA, IEEE, ACM fourth malicious program and Security Conference, 1991 D. Lefkon ed.

[11] F. Cohen, ``Current Trends in malicious program Research", ordinal Annual Invited conference on pc Viruses - keynote speech, Oct. 10, 1988. New York, NY

[12] F. Cohen, ``Models of sensible Defenses Against pc Viruses", IFIP-TC11, ``Computers and Security", V7#6, December, 1988.

[13] M. Cohen, ``A New Integrity primarily based Model for restricted Protection Against pc Viruses'', Masters Thesis, The Pennsylvania State University, faculty Park, PA 1988.

[14] F. Cohen, ``A cryptologic confirmation for Integrity Protection", IFIP-TC11 ``Computers and Security", V6#6 (Dec. 1987), pp 505-810.

[15] Y. Huang and F. Cohen, ``Some Weak Points of 1 quick cryptologic confirmation algorithmic rule and its Improvement", IFIP-TC11 ``Computers and Security", V8#1, February, 1989